TOPICS OF DIVISIBILITY

To contain is to divide

studied and explored by

Bruno Bosbach

2013

Preview

The set of integers forms a commutative ring whose elements admit a unique decomposition into primes.

In this folder three lecture notes are bound, concerning topics, developed by dropping or replacing special properties of this most natural and most special ring.

A. A first lecture note concerns *d-semigroups* (*divisibility-semigroups*). This structure was created by the author as a common abstraction of *d-lattices* (*distributive lattices*) and *ℓ-groups* (*lattice ordered groups*). defined as an *algebra* $(S,\ \cdot\ ,\wedge)$ *of type* (2,2), satisfying:

(A1) $(S,\cdot)$ is a *semigroup*.

(A2) $(S,\wedge)$ is a *semilattice*.

(A3) $\forall\, x,a,b,y:\quad x(a\wedge b)y \;=\; xay\wedge xby\,.$

(A4) $a\leq b \Longrightarrow \exists\, x,y:\ ax \;=\; b \;=\; ya\,.$

Most amazingly, large parts of ℓ-group theory may be transposed to d-semigroups by modified methods, partly by routine, but partly – as well – by strenuous and even most strenuous efforts.

B. In a second contribution an abstract ideal theory is established, based on the structure of algebraic lattices and dominated by the Mori condition:

To contain is to divide.

C. Finally, in part III specializations and generalizations of left-residuation-groupoids are studied, that is groupoids satisfying

$$\forall a,b\,\exists\, a*b:\ \ b\,\Big|_l\, ax \Longleftrightarrow a*b\,\Big|_l\, x\,.$$

Classic examples of this type are for instance boolean algebras, lattice-ordered loops (including lattice ordered groups), and ideal structures of multiplicative structures like rings, semigroups, lattices, etc.

EACH OF THESE LECTURE NOTES is written in a self-contained manner. Presented are the author's main contributions to divisibility until now, except for his early *Decomposition and Ideal Theory for Semigroups* – on the one hand, but enriched by passages unpublished so far, which in any case would justify some articles in their own right – on the other hand.

Kassel, 12. 31. 2014 – B.B.

Divisibility Semigroups

Dedicated to

Jan Jakubík (*1923)
the excellent pioneer and strong lifelong worker
on ordered structures
on the occasion of his 90. birthday

by Bruno Bosbach
2013

Contents

1 Introduction **5**

1.1 Fundamental Notions 5

1.2 Synopsis 8

2 Arithmetics **21**

2.1 Fundamental arithmetic of d-semigroups 21

2.2 The Cone 24

2.3 A Decomposition Formula 26

2.4 Commutativity 28

2.5 Absolute Values 30

2.6 The idempotent Kernel 34

2.7 The cancellative Kernel 34

2.8 The complementary Case 39

3 Classical Extensions **47**

3.1 An Identity Extension 47

3.2 A Quotient Extension 52

4 Ideals **57**

4.1 p-ideals, m-ideals, d-ideals 57

4.2 c-Ideals 62

4.3 v-Ideals and u-Ideals 67

5 Congruences **71**
5.1 Extensions . . . 71
5.2 Concrete Congruences . . . 75
5.3 Finest Congruences . . . 77
5.4 Subdirectly irreducible d-semigroups . . . 80

6 Representation **85**
6.1 Starting from l-ideals . . . 85
6.2 Starting from c-ideals . . . 88
6.3 r-Semigroups . . . 96
6.4 Further Consequences . . . 102

7 Complete d-semigroups **105**
7.1 Completeness and Cone . . . 105
7.2 Continuous d-Semigroups . . . 108

8 Archimedean d-semigroups **119**
8.1 Commutativity . . . 119
8.2 Appendix . . . 124
8.3 The Identity Extension . . . 126

9 Linear d-monoids **131**
9.1 Dense Chains . . . 131
9.2 Continuous Chains . . . 134
9.3 Hölder and Clifford . . . 138
9.4 Archimedean Linear d-semigroups . . . 144
9.5 Interval Semigroups . . . 145

10 Jakubuik Chains in lo-groupoids **149**

11 Special archimedean d-semigroups 155

11.1 Hyper-archimedean d-Semigroups . . . 155

11.2 Super-archimedean d-semigroups . . . 158

11.3 Discrete Archimedean d-Semigroups . . . 164

11.4 Factorial d-Semigroups . . . 166

12 Ideal Extensions 171

12.1 Cut Criteria . . . 171

12.2 Sufficient Conditions . . . 179

13 Polars 183

13.1 Prime c-ideals . . . 183

13.2 Polars . . . 186

13.3 Filets and z-ideals . . . 189

13.4 Minimal prime c-Ideals . . . 192

13.5 Direct Factors . . . 194

14 Orthogonality and Linearity 199

14.1 Lexicographical Extensions . . . 199

14.2 d-Monoids with a Base . . . 206

14.3 Ortho-finite d-Monoids . . . 208

14.4 Projectable d-Monoids . . . 212

14.5 Lateral Completeness . . . 214

15 Real extensions 217

15.1 Subdirect real Products . . . 217

15.2 Direct real Sums . . . 219

15.3 A general Cube Theorem . . . 220

15.4 Continuous Cube Extensions . . . 225

15.5 Lattice Cubes . . . 229

16 Representable d-semigroups **233**

16.1 Foundation 233

16.2 The general Case 234

16.3 d-Monoids 238

16.4 Hyper-normal d-Monoids 242

17 Separative d-semigroups **249**

17.1 The Structure of E·C 250

17.2 Separative congruences 255

18 Inverse divisibility structures **263**

18.1 Inverse left d-semigroups 263

18.2 Representation 267

19 Axiomatical outlook **275**

19.1 Some Axiomatic 275

Chapter 1

Introduction

1.1 Fundamental Notions

By a *lattice group* we mean an algebra $\mathfrak{V} = (V, \cdot, \wedge, \vee, ^{-1})$ of type $(2, 2, 2, 1)$ forming a *group* under $\cdot$ and $^{-1}$ and a *lattice* under $\wedge$ and $\vee$, such that in addition $x(a \wedge b)y = xay \wedge xby$ is satisfied. Lattice groups are briefly called *ℓ-groups.*

The most elementary example is the ℓ-group $(\mathbf{Z}, +, \leq)$, whereas the most classical candidate is the the *module group* $\mathbf{Q}(\vartheta)$, studied for the first time by Richard Dedekind . And similarly to the notion of a *lattice,* by Dedekind exhibited as *dual group,* when establishing *ideal theory,* the notion of an *ℓ-group* was anticipated by him far before *ℓ-group theory* became a theory in its own right.

From the structural point of view the module group above is of a type similar to that of $\mathfrak{Q} = (\mathbf{Q}, \cdot, |_N, ^{-1})$ under $a \,|_N\, b :\Longleftrightarrow \exists n \in \mathbf{N} : a \cdot n = b$. Furthermore – as a classical aspect we notice that any abelian ℓ-group may be considered as the *divisibility monoid* of some suitable *GCD-domain* (Jaffard) even more of some Bézout *domain* (Ohm) . Hence: commutative ℓ-group theory is theory of domains whose *finitely generated ideals* are *principal ideals.*

As the starting point of a general – not necessarily commutative – *ℓ-group theory* we have to mention the ground breaking and pioneering paper [12] of G. Birkhoff, where already the group of *isotone* or equivalently *order preserving chain permutations* is considered under *composition* and *pointwise minimum.* And as the "big break through" we have to mention

The Theorem of Holland. *Any lattice group is a lattice group of order preserving permutations of some suitably chosen chain*,

which provided the "missing link" between ℓ-groups and *chain theory.*

MOREOVER: It was this theorem by which the author was fascinated and motivated and which in a modified version was the central result of his first contribution, [17], to the theory of *divisibility semigroups,* briefly *d-semigroups.*

The crucial idea is simple: Dropping the *cancellation law* but requiring the *factor condition* the class of algebras under consideration contains the *distributive lattice,* for short *d-lattice,* as well. And this leads to

A Theorem of Birkhoff. *Any distributive lattice is a subdirect product of* 2*-element lattices, whence it is also a lattice of sets.*

PRECISELY: By a *d-semigroup* we mean an *algebra* $(S\,\cdot\,,\wedge)$ *of type* (2,2), satisfying:

(A1) $(S,\cdot)$ is a *semigroup.*

(A2) $(S,\wedge)$ is a *semilattice.*

(A3) $\forall\, x,a,b,y: \quad x(a\wedge b)y \;=\; xay\wedge xby\,.$

(A4) $a\leq b \Longrightarrow \exists\, x,y:\; ax \;=\; b \;=\; ya\,.$

AND AGAIN: This defines a common abstraction of the ℓ-group an the d-lattice.

d-semigroups seem to be rather weak, since dropping the *left factor condition* we are led to arbitrary wild structures – consider any lattice and define $ab := b$. On the other hand the *left/right factor condition* yields a strong interdependence between the underlying semigroup and the underlying semilattice.

This will lead to the meta-theorem that large parts of ℓ-group theory, included the theorem of Holland, are carried over, as is evaluated as most amazingly in a review of Keimel. The reason

Factors are strong pseudo-inverses.

As a typical example of a d-semigroup we present the monoid of all finitely generated ideals of an *arithmetical* (*commutative*) *ring.* That is a ring with a distributive ideal lattice, or – equivalently – a ring that satisfies the fundamental implication

$$\langle a_1, \dots, a_n\rangle \supseteq \langle b\rangle \Longrightarrow \langle a_1, \dots, a_n\rangle \,\Big|\, \langle b\rangle\,.$$

These *ideal semigroups* provide most special examples as far as they may be considered as ideal semigroups of *Bézout-rings.* Hence for instance their *filters* $\mathfrak{f}$ satisfy the rules of *ring ideal theory,* in particular the rules below:

(SU) $$a\cdot x \subseteq \mathfrak{b} + a\cdot\mathfrak{y} \;\Longrightarrow\; x \subseteq \mathfrak{b} : a + \mathfrak{y}\,.$$

(AP) $$\begin{aligned}&(\forall a\in\mathfrak{a}\ \exists 1\le i\le n : a\in\mathfrak{p}_i)\\ &\Longrightarrow \mathfrak{a}\subseteq\mathfrak{p}_j\ \ (\exists j : 1\le j\le n)\,.\end{aligned}$$

(PK) $$\mathfrak{R}/P = \overline{\mathfrak{R}} \quad \text{satisfies}\quad \overline{x}\cdot\overline{y} = \overline{x}\cdot\overline{z} \neq \overline{0} \Longrightarrow \overline{y} = \overline{z}\,.$$

BUT: The aim of this note is

A general theory of d-semigroups.

To this end we start from the system (A1) through (A4) above and show first of all:

d-semigroups are ℓ-semigroups – as distributive as possible.

Symptomatical and fundamental, as well, for d-semigroups is:

A Decomposition Theorem: *Any d-semigroup admits a subdirect decomposition into semigroups of order isomorphisms mapping order ideals of a chain onto order filters of this chain, considered under* composition *and* pointwise minimum, *which subsumes both,* HOLLAND*'s and* BIRKHOFF*'s theorem.*

Structures of this type are called – here – *ideal/filter semigroups,* briefly *r-semigroups,* (according to the German "Randisomorphismenhalbgruppe"). r-semigroups need not be d-semigroups, which is shown by the r-semigroup of $\mathbf{Q}$. Observe that in this example the order ideals $A := \{x \mid x < \pi\}$ and $B := \{y \mid y < 0\}$ are isomorphic, whereas the corresponding filters $\mathbf{Q} - A$ and $\mathbf{Q} - B$ are not.

However: It will be shown later on that any *r-semigroup* admits a d-semigroup extension, whence d-semigroups and r-semigroups have the same elementary arithmetic. This is the particular charm of r-semigroup theory.

The interested reader will see that this lecture note provides a good deal of algebraic d-semigroup theory, but only little r-semigroup theory. Here remains much to be done, consult for instance the fundamental lecture note [58] of Andrew M. Glass. In particular:

r-semigroups don't provide *factors* in any case of $a \leq b$, but – roughly speaking – the set of all ax – nicely approximates b. This may be illustrated by a classical example:

In the additive semigroup $\mathfrak{Q}^+[\pi]$, generated by $\mathbf{Q}^{\geq 0}$ and π, we are not in the position to solve $1 + x = \pi$, but in the sense of order topology we are able to "reach" any interval of π. So it seems interesting, whether (A1) & (A2) & (A4) together with this requirement provide an r-semigroup.

BUT: Sofar not to much has been done towards this special problem, and not much more has been done from the general topological point of view, although there are some papers concerning *totally ordered topological semigroups,* consult [39], in particular the results of Faucett, [53], [54].

In order to give an informative survey for the interested *outsider*, in the subsequent *synopsis* we give a preview and outline about the central aspects, according to the chapters of this note. This is much more than a preface of usual type, but offers a concentrated study of the main topics in a most direct manner.

1.2 Synopsis

Chapter 1 presents the basic notion of a d-semigroup.

By a *d-semigroup* we mean an *algebra* $(S, \cdot, \wedge)$ *of type* (2,2), satisfying:

(A1) $(S, \cdot)$ is a *semigroup.*

(A2) $(S, \wedge)$ is a *semilattice.*

(A3) $\forall\, x, a, b, y : \quad x(a \wedge b)y \;=\; xay \wedge xby\,.$

(A4) $a \leq b \Longrightarrow \exists\, x, y :\; ax \;=\; b \;=\; ya\,.$

Obviously, the d-semigroup is a common abstraction of the *lattice group*, which we get by requiring that $(S, \cdot)$ be a *group*, and of the *distributive lattice*, which we get by requiring that $(S, \cdot)$ be *semilattice.*

A d-semigroup $\mathfrak{S}$ is called a *d-monoid*, if it contains an *identity element* 1. A d-monoid is called *right normal*, if in addition to (A1) through (A4) it even satisfies:

$$\forall\ a, b\ \exists\ a^\circ \wedge b^\circ = 1 :\ (a \wedge b)a^\circ = a\ \&\ (a \wedge b)b^\circ = b\ .$$

In case that $\mathfrak{S}$ is right and left normal, $\mathfrak{S}$ is called briefly *normal.*

Normality plays a most important role w. r. t. commutative rings with identity. More precisely:

Theorem. *In a commutative ring with identity the lattice of ideals is distributive iff the condition* $\mathfrak{a} : \mathfrak{b} + \mathfrak{b} : \mathfrak{a} = (1)$ *is satisfied and this is the case iff finitely generated ideals* $\mathfrak{a}$ *satisfy* $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \,|\, \mathfrak{b}$.

Chapter 2 presents the rules of arithmetic. In particular we get: *Any d-semigroup is* $\vee$*-closed and satisfies:*

$$(i) \qquad x(a \wedge b)y = xay \wedge xby\,,$$

$$(ii) \qquad x(a \vee b)y = xay \vee xby\,,$$

$$(iii) \qquad x \wedge (a \vee b) = (x \wedge a) \vee (x \wedge b)\,,$$

$$(iv) \qquad x \vee (a \wedge b) = (x \vee a) \wedge (x \vee b)\,,$$

where (iii) *and* (iv) *are equivalent – as is well known.*

d-semigroups need not contain an *identity element* 1, but according to condition (A4) for any a there exists an element u with $au = a$ and an element v with $va = a$. This leads to some *private unit* e_a, satisfying $ae_a = a = e_a a$, briefly to a unit of a. However, such a unit need neither be *idempotent* nor need it be uniquely determined. Moreover any pair of units e, f of a satisfies $e \vee a = f \vee a =: a^+$, a formula, which follows in d-monoids immediately from the existence of the identity.

In *po-semigroups* a particular and structure determining role is played by the *positive elements.* These are the elements p satisfying $pa \geq a \leq ap$ $(\forall a \in S)$. In a d-semigroup they form a structure determining sub-d-semigroup $\mathfrak{P}$, called the *positive cone,* briefly the *cone.* Positive elements in d-semigroups are characterized by $a = e \vee a$ for at least one and thereby for all units e of a. Therefore condition (A4) is always satisfied even by positive elements x, y.

Large parts of d-monoid theory are developable by studying the cone. With respect to this aspect, not only the *positive value* a^+ but also the *absolute value* $|\,a\,|$ is of great importance.

We define: Let e be a unit of a and suppose $(e \wedge a)a^* = e$. Then $|\,a\,|$ is defined by $|\,a\,| = (e \wedge a)a^*$. This is possible, since $(e \vee a)a^*$ does not depend on the special chosen a^* – as will turn out in chapter 1.

$|\,a\,|$ is built like the absolute value in $\mathbf{R}$, recall $|\,a\,| := -\min(0,a) + \max(0,a)$ *via* $|\,a\,| := a^+ \cdot a^*$ $(ea = a = ae \;\&\; (e \wedge a)a^* = e)$. In particular we get:

(*i*) $$|\,a^+\,| \;=\; a^+ .$$

(*ii*) $$|\,a \cdot b\,| \;\leq\; |\,a\,| \cdot |\,b\,| \cdot |\,a\,| .$$

(*iii*) $$|\,a \wedge b\,| \;\leq\; |\,a\,| \vee |\,b\,| \geq |\,a \vee b\,| .$$

Further essential influence on the structure of a d-semigroup $\mathfrak{S}$ is taken by the *idempotent* and *cancellable* elements. They form the *idempotent kernel* $\mathfrak{E}$ and the *cancellative kernel* $\mathfrak{C}$ of $\mathfrak{S}$.

In addition all idempotent elements are *positive* and *central.*

Next we mention a decomposition formula, matching multiplication and meet:

Proposition. *Choose arbitrary elements* a, b, c, d *and positive elements* a', b'', c', d'', *such that*

$$(a \wedge c)a' = a \;\&\; (a \wedge c)c' = c \;\textit{and}\; b''(b \wedge d) = b \;\&\; d''(b \wedge d) = d$$

are satisfied. Then it follows:

$$ab \wedge cd = (a \wedge c)(a' \wedge d'')(b'' \wedge c')(c \wedge d) \;.$$

In excess of the facts mentioned so far Chapter 1 presents a series of formulas w. r. t. *residuation*, which may be left aside here since they are of auxiliary character.

Chapter 3 is immediately characterized. It is shown:

Let $\mathfrak{S}$ be a d-semigroup without identity 1 , then $\mathfrak{S}$ admits a canonical *monoid extension* Σ, symbolized by $\mathfrak{S}^1$, which might be called the *identity hull,* since each element of this extension is of type $a \cdot (1 \wedge b)^{-1}$ or .... .

Furthermore any d-monoid $\mathfrak{S}$ admits a canonical *quotient extension* $\mathfrak{Q}$ such that all cancellable elements of $\mathfrak{S}$ remain cancellable in $\mathfrak{Q}$ and such that moreover all cancellable elements of $\mathfrak{Q}$ are invertible, whence $\mathfrak{Q}$ might also be called the *quotient hull.*

Chapter 4 provides the basic notions and results of an ideal theory for d-semigroups.

Since any $\mathfrak{S}$ is a *semiring* on the one hand and a *generalized ℓ-group* on the other hand, *lattice ideals* and *lattice filters* on the one hand and *semiring ideals* and *convex sub-d-semigroups* on the other hand take influence on the the theory of d-semigroups in a most natural manner. All at all one might say, that *d-ideals* $\mathfrak{a}$, these are subsets, satisfying $s\mathfrak{a}t \subseteq \mathfrak{a}$ and $\mathfrak{a} + \mathfrak{a} \subseteq \mathfrak{a}$, play a role, most similar to that of *Dedekind ideals* in ring theory, while *p-ideals,* these are *lattice ideals* A, satisfying $P \cap A \neq \emptyset$, will play a crucial role in *congruence theory,* whereas *c-ideals*, these are *convex substructures* containing 1, are essentially responsible for the interplay of *linearity* and *orthogonality.*

As a central result of chapter 4 we present:

Let $\mathfrak{S}$ be a d-semigroup. Then the set of p-ideals of $\mathfrak{S}$, the set of filters of $\mathfrak{S}$, and the set of d-ideals of $\mathfrak{S}$, respectively, form completely distributive lattice semigroups *under the complex operations developed from multiplication, meet, and join. Moreover the lattices of filters and d-ideals, respectively, satisfy the infinite law of distributivity:*

$$A \cap \sum B_i = \sum (A \cap B_i) \ \ (i \in I)\,.$$

Apart from the ideals above, w. r. t. *completion* there are two further types of central importance:

(1) the set of *v-ideals* $\mathfrak{a}$, defined by $(c \in \mathfrak{a} \iff s \mid x\mathfrak{a}y \Rightarrow s \mid ct\,)$

and dually

(2) the set of *u-ideals* $\mathcal{A}$, defined by $(c \in \mathcal{A} \iff x\mathcal{A}y \mid s \Rightarrow ct \mid s\,)$.

Chapter 5 presents a first structural investigation. In particular it turns out:

1. *Congruences are extended in a canonical manner* *from* $\mathfrak{P}$ *to* $\mathfrak{S}$ by:

$$\begin{aligned} a \;\equiv\; b \;\; :\Longleftrightarrow \;\; & \exists\, x, y \in S \;\&\; a_\circ \;\equiv\; b_\circ \in P : \\ & a = x a_\circ y \;\&\; b = x b_\circ y \,, \end{aligned}$$

from $\mathfrak{S}$ *to* $\mathfrak{S}^1$ by:

$$\alpha \equiv_1 \beta \;\; :\Longleftrightarrow \;\; \forall\, x, y \in S : \;\; x \cdot \alpha \cdot y \;\equiv\; x \cdot \beta \cdot y \,,$$

from $\mathfrak{S}$ *to* $\mathfrak{Q}$ by:

$$\alpha \equiv_Q \beta \;\; :\Longleftrightarrow \;\; \exists\, x, y \in C^{1+} \;\; x \cdot \alpha \cdot y \equiv_1 x \cdot \beta \cdot y \,,$$

and in each of these cases subdirect decompositions are respected.

2. *Let I be a lattice ideal of $\mathfrak{S}$, closed under multiplication.*

$$a \equiv b \; (I) \;\; :\Longleftrightarrow \;\; \exists\, e, f \in I : \;\; a \leq be \;\&\; b \leq af$$

generates a left congruence on $\mathfrak{S}$.

3. *Let $\mathfrak{m}$ be a d-ideal of $\mathfrak{S}$. Then*

$$a \equiv b \; (\mathfrak{m}) \;\; :\Longleftrightarrow \;\; \exists\, x \in F \; : \; a \wedge x = b \wedge x$$

generates a congruence on $\mathfrak{S}$.

4. *Let P an* irreducible ideal. *Then*

$$a \equiv b \; (P) \;\; :\Longleftrightarrow \;\; \forall\, s : s \cdot a \in P \Leftrightarrow s \cdot b \in P$$

generates a totally ordered left congruence on $\mathfrak{S}$.

5. *Let C be a c-ideal. Then*

$$a \equiv b \; (C) \;\; :\Longleftrightarrow \;\; \exists\, e, f \in C : a \leq be \;\&\; b \leq af$$

generates a left congruence on $\mathfrak{S}$, and in case of $a \cdot C = C \cdot a$ the left congruences above are transformed to (left/right) congruences.

6. *Let $u \in S$ be* idempotent. *Then*

$$\begin{aligned} & a \;\sigma_u\; b \;\; :\Longleftrightarrow \;\; \exists\, su : a \wedge su = b \wedge su \\ \textit{and} \qquad & a \;\pi_u\; b \;\; :\Longleftrightarrow \;\; au = bu \end{aligned}$$

generate a pair of congruences such that the pair S/σ_u , S/π_u generates a subdirect decomposition *of* $\mathfrak{S}$.

Two positive elements a, b of a d-semigroup are called *archimedean equivalent*, symbolized by $a \approx b$, if there $a \leq b^n$ & $b \leq a^n$ for some suitable $n \in \mathbf{N}$.

7. *Let $\mathfrak{S}$ be a d-semigroup. Then $\approx$ generates the* finest idempotent congruence *η on $\mathfrak{S}$ whence S/η is the* coarsest idempotent homomorphic image *of $\mathfrak{S}$.*

8. *The finest* cancellative congruence *of a d-semigroup is given by*

$$a\, \kappa\, b \;:\Longleftrightarrow\; \exists\, x \in S : xax = xbx\,.$$

9. *Let $\mathfrak{S}$ be a completely distributive lattice semigroup and let $\mathfrak{S}/\theta$ be subdirectly irreducible. Then θ is generated by a* regular filter, that is a filter, maximal w. r. t. not containing – shortly avoiding – some fixed element a.

10. *Let finally $\mathfrak{S}$ be even a positive subdirectly irreducible completely distributive lattice semigroup. Then $\mathfrak{S}$ has a maximum 0 and a uniquely determined hyper-atom (co-atom) h which forms together with 0 a critical pair.*

As a consequence of the preceding theorem it follows:

Any d-semigroup admits an embedding in a normal d-monoid.

In the particular case of a commutative d-semigroup we even get:

Any commutative subdirectly irreducible d-semigroup $\mathfrak{S}$ is totally ordered and 0-cancellative.

In general we obtain as a characteristic condition:

A subdirectly irreducible d-semigroup $\mathfrak{S}$ is totally ordered iff it satisfies: (O) $\quad \mathbf{xay \wedge ubv \leq xby \vee uav}$.

Chapter 6 introduces r-semigroups and presents an analysis of arbitrary d-semigroups based on the notions of l- and c-ideals.

1. 2. 1 Definition. Let $\mathcal{T} := (T, \leq)$ be a *totally ordered set*, briefly: *a chain*. By an *order ideal* of $\mathcal{T}$ we mean any subset of T satisfying $x \leq y \in A \Longrightarrow x \in A$. Dually the *order filter* is defined.

Moreover we call *ideal/filter isomorphism* of $\mathcal{T}$ each *order isomorphism* $\phi : A \longrightarrow B$ of some ideal A to some filter B.

Let ϕ, ψ be ideal/filter order isomorphisms of $\mathcal{T}$. Then the *relation product* $\phi \circ \psi$ and their *pointwise minimum function* $\phi \wedge \psi$, as well, form an ideal/filter order isomorphism of $\mathcal{T}$, and it is easily verified that this structure satisfies the axioms (A1), (A2), (A3). Further it is easily seen, that $\phi \leq \psi$ holds iff the implication $x \in \operatorname{dom}(\phi) \cap \operatorname{dom}(\psi) \Longrightarrow \phi(x) \leq \psi(x)$ is valid.

1. 2. 2 Definition. Let $\mathcal{T}$ be a chain. Then by the *ideal/filter semigroup,* briefly: the *r-semigroup* [1] $\mathfrak{R}(\mathcal{T})$, we mean the set of all ideal/filter isomorphisms of $\mathcal{T}$, considered w. r. t. $\circ$ and $\wedge$.

Main result of chapter 5 is a refined study of the interplay between d-semigroups and r-semigroups culminating in the theorems:

Any d-semigroup admits a subdirect decomposition whose factors admit an embedding in some r-semigroup.

Any r-semigroup admits an embedding in a d-semigroup,

BUT:

Not any r-semigroup is necessarily a d-semigroup.

A Hint: Consider the r-semigroup of $\mathbf{Q}$. Here 0 and π generate isomorphic filters of strictly greater elements but the corresponding ideals are not isomorphic.

The method of proof of the preceding results implicitly provides moreover:

Any commutative d-semigroup admits an embedding in the quotient-d-semigroup of some direct product of bricks.

Chapter 7 A lattice is called *conditionally complete*, if there are no *gaps,* meaning that any *upper bounded subset* is *upper limited.* A conditionally complete lattice is called $\bigwedge$-*distributive*, if it satisfies:

(D$\vee$) $$s = \bigwedge a_i \ (i \in I) \implies x \vee s = \bigwedge (x \vee a_i) \ (i \in I).$$

[1] r- here stands for the German Rand.

Dually the $\bigvee$-*distributive* lattice is defined by the corresponding axiom (D$\wedge$). A conditionally complete lattice is called *absolutely distributive* if existing limits satisfy:

$$\text{(DV1)} \qquad \bigwedge_C \Big[\bigvee_{A_\gamma} a_{\gamma,\alpha} \Big] = \bigvee_\Phi \Big[\bigwedge_C a_{\gamma,\phi(\gamma)} \Big]$$

$$\text{(DV2)} \qquad \bigvee_C \Big[\bigwedge_{A_\gamma} a_{\gamma,\alpha} \Big] = \bigwedge_\Phi \Big[\bigvee_C a_{\gamma,\phi(\gamma)} \Big] \,,$$

where γ runs through C and Φ runs through the set of all mappings ϕ of C into the union of those A_γ, which satisfy $\phi(\gamma) \in A_\gamma$.

Obviously any conditionally complete chain is absolutely distributive, and thereby in particular also $\bigvee$- and $\bigwedge$-distributive. On the other hand (D$\wedge$) and (D$\vee$) are independent.

A conditionally complete d-semigroup is called complete if its multiplication distributes over $\bigwedge$. It is called *continuous* if its multiplication distributes over $\bigwedge$ and $\bigvee$. A d-semigroup is called *archimedean,* if it satisfies:

$$\text{(A)} \qquad a^n \leq b \ \ (\forall\, n \in \mathbf{N}) \implies ab\,,\ ba \leq b\,.$$

As a first principal result this chapter presents:

It suffices to check the cone w. r. t. the various completeness-conditions.

As further principal results chapter 6 contains:

Any complete d-semigroup is archimedean.

Any continuous d-semigroup is commutative.

Chapter 8 presents – based on chapter 6:

Any archimedean d-semigroup is commutative !

Chapter 9 considers totally ordered d-semigroups. In a first section we are concerned with *strictly archimedean* models, these are d-semigroups, satisfying $\forall a > 1,\, b\ \exists n \in \mathbf{N} :\ \ a^n \geq b$. Strictly archimedean d-semigroups are always *totally ordered*. Moreover it holds:

The Theorem of Hölder and Clifford. *Any strictly archimedean d-semigroup* $\mathfrak{S}$ *admits an* order preserving embedding

(i) *into the semigroup of all non negative reals w. r. t. the natural order, henceforth denoted by* $\mathfrak{P}$,

OR (ii) *into the semigroup of all reals of the interval* $[0,1]$ *w. r. t. the usual order and* $ab := \min(a+b, 1)$, *henceforth denoted by* $\mathfrak{P}_1$, *also* $\mathfrak{E}$,

OR (iii) *into the semigroup of all reals of the interval* $[0,1]$, *extended by the symbol* ∞ *and considered under* $ab := a+b$, *if* $a+b \leq 1$, *and* $ab := \infty$, *if* $a+b > 1$, *henceforth denoted by* $\mathfrak{P}_1{}^\circ$.

In a second section totally ordered positive complete d-semigroups ar investigated by means of *interval semigroups*, these are *topological semigroups* defined on a set, endowed with a complete and dense total order and with a semigroup operation such that the *order minimum* acts as semigroup identity and the *order maximum* as zero.

Chapter 10 is again concerned with some particular archimedean property. A d-semigroup is called *hyper-archimedean*, if it satisfies:

$$\forall a, t \in S^+ \, \exists n \in \mathbf{N} : \;\; t \cdot a \cdot t \leq a \vee t^n .$$

Obviously any hyper-archimedean d-semigroup is also archimedean.

Theorem. *The following are pairwise equivalent:*

(i) $\mathfrak{S}$ *is hyper-archimedean.*

(ii) $\forall a, t \in S \, \exists n \in \mathbf{N} : t \cdot a \cdot t \leq a \vee t^n$.

(iii) *Any homomorphic image of* $\mathfrak{S}$ *is archimedean.*

(iv) *The semigroup of lattice ideals is archimedean.*

Moreover Chapter 10 provides an abundance of theorems, among them also some results on *factorial* d-semigroups, these are d-semigroups whose elements are products of *semiprime elements* $(|\,p\,| = |\,a\,||\,b\,| \Longrightarrow |\,p\,| = |\,a\,| \vee |\,p\,| = |\,b\,|)$. Factorial d-semigroups are exactly those d-semigroups, whose ideal semigroup satisfies:

$$A \cdot \bigcap B_i \;=\; \bigcap AB_i \;\; (i \in I) .$$

Chapter 11 considers *complete extensions.*

The central problem: Under which conditions does a d-semigroup admit a *complete extension,* i. e. an extension, satisfying:

$$x \cdot (\bigwedge a_i) \cdot y = \bigwedge (x a_i y) \;\; (i \in I) ,$$

see above, or dually: Under which conditions does a d-semigroup admit some $\bigvee$-*complete extension,* that is an extension, satisfying: $x \cdot (\bigvee a_i) \cdot y = \bigvee(xa_iy)$ $(i \in I)$. In both cases the archimedean property is necessary. But opposite to the classical situation, this property is not sufficient here.

A most important role is played by the pair *v-ideal, u-ideal.* The power of these ideals is that for cancellative d-semigroups they provide cancellative extensions. Observe: The v-ideal semigroup $\mathfrak{V}$ provides a complete extension whenever $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \,|\, \mathfrak{b}$, and the u-ideal semigroup $\mathfrak{T}$ provides a $\bigvee$-complete extension whenever $\mathcal{A} \subseteq \mathcal{B} \Longrightarrow \mathcal{A} \,|\, \mathcal{B}$.

Main results of Chapter 11 are:

1. *Define* $[A] := \{x \,|\, x \,|\, A\}$. $\mathfrak{S}$ *admits a complete extension by* cuts *if and only if its v-ideals satisfy:*

$$\text{(SS)} \qquad [\,\mathfrak{a}\,]^n \subseteq [\,\mathfrak{b}\,] \; (\forall\, n \in \mathbf{N}) \implies \mathfrak{a} \circ \mathfrak{b} = \mathfrak{b} = \mathfrak{b} \circ \mathfrak{a}\,,$$

and in this case any complete cut extension is isomorphic with the v-ideal semigroup.

2. $\mathfrak{S}$ *admits an* $\bigvee$*-complete extension by* cuts *if and only its u-ideals satisfy:*

$$\text{(VS)} \qquad \mathfrak{S} \text{ is archimedean and satisfies } \mathfrak{A} = [\,(\mathfrak{A})\,]\,,$$

and in this case any $\bigvee$*-complete cut extension is isomorphic with the u-ideal semigroup.*

Chapter 12 provides some insight into *cube semigroups.*

According to our definition above ${\mathfrak{P}_1}^I$ is the $|I|$-dimensional cube, considered under the *derived function operations.* We are interested in sub-d-semigroups of ${\mathfrak{P}_1}^I$, henceforth called *cube semigroups.*

1. *A positive d-monoid* $\mathfrak{S}$ *is a cube semigroup iff it satisfies:*

$$\text{(W)} \qquad \text{If } A \text{ is a filter, satisfying } A^n \supseteq \mathsf{b} \;\; (\forall n \in \mathbf{N})\,,$$
$$\text{then the } v\text{-ideal } \mathfrak{a} \text{ generated by } A \text{ satisfies: } \mathfrak{a} \cdot \mathsf{b} = \mathsf{b} = \mathsf{b} \cdot \mathfrak{a}\,.$$

2. *A d-monoid admits a complete extension if its cone admits an embedding into some cube* $\mathfrak{E}^I$.

3. *A positive complete d-monoid* $\mathfrak{S}$ *admits an* infima preserving *embedding into a cube if for any pair* a, b *with* $b \not\leq a$ *there exists a* $\vee$*-irreducible element* p *such that* $p \leq b$ & $p \not\leq a$.

4. *A positive d-monoid $\mathfrak{S}$ admits a lattice point extension iff the lattice semigroup of d-ideals of $\mathfrak{S}$ is archimedean.*

Chapter 13 and Chapter 14 *are closely related to the theory of* chains *and* polars *in ℓ-groups. Let us consider the most classical ℓ-group $\mathfrak{Q} := (\mathbf{Q}^+, \cdot, |_N)$ with $a\,|_N b \Longleftrightarrow a \cdot n = b \ \ (n \in \mathbf{N})$. As is easily seen factorization aspects in $\mathfrak{Q}^+$ are reflected by comparability and orthogonality. For example, we see that the classical prime factorization theorem reads $\mathfrak{Q}^+$ is a direct sum of components of type $\mathfrak{Z}$.*

Essential notions which may carry over to the arbitrary d-monoid situation are for instance direct factor, polar, minimal substructure etc.

It is the merit of ℓ-group pioneers like F. Šik, J. Jakubík, P. F. Conrad, S. J. Bernau *and* J. T. Lloyd *to have studied these substructures in order to clear the structure of arbitrary ℓ-groups.*

Thus, from the conceptual point of view, they contributed to d-semigroup theory, far before this structure was created by the author.

Since: Most surprisingly, large parts of the lecture note due to Bigard-Keimel-Wolfenstein, [10], remain valid in right normal d-semigroups, from the substantial point of view as well as from the methodical point of view.

This is the more important since any d-semigroup admits an embedding into some normal d-monoid.

Chapter 15 is concerned with representable d-semigroups. Although there is an abundance of characterizing properties for representable ℓ-groups, all of them except for condition (vi) below fail in the d-semigroup case. Nevertheless we find some nice descriptions for the general case, see for instance:

For a d-semigroup the following are pairwise equivalent:

- (i) $\mathfrak{S}$ *is representable.*
- (ii) $xay \wedge ubv \leq xby \vee uav$.
- (iii) $\mathfrak{S}^+$ *is representable.*
- (iv) Σ^+ *is representable.*
- (v) $ax \wedge yb \leq ay \vee xb$.
- (vi) $eae \wedge faf = (e \wedge f)a(e \wedge f)$.

Considering special cases we are led to *hyper-normal* d-monoids which are defined by

$$\begin{aligned} x, y \in S^+ \ \&\ ax \wedge ay = a \ &\Longrightarrow\ \exists\, z \perp x : ay = az \\ x, y \in S^+ \ \&\ xa \wedge ya = a \ &\Longrightarrow\ \exists\, z \perp x : ya = za\,. \end{aligned}$$

Obviously this class contains the class of cancellative d-monoids and the class of boolean algebras,as well. But moreover the ideal theory of commutative *arithmetical rings*, that is rings whose ideal lattice is distributive, and thereby in particular that of Bézout rings, that is commutative rings whose finitely generated are principal, is reflected.

Chapter 16 A semigroup is called *separative*, if it satisfies:

$$(ab = aa \ \&\ ba = bb) \vee (ab = bb \ \&\ ba = aa) \text{ implies } a = b\,.$$

Any d-semigroup contains a natural *separative kernel* which is a product $\mathfrak{E} \cdot \mathfrak{C}$ of the *idempotent* and the *cancellative kernel.* Its study provides a most general approach to clearing the structure of inverse d-semigroups, culminating in a theorem of McAlister.

Moreover, let $\mathfrak{S}$ be a d-semigroup. Then we obtain:

1. $\mathfrak{S}$ *is separative if and only if it is a subdirect product of cancellative d-semigroups with or without zero element* 0, so

2. $\mathfrak{S}$ *is separative, if and only if it admits an embedding into an inverse d-semigroup.*

3. *If* $\mathfrak{S}$ *is a subdirect product of an* ℓ*-group* $\mathfrak{G}$ *and a d-lattice* $\mathfrak{L}$*, then this subdirect product is even a direct product.*

Chapter 17

A semigroup is called *inverse*, if there exists for any element a a uniquely determined element a^{-1} satisfying

(1.26) $$a \cdot a^{-1} \cdot a = a \qquad \text{and} \qquad a^{-1} \cdot a \cdot a^{-1} = a^{-1}\,.$$

Hence the inverse semigroup is a common abstraction of *group* and *semilattice.*

A d-semigroup $\mathfrak{S}$ is called inverse, if $(S, \cdot)$ is inverse. Consequently the inverse d-semigroup is a common abstraction of ℓ-group and d-lattice

How powerful the inverse property is, will be demonstrated aside from the structure theorem below by showing that in the inverse case it suffices to require (A3) only one sided.

Let $\mathfrak{S}$ be an inverse d-monoid. Then any $G_u := \{x \mid xx^{-1} = u\}$ is equal to the set of all uc with $u \wedge (1 \vee c)(1 \wedge c)^{-1} = 1$ and $cc^{-1} = 1$, whence any inverse d-semigroup turns out to be a semilattice of ℓ-groups $\mathfrak{G}_u$ with $u \leq v \Longrightarrow (\mathfrak{G}_u)v = \mathfrak{G}_v$.

According to McAlister (and Clifford) any inverse d-semigroup is generated in a canonical manner. To this end one starts from a distributive lattice $\mathfrak{D}$ and a system $\mathfrak{G}_\alpha$ $(\alpha \in D)$ of ℓ-groups together with two directed systems of homomorphisms

$$\phi_{\alpha,\alpha\vee\beta} : \mathfrak{G}_\alpha \longrightarrow \mathfrak{G}_{\alpha\vee\beta} \quad \text{and} \qquad \psi_{\alpha,\alpha\wedge\beta} : \mathfrak{G}_\alpha \longrightarrow \mathfrak{G}_{\alpha\wedge\beta}\,.$$

Finally in

Chapter 18 various types of d-semigroup generalizations are considered and discussed, maybe initiating further investigations of lattice ordered semigroups – in future..

Chapter 2

Arithmetics

2.1 Fundamental arithmetic of d-semigroups

2. 1. 1 Definition. By a *d-semigroup* we mean an *algebra* $(S, \cdot, \wedge)$ *of type* (2,2), satisfying:

(A1) $$(S, \cdot) \text{ is a } \textit{semigroup}\,.$$

(A2) $$(S, \wedge) \text{ is a } \textit{semilattice}\,.$$

(A3) $$\forall\, x, a, b, y : \quad x(a \wedge b)y \;=\; xay \wedge xby\,.$$

(A4) $$a \leq b \Longrightarrow \exists\, x, y : \; ax \;=\; b \;=\; ya\,.$$

As usual $\mathfrak{S}$ is called *linearly ordered* if $(S, \wedge)$ is *totally ordered* (and consequently satisfying in addition $a \leq b \Longrightarrow xa \leq xb \;\&\; ay \leq by)$.

Obviously, the d-semigroup is a common abstraction of the *lattice group*, require that $(S, \cdot)$ be a *group*, and of the *distributive lattice*, require that $(S, \cdot)$ be a *semilattice*.

2. 1. 2 Definition. Let $(S, \cdot)$ be a *monoid* and $\mathfrak{S}$ a d-semigroup. Then $\mathfrak{S}$ is called a d-monoid. A d-monoid is called *right normal*, if in addition to $(A1)$ through $(A4)$ also

$$\forall\; a, b \;\exists\; a^\circ \wedge b^\circ = 1 : \;\; (a \wedge b)a^\circ = a \;\&\; (a \wedge b)b^\circ = b$$

is satisfied. In case that $\mathfrak{S}$ is right and left normal $\mathfrak{S}$ is called briefly *normal.*

Normality will play no role in this chapter, but later we will see, that any d-semigroup admits an embedding into a normal d-monoid.

2. 1. 3 Definition. Let $\mathfrak{S}$ be a d-monoid with zero element 0. $\mathfrak{S}$ is called *right hyper-normal*, if it satisfies

$$au = a \Longrightarrow \exists\, v \in S : \;\; u \wedge v = 1 \;\&\; av = 0\,.$$

Let $\mathfrak{S}$ be right and *left hyper-normal.* Then $\mathfrak{S}$ will be called *hyper-normal.*

Later we will see, that any commutative d-semigroup admits a hyper-normal d-monoid-extension.

Commutative hyper-normal d-monoids are first all the monoids of *finitely generated ideals* of *arithmetical rings*, in particular *principal ideal semigroups* of BÉZOUT-*rings.* Classical hyper-normal d-monoids with 0 are on the one hand the *boolean lattice*, considered under $\vee$ and $\wedge$, and on the other hand the lattice group (with 0), considered under $\cdot$ and $\wedge$.

Like normal also hyper-normal d-semigroups are not studied in this chapter, but merely mentioned, because of the central role they will play later on.

Let henceforth $\mathfrak{S}$ mean some d-semigroup. Then, as first elementary but fundamental arithmetical rules we get:

$$a \leq b \;\&\; ea = a \;\Longrightarrow\; eb = b\,. \tag{2.5}$$

PROOF.

$$\begin{aligned} a \leq b \;\&\; ea = a \;&\Longrightarrow\; au = b\,(\exists u)\\ \&\qquad ea = a \;&\Longrightarrow\; eb = eau = au = b\,. \end{aligned}$$

□

Recall that d-semigroups are defined *right/left dually.* This means that all *left rules* have a *dual right version,* and *vice versa*.

$$x(a \wedge b) \;=\; xa \wedge xb\,. \tag{2.6}$$

$$a \leq b \;\Longrightarrow\; xa \leq xb\,. \tag{2.7}$$

PROOF. $a \leq b \Longrightarrow a = a \wedge b \Longrightarrow xa = xa \wedge xb\,.$ □

Our first aim is a proof that $(S, \leq)$ is not only *inf-closed* but also *sup-closed.* To this end we give

2. 1. 4 Definition. $a \in S$ is called *right positive* if $\forall x : xa \geq x.$

An element $a \in S$ is called *positive*, if it is right and left positive that is if it satisfies: $\forall x : ax, xa \geq x.$ Furthermore the set P of all positive elements is called the *cone* of $\mathfrak{S}$.

2. 1. 5 Lemma. *Suppose* $ea = a \;\&\; (e \wedge a)a' = a$. *Then* ea' *satisfies* $xea' \geq x \;\; (\forall x)$, *that is* ea' *is right positive.*

PROOF. Assume $(e \wedge x)f = e \wedge x$ and $(f \wedge a)a^* = a$. Then it follows $e(f \wedge a)a^* = (e \wedge a)a^* = (e \wedge a)a' = a$ and thereby $xea' = xea^* = xefa^* = xfa^* \geq xf = x$. □

2. 1. 6 Lemma. *Suppose* $a \leq b$. *Then there even exists a right positive factor* y *with* $ay = b$.

PROOF. Assume $ax = b \;\&\; ae = a \;\&\; (e \wedge x)x' = x$. Then $b = ax = a(e \wedge x)x' = aex' \wedge axx' = ax' \wedge bx' = ax' = a(ex')$ where $ex' =: y$ is right positive by 2.1.5 □

Now we are in the position to prove that $(S, \leq)$ is not only *inf-closed* but also *sup-closed*.

2. 1. 7 Proposition. *The semilattice* $(S, \leq)$ *is sup-closed, i. e.* $(S, \leq)$ *is a lattice. More precisely* $R(a, b, a', b') \Longrightarrow a{\cdot}b' = a{\vee}b$, *that is* $R(a, b, a', b') \Longrightarrow a \cdot b' = \sup(a, b)$.

PROOF. As seen above, it holds $a \cdot b' \geq a, b$. Suppose now that $a, b \leq c$ and $a \cdot c' = c$. By the preceding lemma we may assume that a', b', c' are right positive. But then $(a \wedge b)b' = (a \wedge b)(b' \wedge c') = b$ and thereby to $ab = ab' \wedge ac'$, that is $ab' \leq ac' = c$. □

Clearly, by 2.8 in case $R(a, b, a', b')$ and $L(b'', d'', b, d)$ it holds:

$$a''b''(a \wedge b) = a''(a \wedge b)b' = (a \wedge b)a'b' = \sup(a, b) =: a \vee b \,. \tag{2.8}$$

Furthermore we get immediately

$$ax \wedge ay = a \;\Longrightarrow\; axy = ayx \,, \tag{2.9}$$

leading to

$$\begin{array}{ccc} (a \wedge b)a = a & \& & (a \wedge b)b = b \\ & \Longrightarrow & \\ ab & = & ba \,. \end{array} \tag{2.10}$$

Based on 2.8 it results next

$$xa \vee xb = (xa \wedge xb)a'b' = x(a \wedge b)a'b' = x(a \vee b) \,, \tag{2.11}$$

leading by duality to

$$x(a \vee b)y \;=\; xay \vee xby\,. \tag{2.12}$$

Now we are ready to prove:

$$a \vee (b \wedge c) \;=\; (a \vee b) \wedge (a \vee c)\,. \tag{2.13}$$

PROOF. It suffices – as is well known – to show $a \vee (b \wedge c) \geq (a \vee b) \wedge (a \vee c)$. To this end we start from $R(a, b \wedge c, a', s')$. Then it follows:

$$\begin{aligned} a \vee (b \wedge c) &= (a \wedge b \wedge c)s'a' \\ &= (b \wedge c)a' \\ &= ba' \wedge ca'\,. \end{aligned}$$

Moreover, by 2.8 it holds $(b \wedge c)a' = a \vee (b \wedge c) \geq b \wedge c$, which by (2.7) provides $ba' \geq b$ on the one hand and $ca' \geq c$ on the other hand. Hence we get altogether

$$\begin{array}{rcl} ba' \geq a \vee b & \& & ca' \geq a \vee c \\ & \rightsquigarrow & \\ a \vee (b \wedge c) & \geq & (a \vee b) \wedge (a \vee c)\,. \end{array}$$

□

Therefore, d-semigroups are always $\wedge$-, $\vee$- and *lattice distributive*. Lattice ordered semigroups, satisfying these identities were called *dld-semigroups* by Repnitzkii. We define alternately

2. 1. 8 Definition. Let $\mathfrak{S} = (S, \cdot, \wedge, \vee)$ be an algebra of type (2,2,2). Then we call $\mathfrak{S}$ a *completely distributive lattice semigroup*, briefly a *cdl-semigroup,* if $\mathfrak{S}$ satisfies (A3), (2.12), and (2.13) .

2. 1. 9 Proposition. *Any d-semigroup is a cdl-semigroup.*

2.2 The Cone

A d-semigroup need not have an *identity element* 1 . But – in any d-semigroup each element has at least one *private unit.* .

2. 2. 1 Proposition. *For any $a \in S$ there exists at least one element e_a satisfying $ae_a = a = e_a a$.*

PROOF. Suppose $af = a$ and $e(a \wedge f) = a \wedge f$. It follows next $ea = a$ and $ef = f$, leading to:

$$ae \leq ae \vee a = (ae \vee a)f \;=\; aef \vee af = a \vee a = a\,.$$

Hence – by duality – we may start from some pair u, v with

$$\begin{array}{lcl} ua = a & \& & au \leq a \\ va \leq a & \& & av = a\,, \end{array}$$

which implies $$(u \vee v)a = \; a \; = a(u \vee v)\,.$$

This completes the proof. □

We need some further lemmata.

2. 2. 2 Lemma. $ab = cd \Longrightarrow (a \wedge c)(b \vee d) = ab = (a \vee c)(b \wedge d)$.

PROOF. It holds

$$ab \leq a(b \vee d) \wedge c(b \vee d) \quad \& \quad ab \geq (a \wedge c)b \vee (a \wedge c)d\,.$$ □

2. 2. 3 Corollary. $ua = a = au \Longrightarrow a = (u \wedge a)(u \vee a) = (u \vee a)(u \wedge a)$.

2. 2. 4 Corollary. $ae = ea = a = af = fa \Longrightarrow e \vee a = f \vee a =: a^+$.

PROOF. Suppose $u(e \wedge f) = e \wedge f$. Then it follows

$$a = (e \wedge a)(e \vee a) = (ue \wedge a)(e \vee a) = (u \wedge a)(e \vee a)$$

and by analogy we get $a = (u \wedge a)(f \vee a)$. Hence the assertion follows by left multiplication. □

Recall: $a \in S$ is said to be *positive*, if it satisfies $\forall\, x :\; ax \geq x \;\&\; xa \geq x$.

2. 2. 5 Lemma. *$a \in S$ is positive iff there exists at least one element e, satisfying $a = ae = ea = e \vee a =: a^+$. In particular $ae = a = ea$ implies that $e \vee a$ is positive.*

PROOF. Let a be positive. Then it results

$$a = ae = ea \Longrightarrow a = ea = e \vee ea = e \vee a\,.$$

On the other hand suppose $a = ae = ea = e \vee a$ and choose some $x \in S$ and a unit u of $a \wedge x$. Then from 2.2.4 we get first $e \vee a = u \vee a$ and thereby furthermore

$$ax = (e \vee a)x = (u \vee a)x = ux \vee ax = x \vee ax \geq x \,.$$

The rest follows by duality. □

2. 2. 6 Definition. Let $\mathfrak{S}$ be a d-semigroup. We call *positive cone* of $\mathfrak{S}$ the set S^+ of all positive elements of $\mathfrak{S}$. Obviously S^+ is closed under $\cdot$ and $\wedge$. Hence it makes sense to speak of the algebra $\mathfrak{S}^+$. Henceforth this algebra will be called the (*positive*) *cone* of $\mathfrak{S}$.

Observe: We separate the cone of S and the cone of $\mathfrak{S}$. Whenever $\mathfrak{S}$ is uniquely determined we shall also speak of $\mathfrak{P}$ instead of $\mathfrak{S}^+$.

2. 2. 7 Proposition. *The cone of any d-semigroup $\mathfrak{S}$ is a sub-d-semigroup of $\mathfrak{S}$.*

PROOF. On the grounds of duality it suffices to verify the implication (A4') $a \leq b \implies \exists\, x \in P : \; ax = b$ which sharpens 2.1.6.

To this end suppose $as = b$ and $(a \wedge s)e = (a \wedge s)$. This implies $a(e \vee s) = a \vee as = b$ with $e \vee s \in P$. □

2.3 A Decomposition Formula

We now turn to some rules, valid in the cone, which will later on be of importance, again and again. For the sake of convenience we tacitly suppose that for elements a, b, c, d the relations $R(a, c, a', c')$ and $L(b'', d'', b, d)$ are realized by positive elements a', b'', c', d''. Then calculating in $\mathfrak{P}$ we get

$$a \wedge b \cdot c = a \wedge (a \wedge b) \cdot c \tag{2.14}$$

$$a \wedge b \cdot c \leq (a \wedge b)(a \wedge c)\,, \tag{2.15}$$

$$xay = xby \leq xcy, xdy \implies xay = xby \leq x(c \wedge d)y\,. \tag{2.16}$$

and (2.15) leads to the central *decomposition formula*

$$ab \wedge cd = (a \wedge c)(a' \wedge d'')(b'' \wedge c')(b \wedge d) \tag{2.17}$$

$$= (a \wedge c)(b'' \wedge c')(a' \wedge d'')(b \wedge d)\,. \tag{2.18}$$

PROOF. By assumption and (2.15) according to (2.9) and

$$(\star)\quad xay = xby \leq xcy \Longrightarrow x(a \wedge b)y \leq xcy$$

we obtain

$$\begin{aligned} ab \wedge cd &= (a \wedge c)(a'b'' \wedge c'd'')(b \wedge d) \\ &\overset{(2.15)}{\leq} (a \wedge c)(b'' \wedge c')(a' \wedge d'')(b \wedge d) \\ &\overset{(2.9)}{=} (a \wedge c)(a' \wedge d'')(b'' \wedge c')(b \wedge d) \\ &\overset{(\star)}{\leq} (a \wedge c)(a'b'' \wedge c'd'')(b \wedge d) \\ &= ab \wedge cd\,. \end{aligned}$$

Thus we are through. □

Observe next that positive elements d satisfy:

$$\begin{aligned} a \wedge c \cdot d &= (a \wedge c) \cdot (a' \wedge d) \\ &= a \wedge (a \wedge c) \cdot d\,, \end{aligned} \tag{2.19}$$

a formula which is easily calculated from the right to the left.

2. 3. 1 Lemma. *Let x, y, a belong to P and let $x \leq y$ and $(a \wedge y)y' = y$ be satisfied with $y' \in P$. Then there exists an element $x^* \leq y'$ with $(a \wedge x)x^* = x$.*

PROOF.

$$\begin{aligned} (x \wedge a)x' = x \quad &\& \quad x = x \wedge (y \wedge a)y' \\ &\Longrightarrow \\ x &= x \wedge (x \wedge y \wedge a)y' \\ &= x \wedge (x \wedge a)y' \\ &= (x \wedge a)x' \wedge (x \wedge a)y' \ \ (\exists\, x') \\ &= (x \wedge a)(x' \wedge y')\,. \end{aligned}$$

□

2. 3. 2 Lemma. *Any d-semigroup satisfies:*

$$ax \wedge by \;\leq\; ay \vee bx\,.$$

PROOF.

$$\begin{aligned} &(ax \wedge by) \wedge (ay \vee bx) \\ =\;& (ax \wedge by \wedge ay) \vee (ax \wedge by \wedge bx) \\ =\;& (ax \wedge (b \wedge a)y) \vee ((a \wedge b)x \wedge by) \\ =\;& ax \wedge (ax \vee by) \wedge (a \wedge b)(x \vee y) \wedge by \\ =\;& ax \wedge (ax \vee by) \wedge a(x \vee y) \wedge b(x \vee y) \wedge by \\ =\;& ax \wedge by\,. \end{aligned}$$

□

2.4 Commutativity

We start with

2. 4. 1 Proposition. *Let $ab = ba$. Then a, b satisfy the binomial formulas:*

$$(a \wedge b)^n = a^n \wedge b^n . \tag{2.20}$$

$$(a \vee b)^n = a^n \vee b^n . \tag{2.21}$$

PROOF. There is nothing to show for $n = 1$. Therefore suppose that (2.20) is already proven for all m with $1 \leq m \leq n$. This implies for k with $1 \leq 2k \leq n+1$:

$$\begin{aligned} a^{n+1} \wedge b^{n+1} &\leq (a \vee b)^k \cdot (a^{n+1-k} \wedge b^{n+1-k}) \\ &= (a \vee b)^k \cdot (a \wedge b)^{n+1-k} \quad (2k \leq n+1) \\ &= (ab)^k \cdot (a \wedge b)^{n+1-2k} \\ &= (ab)^k \cdot (a^{n+1-2k} \wedge b^{n+1-2k}) \\ &= a^{n+1-k} b^k \wedge a^k b^{n+1-k} . \end{aligned}$$

The rest follows by duality. □

2. 4. 2 Lemma. *A d-semigroup is already commutative, if any pair of comparable positive elements commutes.*

PROOF. Let a, b be positive and suppose that any pair of comparable positive elements commutes. Then in case of $R(a, b, a', b')$ with positive elements a', b' we get:

$$\begin{aligned} ab &= (a \wedge b)a'(a \wedge b)b' \\ &= (a \wedge b)^2 a'b' \\ &= (a \wedge b)^2 b'a' \\ &= ba . \end{aligned}$$

Next we show that $\mathfrak{S}$ is already commutative, if any pair of positive elements commutes. To this end let e be a positive unit of $a \wedge b$ and suppose that l, r are positive, satisfying

$$l(e \wedge a) = \quad e \quad = (e \wedge a)r .$$

Then $$le = l(e \wedge a)r = er = re$$

and thereby
$$\begin{aligned} e \vee b &= (e \vee b)l(e \wedge a) \\ &= l(e \vee b)(e \wedge a) \\ &= le(e \vee b)(e \wedge a) \\ &= re(e \vee b)(e \wedge a) \\ &= r(e \vee b)(e \wedge a)\,. \end{aligned}$$

Hence, multiplying with $(e \wedge a)$ from the left we get:

$$(e \wedge a)(e \vee b) = (e \vee b)(e \wedge a)\,. \tag{2.22}$$

Consequently it suffices to show:

$$(e \vee a)(e \wedge a)(e \wedge b) = (e \vee a)(e \wedge b)(e \wedge a)\,, \tag{2.23}$$

since in this case we obtain:

$$\begin{aligned} ab &\overset{2.2.3}{=} (e \vee a)(e \wedge a)(e \vee b)(e \wedge b) \\ &\overset{(2.22)}{=} (e \vee a)(e \vee b)(e \wedge a)(e \wedge b) \\ &\overset{(2.23)}{=} (e \vee b)(e \vee a)(e \wedge b)(e \wedge a) \\ &\overset{(2.22)}{=} (e \vee b)(e \wedge b)(e \vee a)(e \wedge a) \\ &= ba\,. \end{aligned}$$

To this end suppose $(e \wedge a)x = e$ and $(e \wedge b)y = e$ with positive and thereby commuting elements x, y, and suppose furthermore that f be a unit of $a \wedge b \wedge e \wedge x \wedge y$ and hence a common unit of a, b, e, x, y. In particular suppose that w. r. t. 2.2.5 it holds $x = f \vee x$ and $y = f \vee y$. Then it follows first:

$$(e \vee a)(e \wedge a)(e \wedge b)xy = (e \vee a)(e \wedge b)(e \wedge a)xy\,. \tag{2.24}$$

But by (2.22) the elements $x = f \vee x$ and $y = f \vee y$ commute with the elements $f \wedge a$ and $f \wedge b$. So we obtain:

$$\begin{aligned} &(e \vee a)(e \wedge a)(e \wedge b) \\ =\ &(e \vee a)(e \wedge a)(e \wedge b)e^2 \\ =\ &(e \vee a)(e \wedge a)(e \wedge b)(e \wedge a)(e \wedge b)xy \\ =\ &(e \vee a)(e \wedge a)(e \wedge b)e(f \wedge a)e(f \wedge b)xy \\ =\ &(e \vee a)(e \wedge a)(e \wedge b)(f \wedge a)(f \wedge b)xy \\ =\ &(e \vee a)(e \wedge a)(e \wedge b)xy(f \wedge a)(f \wedge b) \\ =\ &(e \vee a)(e \wedge b)(e \wedge a)xy(f \wedge a)(f \wedge b) \quad (2.24) \\ =\ &(e \vee a)(e \wedge b)(e \wedge a)(f \wedge a)(f \wedge b)xy \\ =\ &(e \vee a)(e \wedge b)(e \wedge a)e(f \wedge a)e(f \wedge b)xy \\ =\ &(e \vee a)(e \wedge b)(e \wedge a)e^2 \\ =\ &(e \vee a)(e \wedge b)(e \wedge a)\,. \end{aligned}$$

Thus the proof is complete. □

2.5 Absolute Values

Based on 2.2.4 in this section a function is exhibited that turned out as most fruitful in theory of ℓ-groups. First of all some remarks:

In the additive ℓ-group $\mathfrak{R}$ of the reals we put $\max(a, -a) =: |\,a\,|$. This definition carries over, of course, to arbitrary ℓ-groups *via* $|\,a\,| := a \vee a^{-1}$ and one easily verifies that also in the general case of a commutative ℓ-group the conditions of an *absolute value function* or a *measure function* are satisfied. More difficult it is, however, to show, that $|\,a\,| \cdot |\,b\,| = |\,ab\,|$ is satisfied only if the underlying ℓ-group is commutative.

Nevertheless, also in the general case strong rules remain valid, which contribute essentially to clearing structure problems, since in many cases such structure problems may be studied by restricting to the positive situation.

In many cases this is also possible by considering the cone, but one has to take into account, that the cone is not closed w. r. t. taking *inverses* which sometimes leads to new problems. So let 's come back to $|\quad|$. In any ℓ-group according to $(1 \wedge a)(a \vee a^{-1}) = (a \vee a^{-1}) \wedge (a^2 \vee 1) \geq 1 \wedge a$ it results firstly $a \vee a^{-1} \geq 1$ and according to $a \cdot a^{-1} = 1 \cdot 1$ by 2.2.2 we get $(1 \wedge a)(1 \vee a^{-1}) = 1$, that is $(1 \wedge a)^{-1} = 1 \vee a^{-1}$. This leads to

$$|\,a\,| = a \vee a^{-1} = 1 \vee a \vee a^{-1} \vee (1 \vee a)(1 \vee a^{-1}) = (1 \vee a)(1 \wedge a)^{-1}$$

that is

$$|\,a\,| = (1 \vee a)^{-1} \cdot a \cdot (1 \wedge a)^{-1}\,. \tag{2.25}$$

But this formula can be modulated for arbitrary d-semigroups, as will now be shown. To begin with we show first:

2. 5. 1 Lemma. *Let*

$$ea = ae = a = fa = af\,. \tag{2.26}$$

$$e''(e \wedge a) = e = (e \wedge a)e'\,. \tag{2.27}$$

$$f''(f \wedge a) = f = (f \wedge a)f'\,. \tag{2.28}$$

be satisfied with positive elements $e', e'', f' f''$. Then it results:

$$e''(e \vee a) = e'(e \vee a) = (e \vee a)e' = (e \vee a)e'' = (f \vee a)f' = (e \vee a)f'.$$

PROOF. By assumption we get:

$$(e \vee a)e'' = (e \vee a)e''e = (e \vee a)e''(e \wedge a)e' = (e \vee a)ee' = (e \vee a)e'$$

which leads to:

$$\begin{aligned} (e \vee a)e' &= e''(e \wedge a)(e \vee a)e' \\ &= e''(e \vee a)(e \wedge a)e' \\ &= e''(e \vee a) \\ &= e'(e \vee a) \\ &= e''(f \vee a)(f \wedge a)f' \\ &= e''(e \wedge a)(e \vee a)f' \\ &= (e \vee a)f' \\ &= (f \vee a)f'. \end{aligned}$$

This completes the proof by symmetry. □

In particular the previous proof implies:

$$e'' \cdot a \cdot e'' = e' \cdot a \cdot e'' = e' \cdot a \cdot e' = f' \cdot a \cdot f' ... \tag{2.29}$$

2. 5. 2 Definition. Let $\mathfrak{S}$ be a d-semigroup and $e \in S$ a unit of $a \wedge b$ with $(e \wedge a)a^* = e = e^{\cdot}(e \wedge a) = e$. Then we symbolize $e \vee a = f \vee a$, recall 2.2.4, by a^+, and call $a^*, a^{\cdot}$ as *local inverses* of $e \wedge a$.

2. 5. 3 Definition. Let $\mathfrak{S}$ be an arbitrary d-semigroup and let $e \in S$ be a unit of a and a^* a local inverse w. r. t. e. We define *the absolute value* $|\,a\,|$ of a by the uniquely determined element $a^* \cdot a \cdot a^* = (e \vee a) \cdot a^* = a^+ a^*$.

By definition absolute values are positive, and it is immediately clear that any homomorphism h respects $|\ |$, that is satisfies

$$h(|a|) = |h(a)|. \tag{2.30}$$

Furthermore we get:

2. 5. 4 Lemma. *The special elements just defined satisfy:*

$$\begin{aligned} (a \wedge b)^+ = a^+ \wedge b^+ \quad &\textit{and} \quad (e \wedge (a \wedge b))(a^* \vee b^*) = e \\ (a \vee b)^+ = a^+ \vee b^+ \quad &\textit{and} \quad (e \wedge (a \vee b))(a^* \wedge b^*) = e. \end{aligned}$$

PROOF. Recall lemma 2.2.2. □

Now we are in the position to show:

2. 5. 5 Proposition. *In any d-semigroup* $\mathfrak{S}$ *the following are valid:*

$$|\,a^+\,| \;=\; a^+\,. \tag{2.31}$$

$$|\,a\cdot b\,| \;\leq\; |\,a\,|\cdot|\,b\,|\cdot|\,a\,|\,. \tag{2.32}$$

$$|\,a\wedge b\,| \;\leq\; |\,a\,|\vee|\,b\,|\geq|\,a\vee b\,|\,. \tag{2.33}$$

PROOF. We show first $a\in P \Longrightarrow |\,a\,| = a$, which provides (2.31). To this end we start from positive elements a, e with $ae = a = ea$, and thereby also with $ea = e\vee a$. Then there exists an element a^* satisfying:

$$|\,a\,| = (e\vee a)a^* \;=\; aa^* = (e\vee a)(e\wedge a)a^* = e\vee a = a\,.$$

Let henceforth e be a common positive unit of a and b. Then we get immediately $(ab)^+ \leq a^+b^+$ and $(e\wedge a)(e\wedge b)\leq e^2\wedge ab$, which means that by suitable elements $a^*, b^*, (ab)^*$ it results:

$$(e^2\wedge ab)b^*a^* \geq (e\wedge a)(e\wedge b)b^*a^* = (e\wedge a)ea^* = e(e\wedge a)a^* = e^2\,.$$

This leads to:

$$|\,ab\,| \leq a^+b^+b^*a^* \leq a^+a^*\cdot b^+b^*\cdot a^+a^* = |\,a\,|\cdot|\,b\,|\cdot|\,a\,|\,.$$

Furthermore, according to 2.5.4, the element $a^*\vee b^*$ is of type $(a\wedge b)^*$ and the element $a^*\wedge b^*$ is of type $(a\vee b)^*$. So we get:

$$\begin{aligned} |\,a\wedge b\,| &= (a^+\wedge b^+)(a^*\vee b^*) \\ &= (a^+\wedge b^+)a^*\vee(a^+\wedge b^+)b^* \\ &\leq |\,a\,|\vee|\,b\,|\,, \end{aligned}$$

and similarly

$$\begin{aligned} |\,a\vee b\,| &= (a^+\vee b^+)(a^*\wedge b^*) \\ &= a^+(a^*\wedge b^*)\vee b^+(a^*\wedge b^*) \\ &\leq |\,a\,|\vee|\,b\,|\,. \end{aligned}$$

This completes the proof. □

By the absolute value the *prime notion* admits a sophisticated investigation.

2. 5. 6 Definition. $p\in S$ is called *semiprime*, if $\qquad |p| = |a||b| \implies |p| = |a| \vee |p| = |b|$,

prime, if $\qquad |p| \leq |a||b| \implies |p| \leq |a| \vee |p| \leq |b|$,

and completely prime, if

$$\begin{aligned} |p|^n \leq |a||b| \implies & |p|^n \leq |a| \vee |p| \leq |b| \\ \& \quad & |p|^n \leq |b| \vee |p| \leq |a|\,. \end{aligned}$$

2. 5. 7 Lemma. *$p \in S$ is semiprime iff p satisfies:*

$$|a| < |p| \ \& \ |b| < |p| \implies |a||b| < |p|\,.$$

PROOF. We may suppose that $p = |p|$, $a = |a|$, $b = |b|$ or equivalently that p, a, b are positive. But this implies $ap = p = bp \rightsquigarrow abp = p \ \& \ ab \neq p$. The rest is obvious. □

2. 5. 8 Proposition. *$p \in S$ is semiprime iff $p \in S$ is prime, and $p \in S$ is prime iff $p \in S$ is completely prime.*

PROOF. Again, let a, b, p be positive. We get immediately: p completely prime $\Longrightarrow$ p prime $\Longrightarrow$ p semiprime.

It remains to show: p semiprime $\Longrightarrow$ p completely prime. To this end suppose $p^n \leq ab$. It follows $p = p \wedge ab \leq (p \wedge a)(p \wedge b)$. But $p \not\leq a \ \& \ p \not\leq b$ would imply $(p \wedge a)(p \wedge b) < p$, a contradiction! Consequently p must be prime.

And this leads to complete primeness, since $p^n \leq ab \ \ \& \ p \not\leq b$ implies:

$$p^n \leq (p^n \wedge a) \cdot (p^n \wedge b) \leq (p^n \wedge a) \cdot (p \wedge b)^n = p^n \wedge a\,,$$

that is $p^n \leq a$, and since the rest follows by duality. □

Obviously, exactly all elements of type $a = 1 \vee x$ with semiprime $1 \vee x$ or of type $a = 1 \wedge x$ with semiprime $(1 \wedge x)^{-1}$ are semiprime and hence even completely prime.

Of special interest are those d-semigroups, in which any $|a|$ has a *prime decomposition*. They are called *factorial* – here – according to modern ring theory. If $(S, \cdot)$ is even a monoid, then $\mathfrak{S}$ is obviously already factorial, if each positive a is a product of primes and in addition each $1 \wedge a$ is a product of elements p^{-1} with prime positive elements p, the classical example being $(\mathbf{Q}, \cdot, |_N)$.

2.6 The idempotent Kernel

We turn to the *idempotents* $u = u^2$ of $\mathfrak{S}$.

2. 6. 1 Lemma. *Any idempotent element e of $\mathfrak{S}$ is positive and central.*

PROOF. First of all we get $ee = e\vee e$, whence e is positive, according to 2.2.5. This means furthermore for all positive elements a firstly $ea = e(e\vee a) = e\vee a$ and thereby next $ea = ae$.

Choose now an arbitrary a and a positive unit u of $e\wedge a$. Then according to 2.2.3 we get $a = (u\wedge a)(u\vee a)$. Hence it suffices to prove $e(u\wedge a) = (u\wedge a)e$. To this end we start from $(u\wedge a)u' = u = u''(u\wedge a)$ with positive elements u', u''. Then we get

$$u'e = eu' = euu' = eu''(u\wedge a)u' = eu' .$$

But this implies

$$(u\wedge a)e = (u\wedge a)eu''(u\wedge a) = (u\wedge a)u'e(u\wedge a) = e(u\wedge a) .$$

Thus our proof is complete. □

2. 6. 2 Definition. Let $\mathfrak{S}$ be a d-semigroup. Then by the *idempotent kernel* of $\mathfrak{S}$ we mean the set $E(S)$ of all idempotent elements. Since $E(S)$ will turn out to be closed under $\cdot$ and $\wedge$, it makes sense to speak of the algebra $\mathfrak{E}(S)$.

Provided $\mathfrak{S}$ is uniquely determined, we shall speak of E instead of $E(S)$ and shall denote the corresponding algebra by $\mathfrak{E}$.

2. 6. 3 Proposition. *The idempotent kernel of any d-semigroup $\mathfrak{S}$ forms a sub-d-semigroup of $\mathfrak{S}$.*

PROOF.
$$\begin{array}{rrcll} a,b\in E \Longrightarrow & (ab)^2 & = & abab = aabb = ab & \\ \& & (a\wedge b)^2 & = & a^2\wedge ab\wedge ba\wedge b^2 & = a\wedge b \\ \& & (a\wedge b)b & = & ab\wedge bb = ab\wedge b & = b\ . \end{array}$$
□

2.7 The cancellative Kernel

$a\in S$ is called *left cancellable* if it satisfies $ax = ay \Longrightarrow x = y$. Dually *right cancellable* elements are defined. Consequently $a\in S$ ia called *cancellable* if it is right and left cancellable.

The set of cancellable elements may, of course, be empty, consider for instance some suitable distributive lattice. But, if $\mathfrak{S}$ is a monoid, at least the identity is cancellable. On the other hand, if $\mathfrak{S}$ contains at least one cancellable element c it also contains an identity, since in this case it follows the implication

$$ec = c = ce \Longrightarrow aec = ac \;\&\; cea = ca \Longrightarrow ae = a = ea\,.$$

2. 7. 1 Definition. Let $\mathfrak{S}$ be a d-monoid. The elements $a, b \in S$ are called *orthogonal*, or synonymously *disjoint*, or *coprime,* denoted by $a \perp b$, if they satisfy $|\,a\,| \wedge |\,b\,| = 1$.

2. 7. 2 Corollary. *In any d-semigroup it holds*

$$a \perp b \;\&\; a \perp c \Longrightarrow a \perp bc \;\&\; a \perp (b \wedge c) \;\&\; a \perp (b \vee c)\,.$$

Let $x''x = 1 = xx'$ be satisfied in an arbitrary monoid. Then we obtain $x'' = x''xx' = x'$. This means that in a d-monoid any $x \leq 1$ has a uniquely determined *inverse* x^{-1} .

2. 7. 3 Definition. Let $\mathfrak{S}$ be a d-semigroup. By the *cancellative kernel* of $\mathfrak{S}$ we mean the set $C(S)$ of all cancellable elements. Since $C(S)$ is obviously closed under $\cdot$ and $\wedge$ it makes sense to speak of the algebra $\mathfrak{C}(S)$.

Provided $\mathfrak{S}$ is uniquely determined, we shall speak of C instead of $C(S)$ and denote the corresponding algebra by $\mathfrak{C}$.

2. 7. 4 Proposition. *Let $\mathfrak{S}$ be a d-semigroup.Then $\mathfrak{C}$ is a sub-d-monoid of $\mathfrak{S}$, unless C is not empty.*

PROOF. Obviously it suffices to prove $ab \in C \Longrightarrow b \in C$. So, suppose $ab \in C$. Then b is left cancellable and because

$$ab \in C \Longrightarrow (1 \wedge a)^{-1}ab \;\; = \;\; (1 \vee a)b = by \in C \;\; (\exists\, y \in S)$$

b is also right cancellable. □

2. 7. 5 Proposition. *In any d-monoid $\mathfrak{S}$ any $a \in S$ admits a uniquely determined* cone decomposition $a = xy^{-1}$ *with $x, y \in S \;\&\; x \perp y$.*

PROOF. Let $a = x \cdot y^{-1}$ satisfy the above condition. Then it results $(1 \wedge x \cdot y^{-1}) \cdot y = 1$, that is $1 \wedge x \cdot y^{-1} = 1 \wedge a = y^{-1}$ and thereby $y^{-1} = 1 \wedge a$

and $x = 1 \vee a$ – recall the cancellation rule and $(1 \vee a)(1 \wedge a) = a$. Hence no decomposition, different from $(1 \vee a)(1 \wedge a)$, satisfies the condition. On the other hand it holds:

$$\begin{array}{rcl} (1 \vee a) \wedge (1 \wedge a)^{-1} & = & a(1 \wedge a)^{-1} \wedge (1 \wedge a)^{-1} \\ & = & (1 \wedge a)(1 \wedge a)^{-1} = 1 \\ & \leadsto & \\ a = (1 \vee a)((1 \wedge a)^{-1})^{-1} & \& & (1 \vee a) \perp (1 \wedge a)^{-1}. \end{array}$$

This completes the proof. □

As usual an element $x \in S$ will be called *invertible*, if it has an inverse x^{-1} satisfying $x \cdot x^{-1} = 1 = x^{-1} \cdot x$. Of course, any invertible element is also cancellable. *Vice versa,* however, cancellable elements need not be invertible. In spite of this any d-semigroup $\mathfrak{S}$ admits a *quotient extension* in which any cancellable element of S becomes invertible. This will be pointed out in a later chapter.

2. 7. 6 Definition. Let $a, c \in S$ be positive, let c be cancellable in $\mathfrak{S}$ and suppose $R(a, c, a', c')$ and $L(a'', c'', a, c)$. Then, because of $c \in C$ the elements a', a'', c', c'' are uniquely determined. We define:

$$\begin{array}{rclcrcl} c * a & := & a' & & a * c & := & c' \\ & & & \& & & & \\ a'' & =: & a : c & & c'' & =: & c : a\,. \end{array}$$

2. 7. 7 Lemma. *Let $a \wedge b$, that is in particular let a or b be cancellable. Then the equations holds:*

$$a * b \wedge b * a = \ 1 \ = a : b \wedge b : a\,.$$

PROOF. $a \wedge b = (a \wedge b)(a * b) \wedge (a \wedge b)(b * a) = (a \wedge b)(a * b \wedge b * a)) \leadsto a * b \wedge b * a = 1\,.$ □

2. 7. 8 Lemma. *Let $a, c \in S$ be cancellable. Then any positive x satisfies:*

$$ax \geq c \Longleftrightarrow x \geq a * c \ \ \textit{and} \ \ xa \geq c \Longleftrightarrow x \geq c : a\,.$$

PROOF. It suffices to prove the $*$-formula. To this end suppose $ax \geq c$. Then – recall (2.19) and 2.7.7 – by cancellation of $a \wedge c$ it results:

$$\begin{array}{rcl} ax \geq c & \Longleftrightarrow & (c * a)x \geq a * c \\ & \Longleftrightarrow & (a * c) \wedge (c * a)x = a * c \wedge x = a * c\,. \end{array}$$ □

2. 7. 9 Lemma. *Let $a, b, c \in S$ be positive and cancellable. Then the equations hold:*

$$ab * c = b * (a * c) \tag{2.34}$$
$$c : ba = (c : a) : b\,. \tag{2.35}$$

PROOF. Again it suffices to prove the $*$-formula which results from:

$$abx \geq c \Longleftrightarrow bx \geq a * c \Longleftrightarrow x \geq b * (a * c)\,. \qquad \square$$

2. 7. 10 Corollary. *Let $a, b \in S$ be cancellable. Then the equation holds:*

$$\begin{aligned} a(a * b) = b(b * a) &= a \vee b \\ &= (a : b)b = (b : a)a\,. \end{aligned}$$

2. 7. 11 Lemma. *Let $a, b, c \in S$ be positive and let in addition a or bc be cancellable. Then the equations hold:*

$$a * bc = (a * b)((b * a) * c) \tag{2.36}$$
$$cb : a = (c : (a : b))(b : a)\,. \tag{2.37}$$

PROOF. Because $a * b \perp b * a \wedge c$ it results from (2.10)

$$\begin{aligned} & (a \wedge bc)(a * b)((b * a) * c) \\ = \ & (a \wedge (a \wedge b)c)(a * b)((b * a) * c) \\ = \ & (a \wedge b)((b * a) \wedge c)(a * b)((b * a) * c) \\ = \ & (a \wedge b)(a * b)((b * a) \wedge c)((b * a) * c) \\ = \ & bc\,. \end{aligned}$$

Thus we are through by duality. $\square$

2. 7. 12 Lemma. *Let $a, b, c \in S$ be positive and let b or c be cancellable. Then the equations hold:*

$$a * (b \wedge c) = a * b \wedge a * c\,. \tag{2.38}$$
$$a * (b \vee c) = a * b \vee a * c\,. \tag{2.39}$$

Let $a, b, c \in S$ be positive and let in addition a, b be cancellable. Then the equations hold:

$$(a \vee b) * c = a * c \wedge b * c\,. \tag{2.40}$$
$$(a \wedge b) * c = a * b \vee b * c\,. \tag{2.41}$$

PROOF.
$$\begin{array}{rcl}
a * (b \wedge c) & \leq & a * b \wedge a * c \\
& \& & \\
(a \wedge b \wedge c)(a * b \wedge a * c) & \leq & (a \wedge b)(a * b) \wedge (a \wedge c)(a * c) \\
& = & b \wedge c \\
& \leadsto & \\
a * (b \wedge c) & \geq & a * b \wedge a * c\,.
\end{array}$$

AND
$$\begin{array}{rcl}
(a \vee b) * c & \leq & a * c \wedge b * c \\
& \& & \\
(a \vee b)(a * c \wedge b * c) & \leq & a(a * c) \vee b(b * c) \\
& = & a \vee b \vee c \\
& \leadsto & \\
(a \vee b) * c & \geq & a * c \wedge b * c\,.
\end{array}$$

The rest follows by lemma 2.7.8. □

As a final remark on cancellable elements we give:

2. 7. 13 Lemma. *Let u be idempotent and b be positive and cancellable. Then the elements u and $u * b$ are coprime.*

PROOF. Under the conditions above $u \wedge b$ is cancellable, and it holds furthermore $(u \wedge b)(u \wedge u * b) = u \wedge b$, which implies $u \wedge u * b = 1$. □

Finally we introduce:

2. 7. 14 Definition. Let $\mathfrak{S}$ be a semigroup with 0. We call $\mathfrak{S}$ 0-*cancellative*, in case that $ax = ay \neq 0 \Longrightarrow x = y$.

Different from the preceding definition, $\mathfrak{S}$ is called *cancellative with* 0 if in addition $a \neq 0 \neq b \Longrightarrow ab \neq 0$ is satisfied – consider domains.

2.8 The complementary Case

In the context of commutativity and measure we will rely on a class of special d-semigroups, which were introduced by the author in [14] as *complementary semigroups*.

2. 8. 1 Definition. By a *complementary semigroup* in this note we mean a poitive d-monoid, in which the sets $\{x \mid ax \geq b\}$ and $\{x \mid xa \geq b\}$, respectively, have uniquely determined smallest elements $a * b$ and $b : a$, respectively.

If $\mathfrak{S}$ is a complementary semigroup, we call $a * b$ the *right complement* of a in b and $b : a$ the *left complement* of a in b.

Thus complementary semigroups by definition are $\wedge$-closed. This means a specialization w. r. t. the structures, investigated by the author, but this provides advantages which we wouldn't miss in this lecture note.

2. 8. 2 Proposition. *Let $\mathfrak{S}$ be a complementary d-monoid. Then the following rules are valid – together with their right/left counterparts:*

$$a * b \leq b\,. \tag{2.42}$$

$$a \leq b \Leftrightarrow b * a = 1\,. \tag{2.43}$$

$$a \leq b \Rightarrow a * c \geq b * c \;\&\; c * a \leq c * b\,. \tag{2.44}$$

$$a(a * b) = a \vee b\,. \tag{2.45}$$

$$ab * c = b * (a * c)\,. \tag{2.46}$$

$$a * (b : c) = (a * b) : c\,. \tag{2.47}$$

$$(a * b) * (a * c) = (b * a) * (b * c)\,. \tag{2.48}$$

PROOF. (2.42) through (2.45) are evident or already verified. In order to prove (2.46) and (2.47) we observe:

$$ax \geq b \Longleftrightarrow x \geq a * b \quad \text{and} \quad xa \geq b \Longleftrightarrow x \geq b : a\,.$$

Then (2.46) results *via:*

$$\begin{aligned} abx \geq c \Longrightarrow bx \geq a * c \;&\Longrightarrow\; x \geq b * (a * c) \\ &\Longrightarrow\; bx \geq a * c \Longrightarrow abx \geq c\,. \end{aligned}$$

and (2.47) results *via:*

$$x \geq a * (b : c) \Leftrightarrow ax \geq b : c \Leftrightarrow axc \geq b \Leftrightarrow xc \geq a * b \Leftrightarrow x \geq (a * b) : c\,.$$

Finally we get (2.48) immediately by (2.45) and (2.46). □

Henceforth, apart from the rules above, we will apply again and again the evident formulas $1 * a = a$, $(a \wedge b) * a = b * a$ and $a * (a \vee b) = a * b$.

Among the complementary d-monoids above all a special structure will play an important role. This structure was introduced by the author in [21] as *Quader-Algebra* and studied in [23] under the denotation *Brick*.

2. 8. 3 Definition. A complementary d-monoid is called a *brick*, if it contains a *zero element* 0 and satisfies:

$$\text{(Q)} \qquad a : (b * a) \;=\; (b : a) * b\,.$$

A brick is called a *complete brick* if it has no *order gaps.*
An intensive and extensive study of bricks is presented in [**?**]. Hence we may restrict our attention to some lemmata, which will be needed within the theory of d-semigroups.

$$a : (b * a) = a \wedge b = (b : a) * b\,. \tag{2.50}$$

PROOF.
$$\begin{aligned} a : (b * a) &= a : ((a \wedge b) * a) \\ &= ((a \wedge b) : a) * (a \wedge b) \\ &= a \wedge b\,, \end{aligned}$$

which implies the rest by symmetry. □

2. 8. 4 Proposition. *Bricks always satisfy all desirable laws of distributivity, more precisely, given a brick, we have* (2.38),...,(2.41) *of* 2.7.12.

PROOF. It suffices to verify (2.38) and (2.40).

Ad (2.38). It holds $a * (b \wedge c) \le a * b \wedge a * c$ and

$$\begin{aligned} & (a * (b \wedge c)) * (a * b \wedge a * c) \\ =\;& ((a * (b \wedge c)) * (a * b)) : ((a * c) * (a * b)) \\ =\;& (((b \wedge c) * a) * ((b \wedge c) * b)) : ((c * a) * (c * b)) \\ =\;& ((b \wedge c) * a) * ((c * b) : ((c * a) * (c * b))) \\ \le\;& ((b \wedge c) * a) * (c * a) \\ \le\;& (c * a) * (c * a) \\ =\;& 1 \\ \rightsquigarrow\;& \\ a * (b \wedge c) \;\ge\;& a * b \wedge a * c \end{aligned}$$

This means $a * (b \wedge c) = a * b \wedge a * c$ and consequently

$$\begin{aligned}(a \vee b) * c &= a(a * b) * c \\ &= (a * b) * (a * c) \\ &= (a * c \wedge a * b) * (a * c) \\ &= (a * (c \wedge b)) * (a * c) \\ &= (a * (c : (b * c))) * (a * c) \\ &= ((a * c) : (b * c)) * (a * c) \\ &= a * c \wedge b * c\,.\end{aligned}$$

Thus our proof is complete. □

2. 8. 5 Corollary. *Bricks are always normal d-semigroups .*

PROOF.
$$\begin{aligned}a * b \wedge b * a &= ((a \wedge b) * b) \wedge ((a \wedge b) * a) \\ &= (a \wedge b) * (a \wedge b) = 1\,.\end{aligned}$$

recall 2.8.4. □

We now turn to complete bricks. However, we will choose an approach as general as possible, in order to save the chance of applying the results to *ideal semigroups.*

2. 8. 6 Proposition. *Let* $\mathfrak{S}$ *be a positive complete* lattice monoid, *this means an algebra* $(S, \cdot, \leq, 1)$ *with* complete lattice $(S, \leq)$*, satisfying moreover* $1 \leq x\ (\forall x \in S)$ *and* $x \cdot (\bigwedge a_i) \cdot y = \bigwedge (x \cdot a_i \cdot y)$*, such that according to*

$$a \star \bigwedge x_i\ (a \cdot x_i \geq b) \quad \& \quad b \div a := \bigwedge x_i\ (x_i \cdot a \geq b)$$

the equation $a \div (b * a) = (b \div a) * b$ *is valid. Then* $\mathfrak{S}$ *is a brick, satisfying:*

(D1∧)	$x(\bigwedge a_i)y = \bigwedge(xa_iy)$	(D1∨)	$x(\bigvee a_i)y = \bigvee(xa_iy)$
(D2∧)	$x \vee \bigwedge a_i = \bigwedge(x \vee a_i)$	(D2∨)	$x \wedge \bigvee a_i = \bigvee(x \wedge a_i)$
(D3∧)	$x \star \bigwedge a_i) = \bigwedge(x \star a_i)$	(D3∨)	$x \star (\bigvee a_i) = \bigvee(x \star a_i)$
(D4∧)	$(\bigwedge a_i) \star x = \bigvee(a_i \star x)$	(D4∨)	$(\bigvee a_i) \star x = \bigwedge(a_i \star x)$

and the corresponding left/right counterparts.

PROOF. $(D1\wedge)$ is part of the definition.

Furthermore (D3$\vee$) and (D4$\wedge$) result by *straightforward* calculation *via*

$$\begin{array}{rrcll} & x \cdot y \geq \bigvee a_i & \Longleftrightarrow & y \geq x \star a_i & \\ \& & (\bigwedge a_i) \cdot y \geq x & \Longleftrightarrow & a_i \cdot y \geq x & \quad (i \in I)\,. \end{array}$$

Next we get
$$\begin{array}{rcl} a \div (b \star a) & = & a \wedge b \\ & = & b \div (a \star b)\,. \end{array}$$

For it results nearly immediately $a \wedge b \geq (a \star b) * a$ and it results by calculation
$$(a \div b) \star a \;\geq\; a \wedge b\,.$$
Observe: $a \wedge b \geq c$, that is $a \star c = 1 = b \star c$ implies

$$\begin{array}{rcl} c \div ((a \div b) \star a) & = & (c \div (a \star c)) \div ((a \div b) \star a) \\ & = & ((a \div c) \star a) \div ((a \div b) \star a) \\ & = & (a \div c) \star (a \div ((a \div b) \star a)) \\ & = & (a \div c) \star ((a \div b) \div (a \star (a \div b))) \\ & = & (a \div c) \star (a \div b) \\ & = & ((a \div c) \star a) \div b \\ & = & (c \div (a \star c)) \div b \\ & = & c \div b = 1\,. \end{array}$$

Hence it results $a \div (b \star a) = a \wedge b = (a \div b) \star a$. But in case of $c \geq \bigvee a_i$ this implies

$$\begin{array}{rrcl} & x & \geq & (\bigvee a_i) \star c \\ \Longrightarrow & c \div x & \leq & \bigvee a_i \\ \Longrightarrow & c \div x & \leq & \bigvee (c \div (a_i \star c)) \\ \Longrightarrow & c \div x & \leq & c \div \bigwedge (a_i \star c) \\ \Longrightarrow & x & \geq & \bigwedge (a_i \star c)\,, \end{array}$$

$$\begin{array}{rrcl} \text{meaning} & (\bigvee a_i) \star c & = & \bigwedge (a_i \star c) \\ \text{and} & c \div (\bigvee a_i) & = & \bigwedge (c \div a_i)\,. \end{array}$$

So we get (D4$\vee$) *via*

$$\begin{array}{rcl} (\bigvee a_i) \star c & = & (\bigvee a_i) \star (c \vee \bigvee a_i) \\ & \geq & \bigwedge (a_i \star c) \\ & \rightsquigarrow & \\ (\bigvee a_i) \star c & = & \bigwedge (a_i \star c)\,. \end{array}$$

Next, if $x \geq a(a \star b)$ we obtain:

$$\begin{array}{rcl} a \vee b & = & x \div ((a \vee b) \star x) \\ & = & x \div (a \star x \wedge b \star x) \\ & = & x \div (((a \star x) \div (b \star x)) \star (a \star x)) \\ & = & x \div ((a \star (x \div (b \star x))) \star (a \star x)) \\ & = & x \div ((a \star b) \star (a \star x)) \\ & = & x \div (a(a \star b) \star x) \\ & = & a(a \star b)\,, \\ & \rightsquigarrow & \\ a \leq b & \Longleftrightarrow & a \,\Big|_{\ell}\, b \;\&\; a \,\Big|_{r}\, b\,. \end{array}$$

Hence the structure under consideration is a complete brick, and it was already shown that (D1$\wedge$), (D3$\vee$), (D4$\bigwedge$) and (D4$\bigvee$) are satisfied.

Furthermore we get (D3$\wedge$) *via* (D4$\bigvee$)

$$\begin{array}{rcl} c \star \bigwedge a_i & = & c \star (0 : ((\bigwedge a_i) \star 0)) \\ & = & (c \star 0) \div \bigvee (a_i \star 0) \\ & = & \bigwedge ((c \star 0) \div (a_i \star 0)) \\ & = & \bigwedge (c \star (0 \div (a_i \star 0))) \\ & = & \bigwedge (c \star a_i)\,. \end{array}$$

We turn to (D2$\bigwedge$). Suppose that both, $(x \wedge \bigwedge a_i)x\,' = x$ and $(x \wedge a_i)x_i = x$, are satisfied with positive elements $x\,' \geq x_i$. Then it results

$$\begin{array}{rcl} x \vee \bigwedge a_i & = & (\bigwedge a_i)x\,' \\ & = & \bigwedge (a_i \cdot x\,') \\ & \geq & \bigwedge (a_i \cdot x_i) \\ & \geq & \bigwedge (x \vee a_i)\ . \end{array}$$

Finally we get:

$$\begin{array}{rcl} x \wedge \bigvee a_i & = & (x : \bigvee a_i) \star x \\ & = & (\bigwedge (x \div a_i)) \star x \\ & = & \bigvee ((x \div a_i) \star x) \\ & = & \bigvee (x \wedge a_i)\,, \end{array}$$

meaning (D2$\bigvee$), and

$$\begin{array}{rcl} x \cdot \bigvee a_i & = & (0 \div x \bigvee a_i) \star 0 \\ & = & ((0 \div \bigvee a_i) \div x) \star 0 \\ & = & ((\bigwedge (0 \div a_i)) \div x) \star 0 \\ & = & \bigvee (((0 \div a_i) \div x) \star 0) \\ & = & \bigvee ((0 \div x a_i) \star 0) \\ & = & \bigvee x a_i\ , \end{array}$$

meaning (D1$\vee$). Thus, by symmetry, the proof is complete. $\square$

2. 8. 7 Definition. A d-semigroup is called *completely integrally closed* if it satisfies:

(G) $\qquad \forall\, t \neq 1, a \in S^+ \;\exists\, n \in \mathbf{N} \;: t^n * a \not\geq t \not\leq a : t^n$

that is equivalently if

$$t \leq \bigwedge_1^\infty (t^n * a) \;\bigvee\; t \leq \bigwedge_1^\infty (a : t^n) \;\; (n \in \mathbf{N}) \Longrightarrow t = 1\,.$$

As will turn out in a later chapter, the importance of this notion results from the fact that a brick is completely integrally closed iff it admits a complete *(brick) extension.* Here we give the first half of that proof:

2. 8. 8 Proposition. *Any brick, admitting a complete extension, is completely integrally closed.*

PROOF. We may restrict the proof to one side and conclude:

$$\begin{array}{rcl}
t & \leq & \bigwedge(t^n * a) = (\bigvee t^n) * a \\
 & \Longrightarrow & \\
(\bigvee t^n) \cdot ((\bigvee t^n) * a) & = & (\bigvee t^n) \cdot \bigwedge(t^n * a) \\
 & = & (\bigvee t^n) t (t * \bigwedge(t^n * a)) \\
 & = & (\bigvee t^n) \cdot (t * ((\bigvee t^n) * a)) \\
 & \Longrightarrow & \\
t * ((\bigvee t^n) * a) & = & (\bigvee t^n) * a \\
 & \Longrightarrow & \\
t & = & ((\bigvee t^n) * a) : (t * ((\bigvee t^n) * a)) \\
 & = & ((\bigvee t^n) * a) : ((\bigvee t^n) * a) \\
 & = & 1\,,
\end{array}$$

that is $t \leq \bigwedge(t^n * a) \Longrightarrow t = 1$. $\square$

An alternative proof could be given by starting from $t * \bigwedge(t^n * a) = \bigwedge(t^n * a)$. But that proof needs all of 2.8.6 whereas in the preceding proof merely (D4$\wedge$) and $(\bigvee t^n) \cdot t = (\bigvee t^n)$ are applied.

Finally we show:

2. 8. 9 Proposition. *Let $\mathfrak{S}$ be a complementary semigroup, in particular a brick. Then C and E are closed under $*$ and $:$.*

PROOF. The assertion is obvious for C.

Let now u and v be idempotent. Then $u \vee v$ is idempotent, too, whence according to $u * v = u * (u \vee v)$ we may suppose w. l. o. g. $u < v$. Putting $u * v =: x$ this provides next $u * (x * x^2) \leq u * (x * ux^2) = v * v = 1$, which means $u(x * x^2) = u$. Suppose now $y(x * x^2) = x$. Then, since $x * x^2$ is a unit of u it is also a unit of any uy, whence in case of $y(x * x^2) = x$ it follows $uy = uy(x * x^2) = ux = v$. So by $x = u * v$ we get $x \leq y$ whence we finally obtain $x^2 = x(x * x^2) \leq y(x * x^2) = x$. □

Chapter 3

Classical Extensions

A d-semigroup $\mathfrak{S}$ need not have an *identity* and if so, the *cancellable* elements of $\mathfrak{S}$ need not be *invertible.* However, any d-semigroup admits a *canonical* smallest *identity extension* Σ and this extension Σ admits a *canonical quotient extension* $\mathfrak{Q}$, such that all cancellable elements of $\mathfrak{S}$ become invertible in $\mathfrak{Q}$.

3.1 An Identity Extension

Throughout this section let $\mathfrak{S}$ be a s-semigroup without identity. Clearly, there may exist a monoid extension, and if so the definition $\alpha \equiv \beta :\Longleftrightarrow x \cdot \alpha = x \cdot \beta \ \ (\forall x \in S)$ defines a congruence satisfying $x\alpha, \alpha y \in S$ which will turn out to be the finest identity extension with this property.

But does there exist always such an extension?

In fact, this is the case, as will now be shown.

To this end we start from the set of all *endomorphisms* F, G of the semilattice $(S, \wedge)$, considered under *composition* $\circ$ and *pointwise meet* defined by

$$x(\mathrm{F} \wedge \mathrm{G}) := x\mathrm{F} \wedge x\mathrm{G}\,.$$

This algebra is a monoid, satisfying (A1) through (A4), maybe except axiom (A4). Moreover it contains a substructure, isomorphic with $\mathfrak{S}$ with carrier $\{\mathrm{F}_a\}$,*via*

$$\mathrm{F}_a : \quad x \longmapsto xa\ .$$

Apart from these endomorphisms F_a the endomorphisms of type

$$\overline{\mathrm{F}}_a : \quad x \longmapsto x \wedge xa$$

will turn out to be most important, since the substructure, generated by the endomorphisms of type F_a and of type $\overline{\mathrm{F}}_a$ satisfies in addition axiom (A4).

3. 1. 1 Lemma. *Any endomorphism $\overline{\mathrm{F}}_a$ is even an automorphism.*

PROOF. $\overline{\mathrm{F}}_a$ is surjective: Suppose that e is a unit of $a \wedge x$ and that e' is positive, satisfying $e'(e \wedge a) = e$. Then it follows;

$$x = xe = xe'(e \wedge a) = xe' e \wedge xe' a = (xe') \wedge (xe')a = (xe')\overline{\mathrm{F}}_a \, .$$

Next $\overline{\mathrm{F}}_a$ is injective: Suppose $x\,\overline{\mathrm{F}}_a = x \wedge xa = y \wedge ya = y\,\overline{\mathrm{F}}_a$. Then in case of $(x \wedge y)e = x \wedge y$, $(e \wedge a)e' = e$ it results

$$x = x(e \wedge a)e' \;=\; y(e \wedge a)e' = y \, .$$

This completes the proof. □

3. 1. 2 Lemma. *For any pair $a, b \in S$ there exists a pair $a', b' \in S$ with*

$$\begin{array}{rclcrcl} \overline{\mathrm{F}}_a \circ \overline{\mathrm{F}}_b & = & \overline{\mathrm{F}}_{b'} \circ \overline{\mathrm{F}}_a & \textit{and} & \overline{\mathrm{F}}_a \circ \overline{\mathrm{F}}_b & = & \overline{\mathrm{F}}_b \circ \overline{\mathrm{F}}_{a'} \\ & & & \rightsquigarrow & & & \\ \overline{\mathrm{F}}_a \circ \overline{\mathrm{F}}_b^{-1} & = & \overline{\mathrm{F}}_{b'}^{-1} \circ \overline{\mathrm{F}}_a & \textit{and} & \overline{\mathrm{F}}_b^{-1} \circ \overline{\mathrm{F}}_a & = & \overline{\mathrm{F}}_{a'} \circ \overline{\mathrm{F}}_b^{-1} \, . \end{array}$$

PROOF. Suppose $(x \wedge b)e = x \wedge b$, $e''(e \wedge a) = e$ with positive e'' and put $(b \wedge ab)e'' =: b'$. Then it follows $(x \wedge b')e = x \wedge b'$, and it results:

$$\begin{array}{rcl} x(\overline{\mathrm{F}}_a \circ \overline{\mathrm{F}}_b) & = & (x \wedge xa)\overline{\mathrm{F}}_b \\ & = & x \wedge xa \wedge xb \wedge xab \\ & = & x(e \wedge a) \wedge x(b \wedge ab)e''(e \wedge a) \\ & = & x(e \wedge a) \wedge xb'(e \wedge a) \\ & = & (x \wedge xb')(e \wedge a) \\ & = & (x \wedge xb') \wedge (x \wedge xb')a \\ & = & x(\overline{\mathrm{F}}_{b'} \circ \overline{\mathrm{F}}_a) \, . \end{array}$$

Thus the proof is complete by duality. □

We now show that any $\mathrm{F}_a \circ \overline{\mathrm{F}}_b^{-1}$ and any $\overline{\mathrm{F}}_b^{-1} \circ \mathrm{F}_a$ is of type F_s.

3. 1. 3 Lemma. *Let $ae = a$ and $e''(e \wedge b) = e$ be satisfied with some positive element e''. Then it holds:*

$$\mathrm{F}_a \circ \overline{\mathrm{F}}_b^{-1} \;=\; \mathrm{F}_{ae''} \, .$$

and it follows dually: Let $ea = a$ and $(e \wedge b)e' = e$ be satisfied with some positive element e'. Then it holds:

$$\overline{\mathrm{F}}_b^{-1} \circ \mathrm{F}_a \;=\; \mathrm{F}_{e'a} \,.$$

PROOF. Under the above conditions we obtain:

$$x\mathrm{F}_a = xa = xae''(e \wedge b) = xae'' \wedge xae''b$$

in the first case, and in the second case we get:

$$x\mathrm{F}_a = xea = x(e \wedge b)e'a = (x \wedge xb)e'a = x(\overline{\mathrm{F}}_b \circ \mathrm{F}_{e'a}) \,. \qquad \square$$

Now we are in the position to prove:

3. 1. 4 Proposition. *The set Σ of all endomorphisms of $(S, \wedge)$, representable by some $\mathrm{G} \circ \overline{\mathrm{F}}_b^{-1}$, where $\mathrm{G} = \mathrm{I}$ or $\mathrm{G} = \mathrm{F}_a$ or $\mathrm{G} = \overline{\mathrm{F}}_a$, is closed under $\circ$ and the set Σ_S of all F_a forms a subsemigroup, isomorphic with $(S, \cdot)$.*

PROOF. It holds $\mathrm{F}_a \circ \overline{\mathrm{F}}_b = \mathrm{F}_{a \wedge ab}$, $\overline{\mathrm{F}}_a \circ \mathrm{F}_b = \mathrm{F}_{b \wedge ab}$ and $\overline{\mathrm{F}}_a \circ \overline{\mathrm{F}}_b = \mathrm{F}_{a \wedge b \wedge ab}$ whence Σ according to 3.1.2 and 3.1.3 is $\circ$-closed because $\overline{\mathrm{F}}_a^{-1} \circ \overline{\mathrm{F}}_b^{-1} = (\overline{\mathrm{F}}_b \circ \overline{\mathrm{F}}_a)^{-1}$.

Furthermore we have $ea = a \neq b = eb \implies \mathrm{F}_a \neq \mathrm{F}_b$ and $\mathrm{F}_a = \mathrm{F}_{a \wedge ab} \circ \overline{\mathrm{F}}_b^{-1}$ and $\mathrm{F}_a \circ \mathrm{F}_b = \mathrm{F}_{ab}$. $\square$

We now turn to $\wedge$:

3. 1. 5 Lemma. *In the set Σ w. r. t. $\wedge$ it holds:*

$\wedge$	I	F_b	$\overline{\mathrm{F}}_b$
I	I	$\overline{\mathrm{F}}_b$	$\overline{\mathrm{F}}_b$
F_a		$\mathrm{F}_{a \wedge b}$	$\overline{\mathrm{F}}_{a \wedge b}$
$\overline{\mathrm{F}}_a$			$\overline{\mathrm{F}}_{a \wedge b}$

PROOF. This follows by *straightforward* calculations. $\square$

3. 1. 6 Lemma. *Any two endomorphisms $\mathrm{G} \circ \overline{\mathrm{F}}_a^{-1}, \mathrm{H} \circ \overline{\mathrm{F}}_b^{-1}$ where G,H have the denominator 1 admit a representation with a common denominator.*

PROOF. It suffices to settle the case for pairs of type $\overline{\mathrm{F}}_a^{-1}, \overline{\mathrm{F}}_b^{-1}$, and according to 3.1.2 we may suppose that $\overline{\mathrm{F}}_a \circ \overline{\mathrm{F}}_b = \overline{\mathrm{F}}_b \circ \overline{\mathrm{F}}_{a'}$ is satisfied. Consequently we get:

$$\begin{aligned} (3.1) \qquad \overline{\mathrm{F}}_a^{-1} &= \overline{\mathrm{F}}_b \circ \overline{\mathrm{F}}_b^{-1} \circ \overline{\mathrm{F}}_a^{-1} = \overline{\mathrm{F}}_b \circ (\overline{\mathrm{F}}_a \circ \overline{\mathrm{F}}_b)^{-1} = \overline{\mathrm{F}}_b \circ \left(\overline{\mathrm{F}}_{a\wedge b\wedge ab}\right)^{-1} \\ (3.2) \qquad \overline{\mathrm{F}}_b^{-1} &= \overline{\mathrm{F}}_{a'} \circ \overline{\mathrm{F}}_b^{-1} \circ \overline{\mathrm{F}}_a^{-1} = \overline{\mathrm{F}}_{a'} \circ (\overline{\mathrm{F}}_a \circ \overline{\mathrm{F}}_b)^{-1} = \overline{\mathrm{F}}_{a'} \circ \left(\overline{\mathrm{F}}_{a\wedge b\wedge ab}\right)^{-1} . \end{aligned}$$

This completes the proof. □

Now we are in the position to show:

3. 1. 7 Proposition. *The set* Σ *of endomorphisms* $\mathrm{G} \circ \overline{\mathrm{F}}_b^{-1}$ (*recall* 3.1.4) *is closed under* $\wedge$, *and the set* Σ_S *of all* F_s *forms a semilattice under* $\wedge$, *which is isomorphic with* $(S, \wedge)$.

PROOF. Let G and H have denominator 1. Then $\mathrm{G} \wedge \mathrm{H}$ is contained in Σ, and it holds:

$$\mathrm{G} \circ \overline{\mathrm{F}}_b^{-1} \wedge \mathrm{H} \circ \overline{\mathrm{F}}_b^{-1} = (\mathrm{G} \wedge \mathrm{H}) \circ \overline{\mathrm{F}}_b^{-1} .$$

Hence Σ_S is closed under $\wedge$. Furthermore it holds:

$$x\mathrm{F}_{a\wedge b} = xa \wedge xb = x\mathrm{F}_a \wedge x\mathrm{F}_b = x(\mathrm{F}_a \wedge \mathrm{F}_b) .$$

Hence $(\Sigma_S, \wedge)$ and $(S, \wedge)$ are isomorphic. □

Finally we get nearly immediately:

3. 1. 8 Lemma. $\sum := (\Sigma, \circ, \wedge)$ *satisfies axiom* (A4).

PROOF. It suffices to show that $\mathrm{G} \wedge \mathrm{H}$ is a *left* and also a *right divisor* of G, in case that G and H have denominator 1. But this is shown – nearly immediately – by the tabular above, since in all cases but one the *inverse mapping* of $\mathrm{G} \wedge \mathrm{H}$ exists, and since $\mathrm{F}_{a\wedge b}$ is a right/left divisor of F_a (in $\mathfrak{S}$) according to (A4). □

Moreover we obtain;

3. 1. 9 Lemma. Σ *satisfies*

$$(3.3) \qquad \alpha = \beta \Longleftrightarrow \alpha \cdot x = \beta \cdot x \ \ (\forall\, x \in S) \Longleftrightarrow x \cdot \alpha = x \cdot \beta \ \ (\forall\, x \in S) .$$

PROOF. It remains to prove (3.3). Ti this end first of all observe (again) $\alpha \in \Sigma$ & $x \in S$ implies $x\alpha \in S$. Recall $x(1 \wedge a) = x \wedge xa$ and $x(1 \wedge b)^{-1} \in S$, since $(1 \wedge b)^{-1}$ is an automorphism of $\mathfrak{S}$.

We have to consider the cases:

$$
\begin{array}{lrcll}
(3.4) & x \cdot 1 & = & x \cdot v \;\; (\forall x \in S) & (1)\\
(3.5) & x \cdot u & = & x \cdot v \;\; (\forall x \in S) & (2)\\
(3.6) & x \cdot u & = & x \cdot (1 \wedge b) \;\; (\forall x \in S) & (3)\\
(3.7) & x \cdot 1 & = & x \cdot (1 \wedge b) \;\; (\forall x \in S) & (4)\\
(3.8) & x \cdot (1 \wedge a) & = & x \cdot (1 \wedge b) \;\; (\forall x \in S) & (5)
\end{array}
$$

(1) cannot hold, since by $v = v^2$ we would get $xv = x = vx$ although $\mathfrak{S}$ is assumed not to contain an identity.

(2) implies $u = v$, let x be a unit of $u \wedge v$.

(3) leads to $x \cdot u(1 \wedge b)^{-1}$, but $u(1 \wedge b)^{-1}$ belongs to S whence $e := u(1 \wedge b)^{-1}$ would act as identity, although $\mathfrak{S}$ is assumed not to contain an identity. So also (3) cannot hold.

(4) implies $x \wedge xb = x \;\; (\forall x \in S)$ that is $x \in S^+$ and hence $1 \leq b$ and thereby $1 \wedge b = 1$.

Finally, let's start from (5), that is from $x \cdot (1 \wedge a) = x \cdot (1 \wedge b) \;\; (\forall x \in S)$.

$(1 \wedge a)$ and $(1 \wedge b)$, respectively, stand for $I \wedge F_a$ and $I \wedge F_b$, respectively. And (5) means $I \wedge F_a = I \wedge F_b$. □

So, summarizing we get:

3. 1. 10 Theorem. $\sum = (\Sigma, \circ, \wedge)$ *is an* identity-extension *of* $\mathfrak{S} = (S, \cdot, \wedge)$ *in which* $\mathfrak{S}$ *is embedded by* $s \longmapsto F_s$.

Moreover, putting $I =: 1$ *and* $1 \cdot a = a = a \cdot 1$ *we get*

$$(3.9) \qquad \alpha = \beta \Longleftrightarrow \alpha \cdot x = \beta \cdot x \;\; (\forall\, x \in S) \Longleftrightarrow x \cdot \alpha = x \cdot \beta \;\; (\forall\, x \in S).$$

Henceforth, we will denote $\sum$ also by $\mathfrak{S}^1$ always having in mind that this $\mathfrak{S}^1$ is assumed to be the extension by endomorphisms.

3.2 A Quotient Extension

In this section we could start from the *quotient hull* exhibited by MURATA. But, in order to be as *self-contained* as possible and also to benefit from the special situation we start from the set R of all pairs $a.b$ with positive a and some positive cancellative element b. Provided this set is empty there is nothing to show. Otherwise $\mathfrak{S}$ is a monoid whence in particular there are the pairs of type $a.1$ and $1.b$. Again, recall the *residuation arithmetic.*

3. 2. 1 Lemma. *The set R of all pairs $a.b$ with left cancellable* component *b forms a monoid under the operation $a.b \circ c.d := a(b*c).d(c*b)$.*

PROOF. First of all observe $a.b = a.1 \circ 1.b$. This leads next to

$$\begin{aligned} (a.b \circ x.1) \circ c.d &= a(b*x).(x*b) \circ c.d \\ &= a(b*x)((x*b)*c).d(c*(x*b)) \\ &= a(b*xc).d(xc*b) \\ &= a.b \circ xc.d \\ &= a.b \circ (x.1 \circ c.d) \end{aligned}$$

and

$$\begin{aligned} (a.b \circ 1.y) \circ c.d &= a.yb \circ c.d \\ &= a(yb*c).d(c*yb) \\ &= a(b*(y*c)).d(c*y)((y*c)*b) \\ &= a.b \circ (y*c).d(c*y) \\ &= a.b \circ (1.y \circ c.d) \ . \end{aligned}$$

From this results *general associativity via*:

$$\begin{aligned} (a.b \circ x.y) \circ c.d &= (a.b \circ (x.1 \circ 1.y)) \circ c.d \\ &= ((a.b \circ x.1) \circ 1.y) \circ c.d \\ &= (a.b \circ x.1) \circ (1.y \circ c.d) \\ &= \ \dots \\ &= a.b \circ (x.y \circ c.d) \ . \end{aligned}$$

So R forms a semigroup, and by

$$1.1 \circ a.b = a.b = a.b \circ 1.1$$

this semigroup is even a monoid. □

3. 2. 2 Lemma. *In R the definition*

$$a.b \equiv c.d \ \ :\Longleftrightarrow \ \ a : b = c : d \ \& \ b : a = d : c$$

generates a congruence relation w. r. t. $\circ$.

PROOF. Obviously $\equiv$ is an equivalence relation. Furthermore, cancellable elements x satisfy:

$$ax : bx \ = \ (ax : x) : b = a : b$$

and thereby $ax.bx \equiv a.b$. Suppose now $x, y \in C \cap P$. Then we get in particular:

$$\begin{aligned}
ax.bx \circ c.d &\equiv ax(bx * c).d(c * bx) \\
&\equiv ax(x * (b * c)).d(c * b)((b * c) * x) \\
&\equiv a(b * c)((b * c) * x).d(c * b)((b * c) * x) \\
&\equiv a(b * c).d(c * b) \\
&\equiv a.b \circ c.d \\
&\equiv a(b * c).d(c * b) \\
&\equiv a(b * c)((c * b) * y).d(c * b)((c * b) * y) \\
&\equiv a(b * c)((c * b) * y).dy(y * (c * b)) \\
&\equiv a(b * cy).dy(cy * b) \\
&\equiv a.b \circ cy.dy \ .
\end{aligned}$$

Hence it results:

$$\begin{aligned}
& a.b \equiv a'.b' \ \ \& \ \ c.d \equiv c'.d' \\
\Longrightarrow \quad a.b \circ c.d &\equiv (a : b).(b : a) \circ (c : d).(d : c) \\
&\equiv (a' : b').(b' : a') \circ (c' : d').(d' : c') \\
&\equiv a'.b' \circ c'.d' \ .
\end{aligned}$$

This completes the proof. □

We denote $(R, \circ)/\!\equiv$ by $\mathfrak{Q}$ and the elements of $\mathfrak{Q}$ by lower case Greek letters. Obviously the special classes $a.1/\equiv$ form a subsemigroup of $\mathfrak{Q}$, which is isomorphic with $\mathfrak{P}$, because

$$a.1 \circ b.1 \equiv ab.1 \ \text{ and } \ a.1 \equiv b.1 \Longleftrightarrow a = a : 1 = b : 1 = b \ .$$

Furthermore the set of all classes $1.b/\!\equiv$ forms a subsemigroup, which is *anti-isomorphic* with $\mathfrak{C} \cap \mathfrak{P}$, because

$$1.b \circ 1.d = 1.db \ \text{ and } \ 1.b \equiv 1.d \Longleftrightarrow \ b = b : 1 = d : 1 = d \ .$$

Finally $b \in C \cap P$ satisfies:

$$1.b \circ b.1 \equiv 1.1 \equiv b.b \equiv b.1 \circ 1.b \text{ and } 1.1 \circ a.b \equiv a.b \equiv a.b \circ 1.1 \ .$$

Hence, abbreviating $a := a.1$ and $b^{-1} := 1.b$ we are led to $a.b = ab^{-1}$ and $ab^{-1} \circ cd^{-1} = ab^{-1}.cd^{-1}$ without any complications.

Before presenting a further embedding theorem, recall that any α has a representation by some pair of coprime components a, b and that any two elements $\alpha, \beta \in Q$ may be assumed to have the same denominator. Observe that in case of $d \in C \cap P$ the element ab^{-1} may also be written in the extended form $a(b * d)(b \vee d)^{-1}$.

This in mind we turn to

3. 2. 3 Proposition. *Any d-semigroup $\mathfrak{S}$ admits a* quotient hull, *that is a uniquely determined $\mathfrak{Q}$, satisfying:*

(*i*) *Any cancellable element of $\mathfrak{S}$ remains cancellable in $\mathfrak{Q}$ and any cancellable element of $\mathfrak{Q}$ is invertible.*
(*ii*) *Any $\alpha \in Q$ has an orthogonal decomposition that is equals some $a \cdot b^{-1}$ with $a \in P$ & $b \in C \cap P$.*

PROOF. We start from the extension $\mathfrak{Q}$ constructed above and show in a first step that the definition $\alpha \leq \beta \iff \alpha x = \beta \ (x \in P)$ leads to a *partial order* $\leq$ of $\mathfrak{Q}$, respected by multiplication. To this end observe first that $ab^{-1} \cdot x$ with positive x equals some $y \cdot ab^{-1}$ with positive y and *vice versa,* since

$$xb = bx' \ \& \ ax' = ya \implies ab^{-1} \cdot x = ax'b^{-1} = y \cdot ab^{-1} \ . \tag{3.10}$$

$$ya = ax'' \ \& \ bx'' = zb \implies y \cdot ab^{-1} = ax''b^{-1} = ab^{-1} \cdot z \ . \tag{3.11}$$

This implies

$$ab^{-1} \leq cd^{-1} \Longrightarrow uv^{-1} \cdot ab^{-1} \cdot xy^{-1} \leq uv^{-1} \cdot cd^{-1} \cdot xy^{-1} \ . \tag{3.12}$$

Furthermore it is immediately seen that $\leq$ is *reflexive* and *transitive,* and it is easily shown that $\leq$ is also *antisymmetric*, since in case of $\alpha = ab^{-1}$ and $x\alpha = \beta \ \& \ y\beta = \alpha \implies yx\alpha = \alpha$ we get $yxa = a$ and thereby $xa = a$, which means $x\alpha = \alpha = \beta$.

We now show that $\mathfrak{Q}$ forms a semilattice w. r. t. $\leq$. To this end we recall that for orthogonal components $uv^{-1} \leq ab^{-1}$ is valid iff $ub \leq va$ is valid, from which follows that $u \leq a$ & $b \leq v$ is valid. But this implies – according to $a \perp b$ & $c \perp d \implies (a \wedge c) \perp (b \vee d)$ – that $(a \wedge c)(b \vee d)^{-1} =: ab^{-1} \wedge cd^{-1}$ is *infimum* of the elements ab^{-1} and cd^{-1}.

It remains to show that $\mathfrak{Q}$ satisfies also axiom (A3). To this end we may start from two elements α, β with common denominator, say $\alpha = ab^{-1}$ and $\beta = cb^{-1}$. Then it follows:

$$\begin{aligned} \gamma \leq \alpha x^{-1} \ \& \ \gamma \leq \beta x^{-1} &\iff \gamma x \leq a \ \& \ \gamma x \leq b \\ &\iff \gamma x \leq a \wedge b \\ &\iff \gamma \leq (a \wedge b) x^{-1} , \end{aligned}$$

whence by $yb = by'$ with $y \in P$ it results further

$$\begin{aligned} \gamma \leq \alpha y \ \& \ \gamma \leq \beta y &\iff \gamma \leq ab^{-1} y \ \& \ \gamma \leq cb^{-1} y \\ &\iff \gamma \leq ay' b^{-1} \ \& \ \gamma \leq cy' b^{-1} \\ &\iff \gamma \leq (ay' \wedge cy') b^{-1} \\ &\iff \gamma \leq (a \wedge c) y' b^{-1} \\ &\iff \gamma \leq (a \wedge c) b^{-1} y \\ &\iff \gamma \leq (ab^{-1} \wedge cb^{-1}) y . \end{aligned}$$

Thus axiom (A3) is proven from the right, and it follows the left side version by duality.

Finally, according to 2.7.4 and by the calculating rules for $\cdot, \wedge$ and $\circ, \wedge$, respectively, it follows nearly immediately that $(S, \cdot, \wedge)$ is embedded in $(Q, \circ, \wedge)$ and that $\mathfrak{Q}$ is uniquely determined by (i) and (ii) – up to isomorphism. $\square$

We finish this section by reminding the reader at two classical quotient extensions, namely that of $(\mathbf{N}, +, \min)$ by $(\mathbf{Z}, +, \min)$ and that of $(\mathbf{N}^+, \cdot, \mathrm{GCD})$ by $(\mathbf{Q}^+, \cdot, \mathrm{GCD}_N)$, respectively. Here $\mathrm{GCD}_N(a, b)$ means the infimum of $a, b \in \mathbf{Q}^+$ with respect to $a \,|_N\, b :\iff \exists n \in \mathbf{N} : a \cdot n = b$.

Chapter 4

Ideals

In order to enable an analysis of special d-semigroups in later chapters, in this chapter special substructures and basic relations are introduced. A fundamental role is played by *ideals* arising in *lattice theory* or carried over from *ring* or *ℓ-group theory,* respectively.

4.1 p-ideals, m-ideals, d-ideals

4. 1. 1 Definition. $I \subseteq S$ is called a *lattice ideal*, or briefly an *l-ideal,* if it satisfies:

$$a \vee b \in I \iff a \in I \ \& \ b \in I.$$

If moreover I satisfies:

$$a \wedge b \in I \iff a \in I \bigvee b \in I,$$

I is called an *irreducible* or synonymously a *prime* ideal. .

As a first characterization of prime ideals we get:

4. 1. 2 Lemma. *The following are pairwise equivalent:*

(i) *P is a prime ideal.*

(ii) *Whenever two ideals A, B satisfy $A \cap B = P$, then it follows $A = P$ or $B = P$.*

PROOF. If (i) is valid and $A \cap B = P$ is valid according to (ii), then in case of $A \neq P$ and $a \in A \setminus P$ by assumption any $b \in B$ satisfies $a \wedge b \in P$, and thereby $b \in P$.

If however (ii) is valid and $a \wedge b \in P,\ b \notin P$, then the set of all x satisfying $b \wedge x \in P$ forms an ideal A and the set of all y with $z \in A \Longrightarrow y \wedge z \in P$ forms an ideal $B \neq P$. But, by construction it holds $A \cap B = P$. This implies $a \in P$. □

4. 1. 3 Lemma. *For each pair of different elements $x, y \in S$ there exists a prime ideal $M_{x,y}$, which contains exactly one of these two elements.*

PROOF. Suppose w. l. o. g. that it holds $y \not\leq x$. Then we get $y \notin (x]$. Hence, by Zorn's lemma, in the set of all ideals containing x but not containing y there exists a maximal ideal M. Assume now $a \wedge b \in M$ and form A and B according to the proof of 4.1.2. Then it follows $A \cap B = M$. So in case of $A \neq M$ and $B \neq M$ it would follow $x \in A$ & $x \in B$, meaning $x = x \wedge x \in M$, a contradiction. Hence one of the two ideals A, B must be equal to M. □

As an immediate consequence we get:

4. 1. 4 Proposition. *Any ideal is an intersection of prime ideals.*

PROOF. Let A be an ideal and D be the intersection of all prime ideals, containing A. Then, provided $c \in D \backslash A$, we could extend A to some maximal c not containing ideal M. But – along the proof lines of 4.1.2 this M must be prime, a contradiction! □

Dually w. r. t. the notion of a lattice ideal the notion of a *lattice filter* or briefly a *filter* is defined. Consequently in a given lattice $\mathfrak{L}$ filters are the ideals of the dual lattice of $\mathfrak{L}$. Hence all notions concerning lattice ideals can be carried over to lattice filters in a natural manner. In particular the results above on lattice ideals carry over to lattice filters.

Besides *prime filters* and *prime ideals* there are two further types of ideals, which will contribute essentially to clearing structure problems in d-semigroup theory.

4. 1. 5 Definition. Let $\mathfrak{S}$ be an arbitrary d-semigroup. By a *p-ideal* of $\mathfrak{S}$ we mean a *lattice ideal,* for short l-ideal, containing at least one positive element.

A p-ideal is called an *m-ideal* if it is closed under multiplication.

Furthermore, by a *p-filter* of $\mathfrak{S}$ we mean a filter, each element of which is positive.

Finally we call *d-ideal* any subset $\mathfrak{a}$ of S, which is closed under $\wedge$ and which moreover satisfies $S \cdot \mathfrak{a} \cdot S \subseteq \mathfrak{a}$.

Observe and keep in mind: S itself is always an ideal/filter whatever.

Obviously the notion of a d-ideal is “copied” from ring theory and it is easily verified that any d-ideal is a *lattice filter*, too. To this end recall that a given d-ideal $\mathfrak{a}$ contains any px with $p \in P$ & $x \in \mathfrak{a}$. Consequently d-ideals could also have been defined as filters, satisfying $S \cdot F \cdot S \subseteq F$.

Summarizing: Ideals and filters are defined strictly according to lattice theory, p-ideals, m-ideals and p-filters depend on the particular situation in d-semigroups and d-ideals are taken from Dedekind.

Given two ideals (filters) A, B we will denote by $A + B$ the corresponding ideal (filter), generated by $A \cup B$. Consequently $\sum B_i$ $(i \in I)$ will denote the ideal (filter) generated by the family B_i $(i \in I)$.

4. 1. 6 Proposition. *Let $\mathfrak{S}$ be a d-semigroup. Then the set of p-ideals and the set of d-ideals, as well, form a cdl-semigroup under the corresponding* complex operations *of* $\mathfrak{S}$.

Moreover, both, the lattice of filters and the lattice of d-ideals satisfy the infinite distributivity law:

(DIF) $$A \cap \sum B_i = \sum (A \cap B_i) \ \ (i \in I).$$

PROOF. Let A, B be two p-ideals. We show first, that the *complex product* $A \cdot B := \{ab \,|\, a \in A, b \in B\}$ forms a p-ideal. To this end we may start from two positive elements $p \in A$ and $q \in B$.

$A \cdot B$ is an *order ideal* of $(S, \leq)$. Observe: $x \leq ab \Longrightarrow x \leq (a \vee p)(b \vee q)$, whence a and b may be assumed to be positive. And in case of $(a \wedge x)x' = x$ this leads to
$$x = xx' \wedge xb \wedge ax' \wedge ab = (x \wedge a)(x' \wedge b).$$

But $A \cdot B$ is not only an order ideal but even a lattice ideal. Observe: If p and q are positive, then also pq is positive and if $a_1, a_2 \in A$ and $b_1, b_2 \in B$ then we get $a_1 \cdot b_1 \vee a_2 \cdot b_2 \leq (a_1 \vee a_2) \cdot (b_1 \vee b_2) \in A \cdot B$.

Furthermore the *complex supreme* $A \vee B := \{a \vee b \,|\, a \in A, b \in B\}$ is an ideal, more precisely the ideal, generated by the join $A \cup B$, and similarly the *complex infimum* $A \wedge B := \{a \wedge b \,|\, a \in A,\, b \in B\}$ is an ideal.

Finally the semigroup of p-ideals is completely distributive, since it follows

$$\begin{array}{rrcl} \text{immediately} & A \wedge (B \vee C) & = & (A \wedge B) \vee (A \wedge C) \\ \& & A \cdot (B \vee C) & = & A \cdot B \vee A \cdot C \\ \text{and by calculation} & A \cdot (B \wedge C) & = & A \cdot B \wedge A \cdot C\,. \end{array}$$

For, consider a_1, $a_2 \in A$ and $b \in B$, $c \in C$. Then we get:

$$a_1 b \wedge a_2 c \leq (a_1 \vee a_2)(b \wedge c) \in A \cdot (B \wedge C)\,.$$

So, p-ideals satisfy the laws above.

But these laws are also satisfied by filters and hence by d-ideals, since it is easily seen that together with each pair of d-ideals $\mathfrak{a}$, $\mathfrak{b}$ also their complex product forms an order filter, and that the rest follows by analogy to the first part of the proof.

Finally filters and d-ideals satisfy:

$$A \cap \sum B_i = \sum (A \cap B_i) \ \ (i \in I).$$

It suffices to verify $\sum (A \cap B_i) \supseteq A \cap \sum B_i \ \ (i \in I)$, whence we are through by

$$\begin{array}{rl} & x \in A \cap \sum B_i \\ \Longrightarrow & x \in A \ \& \ x \in \sum B_i \ \ (i \in I) \\ \Longrightarrow & x \in A \ \& \ x \geq b_{i_1} \wedge \ldots \wedge b_{i_n} \ \ (\exists b_{i_1} \in B_{i_1}, \ldots, b_{i_n} \in B_{i_n}) \\ \Longrightarrow & x \in (A \cap B_{i_1}) + \ldots + (A \cap B_{i_n}) \\ \Longrightarrow & x \in \sum (A \cap B_i) \ \ (i \in I)\,. \end{array}$$

□

Obviously p-ideals and m-ideals, as well, w. r. t. to d-monoids, and d-ideals, w. r. t. *d-semigroups with* 0, satisfy the *intersection theorem*, that is the condition that the intersection of all some not empty set A containing *"x"-ideals* is again such an x-ideal, in general denoted by A^x and in particular by a^x, if A is a *singleton* $\{a\}$. Thus any not empty $A \subseteq S$ generates a p-ideal A^p and a d-ideal A^d, namely the intersection of all x-ideals, containing A.

On the other hand, these *hulls* admit an "inner description".

In order to construct A^p, first we form all finite joins $a_1 \vee \ldots \vee a_n \in P$ and next we adjoin all elements x lying below some finite join.

In order to construct A^d, starting from an arbitrary non empty set A, we form first all meets of elements of A and next all multiples of such elements.

Hence, p-filters (recall they are d-ideals of $\mathfrak{P}$), p-ideals, and d-ideals are of *finite character*. This means that x is contained in $\sum B_i$ of some *family* $B_i\ (i \in I)$ iff x belongs to the sum of some *finite subfamily* of $B_i\ (i \in I)$.

Furthermore, w. r. t. the complex operations it holds – as is easily checked by applying the distributivity laws from above:

4. 1. 7 Lemma. *The operators d and p satisfy*

$$\begin{array}{rclcrcl} A^p \cdot B^p & = & (AB)^p & \textit{and} & A^d \cdot B^d & = & (AB)^d\,, \\ A^p \cap B^p & = & (A \wedge B)^p & \textit{and} & A^d \cap B^d & = & (A \vee B)^d\,, \\ A^p \vee B^p & = & (A \vee B)^p & \textit{and} & A^d + B^d & = & (A \cup B)^d\,. \end{array}$$

Hence, summarizing we get:

4. 1. 8 Proposition. *In a d-monoid $\mathfrak{S}$ with 0 p-ideals, filters and d-ideals of $\mathfrak{S}$, as well, form respectively algebraic lattice semigroups, in which multiplication and meet distribute over sums.*

PROOF. The difficult part was proven above, the rest my be left to the reader. □

As we shall see, structure properties of the *ideal semigroup* of some d-semigroup $\mathfrak{S}$ are responsible for the *archimedean degree* of $\mathfrak{S}$. This results essentially from the fact that irreducible ideals play a crucial role w. r. t. generating congruences, which will turn out above all in the chapters on *hyperarchimedean* and *representable* d-semigroups.

The subsequent notions will turn out be most fruitful:

4. 1. 9 Definition. Let I be an arbitrary ideal of $\mathfrak{S}$. I is called *archimedean* if it satisfies:

$$\forall\, n \in \mathbf{N} : t^n \in I \implies t \cdot I\,,\, I \cdot t \subseteq I\,.$$

Let F be a filter of $\mathfrak{S}$. F is called *primary*, if it satisfies:

$$ab \in F \;\&\; a, b \notin F \implies \exists n \in \mathbf{N} : a^n, b^n \in F\,.$$

Obviously an irreducible ideal is archimedean iff the corresponding irreducible filter is primary.

4. 1. 10 Definition. Let some ideal (or filter) A be maximal w. r. t. not containing some given element a. Then A is called *regular.*

Let the lattice ideal I be the set theoretical complement of the regular filter F. Then I is called *co-regular.*

Thus *co*-regular ideals are always irreducible and minimal w. r. t. containing a given element a. The importance of regular elements in the theory of *algebraic lattices* $\mathfrak{V}$ on the one hand results from the fact that any regular element is $\bigwedge$-irreducible, and on the other hand it results from the fact that any $a \in V$ is the intersection of regular elements. This will be shown concretely for *c*-ideals, and this will turn out as a fruitful tool in later chapters on *linearity* and *orthogonality*.

4. 1. 11 Definition. Let t be positive. By $C(t)$ we mean the set of all $a \in S$, satisfying in $\mathfrak{S}^1$ the equation $(1 \vee a)(1 \wedge a)^{-1} \leq t^n \ \ (\exists n \in \mathbf{N})$.

Finally we remark w. r. t. representability:

4. 1. 12 Definition. Let A be an ideal, then by ker(A), the *kernel* of A, we mean the set of all $k \in A$ satisfying the implication $s \cdot t \in A \Longrightarrow s \cdot k \cdot t \in A$.

Let A be a filter, then by rad$\,(A)$, the *radical* of A, we mean the set of all $r \in A$ satisfying $r^n \in S \backslash A \ \ (\exists n \in \mathbf{N})$.

Obviously the kernel of an ideal forms always again an ideal and the radical of an filter forms always a filter.

4.2 c-Ideals

Sofar, *lattice-* and *ring-theoretical* notions have dominated, but a pendant of the *convex* subgroup of an ℓ-group has not yet been presented. Let $\mathfrak{G}$ be – even – an ℓ-group. Then a subgroup $\mathfrak{C}$ of $\mathfrak{G}$ is *convex* in $\mathfrak{G}$ iff $\mathfrak{C}$ satisfies:

$$\text{(K)} \qquad |\,x\,| \leq |\,a\,| \ \&\ a \in C \ \Longrightarrow\ x \in C\,.$$

Let $\mathfrak{C}$ be a convex subgroup of $\mathfrak{G}$. Then we get first $|\,a\,| \in C \Longleftrightarrow a \in C$. Let $\mathfrak{C}$ be a convex subgroup, and assume $|\,a\,| \in C$ that is $a \vee a^{-1} \in C$. Then it results $|\,a\,|^{-1} = a^{-1} \wedge a \in C$ and thereby $C \ni a \wedge a^{-1} \leq a \leq a \vee a^{-1} \in C$ implying $a \in C$. Conversely $a \in C \Longrightarrow a \in C \ \&\ a^{-1} \in C \Longrightarrow |\,a\,| \in C$.

Hence it results: $|x| \leq |a|$ & $a \in C \Longrightarrow 1 \leq |x| \leq |a| \in C$.

Let now (K) be satisfied by $\mathfrak{C}$. Then in case of $C \ni a \leq b \leq c \in C$ it follows $c^{-1} \leq b^{-1} \leq a^{-1}$ and hence, by definition, $|b| \leq |a| \vee |c| \leq |a| \cdot |c| \in C$.

The preceding characterization of convex subgroups gives rise to the following

4. 2. 1 Definition. Let $\mathfrak{S}$ be a d-semigroup. By a c-ideal of $\mathfrak{S}$ we mean a subset C of S, closed under multiplication and satisfying in addition:

$$\text{(K)} \qquad |x| \leq |a| \ \& \ a \in C \implies x \in C .$$

By observing $||x|| = |x|$, we get $a \in C \iff |a| \in C$, for if $|a| \in C$ we have $|a| \leq ||a||$ & $|a| \in C \rightsquigarrow a \in C$, and since in case of $a \in C$ we get $||a|| \leq |a|$ & $a \in C \Longrightarrow |a| \in C$.

Next from definition 4.2.1 it follows that any c-ideal A is convex. To realize this, we suppose $A \ni a \leq b \leq c \in A$ and $e(a \wedge b \wedge c) = a \wedge b \wedge c = (a \wedge b \wedge c)e$. There are positive elements x, y, a', b', c' satisfying the equations $(e \wedge a) \cdot x = e \wedge b$ & $(e \wedge b) \cdot y = c$ and $(e \wedge a) \cdot a' = (e \wedge b) \cdot b' = (e \wedge c) \cdot c' = e$. But this leads to $(e \wedge a)xyc' = e$ & $(e \wedge b)yc' = e$, whence we may start from a triple $a^* \geq b^* \geq c^*$ in the role of a', b', c'. Consequently we get $|b| \leq |c| \cdot |a| = ||c| \cdot |a||$. This implies $b \in A$ by condition (K) since $a, c \in A \rightsquigarrow |a|, |c| \in A \rightsquigarrow |c| \cdot |a| \in A$.

Furthermore any c-ideal A of $\mathfrak{S}$ is also a sublattice, because $a, b \in A \Longrightarrow |a \wedge b|, |a \vee b| \leq |a| \vee |b| \leq |a| \cdot |b| = ||a| \cdot |b||$ with $|a| \cdot |b| \in A$.

Finally, if $\mathfrak{S}$ is a monoid then, by definition, 1 belongs to any c-ideal, and if the inverse a^{-1} of a exists, a^{-1} belongs to the c-ideal A if and only if a belongs to A, recall the introduction where we started from $|a| := a \vee a^{-1}$, implying of course $|a| = |a^{-1}|$.

Finally we emphasize: Let $\mathfrak{S}$ be a d-monoid. Then by (K) 1 is contained in any c-ideal of $\mathfrak{S}$. Hence, together with any family of c-ideals also the intersection of this family is again a c-ideal. Consequently any subset A of S generates a uniquely determined c-ideal A^c, in particular any element a generates a uniquely determined $a^c := \{a\}^c$. Moreover, $\emptyset^c = \{1\}$.

Next, since S itself is a c-ideal, we get

4. 2. 2 Proposition. *Let $\mathfrak{S}$ be a d-monoid. Then the set of all c-ideals of $\mathfrak{S}$ forms a complete lattice with respect to $\subseteq$.*

Furthermore, because $a \in C \iff |\,a\,| \in C$, we get by definition

4. 2. 3 Lemma. *Let $\mathfrak{S}$ be a d-semigroup. Then two c-ideals A and B are equal iff their cones A^+ and B^+ are equal.*

This leads next to

4. 2. 4 Proposition. *Let $\mathfrak{S}$ be a d-semigroup and let M be a non empty subset of S. Then M^c is equal to*

$$C(M) := \big\{x \,|\, |\,x\,| \le \prod |\,m_i\,| \ \ (m_i \in M) \ \ (1 \le i \le n)\big\}$$

whence the lattice of all c-ideals is algebraic, *with respect to* $\sum$.

PROOF. Obviously all elements of the given type belong to M^c. Furthermore, according to 2.5.5, M^c is closed with respect to $\wedge, \vee$ and $\cdot$. Finally the implication (K) holds (nearly) by definition. □

In particular, according to the preceding proposition the "sum" $A \vee B$ of two c-ideals is equal to the set of all elements x w. r. t. satisfying $|\,x\,| \le \prod\limits_1^n (a_i^+ \cdot b_i^+)$ $(a_i \in A, b_i \in B)$, since by construction A and B are contained in this set whereas this set forms a sub-d-semigroup of any sup-c-ideal of A and B.

The preceding characterization provides

4. 2. 5 Proposition. *in any d-semigroup the set $C(\mathfrak{S})$ forms a distributive lattice under $\cap$ and $\vee$.*

PROOF. $x \in A \cap (B \vee C) \Longrightarrow |x| \in A \ \&\ |\,x\,| \le \prod\limits_1^n (b_i^+ \cdot c_i^+)\ (\exists b_i \in B, c_i \in C)$. The rest follows by extending and applying (2.19) to finitely many factors. □

Summarizing, so far it has been shown that the family $C(\mathfrak{S})$ of all c-ideals of a given d-monoid forms a distributive algebraic lattice with respect to $\sum$ and $\bigcap$.

Let now $\mathfrak{S}$ be a d-monoid. A c-ideal P is called *prime* if $a \wedge b \in P \Longrightarrow a \in P \bigvee b \in P$. Obviously S itself is a prime c-ideal and together with a chain $\{P_i\}$ $(i \in I)$ of prime c-ideals their intersection D is again a prime c-ideal, since

$$a \wedge b \in D \ \&\ a \notin D \Longrightarrow \exists P_j : a \notin P_j \Longrightarrow b \in D\,.$$

Hence, since by ZORN there exist maximal chains of prime c-ideals, given some c-Ideal M, there exists at least one *minimal prime* c-ideal $P \supseteq M$.

Moreover, nearly by definition, with each chain of c-ideals its union is also a c-ideal. Consequently, since $\{1\}$ is a c-ideal, by ZORN there exist maximal chains of c-ideals not containing $a \neq 1$ and thereby c-ideals M maximal w. r. t. property of not containing a. Such maximal ideals are called *values* of a. These values – say W – are necessarily prime. This is verified as follows:

Recall the proof of (4.1.2)), and let W be a value of a, and assume $x \wedge y \in W$ but $x, y \notin W$. Then in case of $R(x, y, x^\circ, y^\circ)$ it follows $x^\circ, y^\circ \notin W$. But it holds $x^\circ \wedge y^\circ = 1 \in W$. Now consider the set $U := \{u \,|\, x^\circ \wedge |\, u \,| \in W\}$. This set forms a c-ideal as is easily seen, and since y° belongs to U but not to W we get $a \in W \subset U$. Now define $V = \{v \,|\, |\, u \,| \wedge |\, v \,| \ \ (\forall u \in U)\}$. Then by analogy we get $a \in W \subset V$. But this would lead to $a \wedge a = a \in W$, a contradiction. Hence any value is a prime c-ideal.

In later chapters we want to clear the structure of right normal d-semigroups. To this end we introduce *irreducible* and *prime c-ideals* in analogy with irreducible and prime lattice ideals. Observe that, given a c-ideal C, for any $a \notin C$ also the set of all x with $|\, a \,| \wedge |\, x \,| \in C$ forms a c-ideal.

Moreover, not only for elements but also for (quotient) subsets of type $\langle a \rangle * \langle b \rangle + \langle b \rangle * \langle a \rangle$ with $\langle a \rangle * \langle b \rangle := \{x \,|\, ax \geq b\}$ there exist maximal c-ideals K w. r. t. $K \cap \langle a \rangle * \langle b \rangle + \langle b \rangle * \langle a \rangle = \emptyset$, which are in addition prime.

4. 2. 6 Definition. Let $\mathfrak{S}$ be a d- monoid. A filter U is called an *ultrafilter*, if it is maximal w. r. t. not containing 1.

A c-ideal is called *minimal prime*, if it is minimal in the set of all prime c-ideals.

4. 2. 7 Proposition. *The set theoretical complement of a prime ideal is a prime filter and* vice versa.

In $\mathfrak{S}^+$ the set theoretical complement of an ultrafilter is a minimal prime c-ideal and vice versa.

PROOF. The first assertion is nearly obvious.

So, let $\mathfrak{S}$ be positive and U an ultrafilter. Then, by definition, $S \backslash U$ satisfies the implication $x \leq y \notin U \Longrightarrow x \notin U$. But moreover it holds, too,

$$\begin{aligned} a, b \notin U &\Longrightarrow a \wedge x = 1 = b \wedge y \ \ (\exists\, x, y \in U) \\ &\Longrightarrow ab \wedge (ay \wedge xb \wedge xy) = 1 \\ &\Longrightarrow ab \notin U\,. \end{aligned}$$

Hence, the complement of an ultrafilter is a prime c-ideal. Provided now, this c-ideal would properly contain a further prime c-ideal, then this complement had to be a prime filter, properly containing U, a contradiction!

Finally, let M be a *minimal prime c-ideal*. Then the complement F of M is a filter, embedded by ZORN in an ultrafilter U, and $S\backslash U$ is a prime sub-c-ideal of M, and thereby equal to M. This means $F = U$, whence F is an ultrafilter. □

4. 2. 8 Corollary. *In d-monoids the ultrafilters correspond in a unique manner with the minimal prime c-ideals. Precisely:*

$$U \textit{ is an ultrafilter in } \mathfrak{S}^+ \ \textit{ iff } S\backslash U \textit{ is a minimal prime c-ideal in } \mathfrak{S}\,.$$

That any d-monoid contains minimal prime c-ideals, follows nearly immediately from the next proposition, by ZORN.

4. 2. 9 Proposition. *Let $\mathfrak{S}$ be d-monoid and C_i $(i \in I)$ a chain of prime c-ideals of $\mathfrak{S}$. Then intersection and union of these C_i form again prime c-ideals.*

Within the class of prime c-ideals there is a class of special prime c-ideals of most interest, namely the class of $\bigcap$*-prime c-ideals.*

4. 2. 10 Definition. Let $\mathfrak{S}$ be a d-monoid. We call $R \in C(\mathfrak{S})$ $\bigcap$-prime, if R fails to be an *intersection* of of proper sup-c-ideals.

4. 2. 11 Proposition. *Let $\mathfrak{S}$ be a d-monoid. Then $R \in C(\mathfrak{S})$ is $\bigcap$-prime iff there exists some $c \notin R$, belonging to all c-ideals A_i $(i \in I)$, properly containing R.*

PROOF. Let R be $\bigcap$-prime. We form the intersection D of all $A_i \in C(\mathfrak{S})$, properly containing R and choose $c \in D\backslash R$.

Let now c be some element of the required type w.r.t. R. Then c belongs to all c-ideals of $\mathfrak{S}$, which properly contain R, and hence also to their intersection. □

Finally we consider *regular c-ideals*, built by analogy to the regular lattice ideal – recall 10.0.10. This notion will be of great importance in later chapters. Like the notion of a prime ideal, from the abstract point of view it is a notion of *algebraic lattice theory,* observe that these notions are defined merely by lattice operations.[1]

Immediately we get by 4.2.11:

4. 2. 12 Corollary. *Regular c-ideals are exactly the $\bigcap$-irreducible c-ideals.*

As a final result of this section we give:

4. 2. 13 Proposition. *Any c-ideal is equal to some intersection of regular c-ideals.*

PROOF. Recall the proof of 4.2.7. $\square$

Hereafter we intermit our investigation. The study of c-ideals will be taken up again in context with linearity and orthogonality. The concept of this ideal type is crucial, above all in the ℓ-group case.

4.3 v-Ideals and u-Ideals

In a later section we will be concerned with the question, under which conditions a d-semigroup admits a $\bigwedge$-*complete* or a $\bigvee$-*complete extension,* respectively. In this context a special class of d-ideals and a special class of p-ideals will turn out as most relevant tools. This has to do with the fact, that different from the classical case the archimedean property is not strong enough to guarantee an embedding into a complete sup-structure. This is shown by the following example:

Let $\mathbf{E}$ be the unit interval and ω an element, not belonging to $\mathbf{E}$. We put $x+\omega := \omega \ (\forall x \in \mathbf{E})$, $a \circ b := a+b$, in case of $a+b \not> 1$, and $a \circ b := \omega$ otherwise. Then w.r.t. $a \wedge b := \min(a,b)$ $(\mathbf{E}, \omega, \circ, \wedge)$ is a *positive totally ordered d-*semigroup without any $\bigwedge$-complete extension, since in any extension of this type for $X := \mathbf{E} - \{0\}$ it must result:

$$\bigwedge X \circ \bigwedge X = \bigwedge(X \cdot X) = \bigwedge X \rightsquigarrow 1 = 1 \circ \bigwedge X = \bigwedge(1 \circ X) = \omega\,.$$

[1]Since we gave no lattice theoretical introduction here, we will work ad hoc, according to the concrete situations.

As will turn out w. r. t. complete extensions we may restrict our attention to d-monoids with 0. So, for the sake of convenience, let us suppose henceforth this special situation.

4. 3. 1 Definition. Let $\mathfrak{S}$ be a positive d-monoid. $\mathfrak{a}$ is called a *v-ideal* (*Vielfachenideal*), if $\mathfrak{a}$ contains all elements c of S, satisfying

$$s \leq x\mathfrak{a}y \Longrightarrow s \leq xcy\ .$$

The notion of a v-ideal for cancellative monoids goes back to Arnold [4] and van der Waerden [96], the general notion was given by Clifford [41]. But, for the sake of fairness, in the very classical situation of $\mathfrak{Q}$ it had been anticipated already by Richard Dedekind who introduced what is called a cut of $(\mathbf{Q}, \leq, +)$. Consider the right components!

Obviously S itself is always a v-ideal, and in addition it is easily seen, that together with any family of v-ideals also the intersection of this family is a v-ideal, provided there exists a *zero element.* Hence any subset A of S generates a v-ideal A^v which will also be denoted by $\mathfrak{a}$. So, choosing the symbol $\mathfrak{a}$ includes tacitly $\mathfrak{a} = A^v$. In order to emphasize that $\mathfrak{a}$ is a *principal v-ideal*, that is generated by some singleton $\{a\}$, we write – also – a or $\underline{a}$.

Obviously A^v consists of all $c \in S$ with $s \leq uAv \Longrightarrow s \leq ucv$, whence A^v and B^v are equal iff $s \leq uAv \Longleftrightarrow s \leq uBv$. This means in particular $S\mathfrak{a}S \subseteq \mathfrak{a}$ and $a = SaS$.

Let A^v, B^v be two v-ideals of $\mathfrak{S}$. Then A^v and B^v give rise to various operations, one of them the set theoretic meet. Furthermore:

4. 3. 2 Definition. Let $\mathfrak{a} := A^v$, $\mathfrak{b} := B^v$ be two v-ideals of $\mathfrak{S}$. By $\mathfrak{a} \circ \mathfrak{b}$ we mean the v-ideal $(AB)^v$, where AB is the complex product, by $\mathfrak{a} * \mathfrak{b}$ we mean the set of all x with $\mathfrak{a}x \subseteq \mathfrak{b}$, and by $\mathfrak{b} : \mathfrak{a}$ we dually mean the set of all x with $x\mathfrak{a} \subseteq \mathfrak{b}$. Finally we put $\mathfrak{a} + \mathfrak{b} := (A \cup B)^v$.

$\mathfrak{a} \circ \mathfrak{b} =: \mathfrak{a}\mathfrak{b}$, $\mathfrak{a} * \mathfrak{b}$ and $\mathfrak{b} : \mathfrak{a}$ are usually called *ideal product*, and *right* and *left quotient ideal*, respectively, and $\mathfrak{a} + \mathfrak{b} =: \mathfrak{a} \vee \mathfrak{b} = (A, B)^v$ is called the *ideal sum* of $\mathfrak{a}$ and $\mathfrak{b}$.

That these operations are *stable* is seen as follows:

$\mathfrak{a}\mathfrak{b}$ is obviously a v-ideal, and furthermore $\mathfrak{a}\mathfrak{b}$ is uniquely determined, since from $A^v = C^v$ and $B^v = D^v$ it results:

$$s \leq uABv \ \Longrightarrow\ s \leq uCBv \ \Longrightarrow\ s \leq uCDv\ .$$

Next $\mathfrak{a} * \mathfrak{b}$ and $\mathfrak{b} : \mathfrak{a}$ are unique by definition, and they turn out to be v-ideals, because

$$\begin{array}{ccccc} & & s \leq u(\mathfrak{a} * \mathfrak{b})v \Rightarrow s \leq ucv & & \\ & & \Longrightarrow & & \\ s \leq u\mathfrak{b}v \Rightarrow & & s \leq u\mathfrak{a}(\mathfrak{a} * \mathfrak{b})v & & \Rightarrow s \leq u\mathfrak{a}cv \\ & & \Longrightarrow & & \\ & \mathfrak{a}c & \subseteq & \mathfrak{b} & \end{array}$$

and the dual implication.

Obviously v-ideals satisfy axioms (A1) through (A3) and the equations (2.42), (2.43), (2.44), (2.46), and (2.47), given in 2.8.2.

The proof is left to the reader, but we summarize:

4. 3. 3 Proposition. *Let $\mathfrak{S}$ be a positive d-monoid with* 0 *and $\mathfrak{V}$ its v-ideal semigroup. Then it holds*

(A1) $\qquad (\mathfrak{V}, \cap, \circ, +)$ *is a semigroup.*

(V) $\qquad (\mathfrak{V}, \cap, +)$ *is a lattice.*

(A3) $\qquad \mathfrak{x} \circ (\mathfrak{a} + \mathfrak{b}) \circ \mathfrak{y} = \mathfrak{x} \circ \mathfrak{a} \circ \mathfrak{y} + \mathfrak{x} \circ \mathfrak{b} \circ \mathfrak{y}\,.$

(Q1) $\qquad (\mathfrak{a} \circ \mathfrak{b}) * \mathfrak{c} = \mathfrak{b} * (\mathfrak{a} * \mathfrak{c})\,.$

(Q2) $\qquad \mathfrak{a} * (\mathfrak{b} : \mathfrak{c}) = (\mathfrak{a} * \mathfrak{b}) : \mathfrak{c}\,.$

$\mathfrak{V}$ seems to be close to the brick. But in general the implication $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a}\mathfrak{x} = \mathfrak{b} = \mathfrak{y}\mathfrak{a}$ fails to be satisfied. The question, when this is the case, will be settled in a later section. In particular we will be interested in the question when the v-ideal semigroup of a brick is again a brick.

Besides v-ideals so called u-ideals will play a central role. They are defined nearly dually w. r. t. v-ideals.

4. 3. 4 Definition. Let $\mathfrak{S}$ be a positive d-monoid. $\mathcal{A} \subseteq \mathcal{S}$ is called a *u-ideal* (*Teilerideal*), if $\mathcal{A}$ contains all elements c of S, satisfying:

$$x\mathcal{A}y \leq s \Longrightarrow xcy \leq s\ .$$

As mentioned above, v-ideals are special d-ideals and u-ideals are special p-ideals.

Nearly dually w. r. t. v-ideals u-ideals satisfy:

S is a u-ideal and the intersection of a family of u-ideals is again a u-ideal. Hence any subset A of S generates a uniquely determined u-ideal A^u. This provides – on the one hand – for any pair of u-ideals a uniquely determined $A^u \vee B^u := (A \cup B)^u$ and on the other hand it provides the possibility of a u-ideal multiplication. Observe: $A^u = C^u$ & $B^u = D^u \Longrightarrow (AB)^u = (CD)^u$. So we may define $A^u \circ B^u := (AB)^u$.

Furthermore, assuming $\mathcal{X} := X^u$ in case of $\mathcal{A} \subseteq \mathcal{B}$ the set of all x with $A \cdot x \subseteq \mathcal{B}$ forms a u-ideal, which we will call the *right quotient ideal* $\mathcal{A} \nearrow \mathcal{B}$ of $\mathcal{A}$ w. r. t. $\mathcal{B}$ (and, of course, the *left quotient ideal* $\mathcal{A} \nwarrow \mathcal{B}$ is defined dually).

Obviously the quotient operations extend to arbitrary pairs $\mathcal{A}$, $\mathcal{B}$ of u-ideals by forming $\mathcal{A} \nearrow \mathcal{B} := \mathcal{A} \nearrow \mathcal{A} \vee \mathcal{B}$.

One advantage of v- and u-ideals is the fact that they provide *cancellative stable extensions* (if $\mathfrak{S}$ is cancellative).

Furthermore the semigroup of principal ideals $\{a\}^v =: \underline{a}$ and $\{a\}^u =: \overline{a}$, respectively, – recall $\{a\}^v = \{x \mid a \leq x\}$ and $\{a\}^u = \{x \mid x \leq a\}$ – is isomorphic with $(S, \cdot, \wedge, \vee)$ w. r. t. $\cdot, \wedge, \vee$ and it is easily checked that $\underline{a}$ is a cancellable v-ideal and $\overline{a}$ a cancellable u-ideal, respectively, if a is cancellative in $\mathfrak{S}$. This means – according to the preceding development – that the v-ideal semigroup is a $\bigwedge$-complete extension if $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \mid \mathfrak{b}$ is satisfied, while the u-ideal semigroup is a $\bigvee$-complete extension of $\mathfrak{S}$ if $\mathcal{A} \subseteq \mathcal{B} \Longrightarrow \mathcal{A} \mid \mathcal{B}$ is satisfied. Here $\mid$ means right/left divisibility.

But, in any case, each of these extensions provides a complete sup-lattice-monoid, which is $\bigwedge$-distributive in the v-case and $\bigvee$-distributive in the u-case.

Chapter 5

Congruences

In this chapter we exhibit (*left*) *congruences,*which will prove most relevant for the further theory. We start with some canonical extension theorems and then turn to representation theorems. Finally we consider subdirectly irreducible d-semigroups.

5.1 Extensions

5. 1. 1 Lemma. *Homomorphic images $\overline{\mathfrak{S}}$ of d-semigroups are again d-semigroups.*

PROOF. Obviously $\overline{\mathfrak{S}}$ satisfies (A1) through (A3). But axiom (A4) holds as well, according to: $\overline{a} \leq \overline{b} \Longrightarrow \overline{a} = \overline{a} \wedge \overline{b} \Longrightarrow \overline{b} = (\overline{a} \wedge \overline{b})\overline{x} \ (\exists x)$. The rest follows by duality. $\square$

Next we give some extension principles.

5. 1. 2 Proposition. *Let $\mathfrak{S}$ be a d-semigroup. If $\equiv_p$ is a congruence on $\mathfrak{P}$, then $\equiv_p$ extends uniquely from $\mathfrak{P}$ to $\mathfrak{S}$ via:*

(i)
$$\begin{aligned} a \equiv b \ :\Longleftrightarrow\ & \exists\, x, y \in S\,, a_\circ, b_\circ \in P\ : a_\circ \equiv_p b_\circ \\ \& \quad & a = x \cdot a_\circ \cdot y \ \&\ b = x \cdot b_\circ \cdot y\,, \end{aligned}$$

or equivalently:

(ii)
$$\begin{aligned} a \equiv b \ :\Longleftrightarrow\ & \exists\, x, y \in S\,, a_\circ b_\circ\,, e \in P:\ (x \wedge a_\circ \wedge b_\circ \wedge y) = \\ & = e \cdot (x \wedge a_\circ \wedge b_\circ \wedge y) = (x \wedge a_\circ \wedge b_\circ \wedge y) \cdot e \\ \& \quad & a = (e \wedge x) \cdot a_\circ \cdot (e \wedge y) \\ \& \quad & b = (e \wedge x) \cdot b_\circ \cdot (e \wedge y)\,. \end{aligned}$$

PROOF. First we show $(i) \iff (ii)$.

$(ii) \Longrightarrow (i)$ holds by definition.

$(i) \Longrightarrow (ii)$: Let $e \in P$ be a unit of $x \wedge a_\circ \wedge b_\circ \wedge y$. Then by 2.2.3 we get:

$$\begin{aligned} x \cdot a_\circ \cdot y &= (e \wedge x)(e \vee x) \cdot a_\circ \cdot (e \vee y)(e \wedge y) \\ x \cdot b_\circ \cdot y &= (e \wedge x)(e \vee x) \cdot b_\circ \cdot (e \vee y)(e \wedge y) \end{aligned}$$

where $$(e \vee x) \cdot a_\circ \cdot (e \vee y) \equiv_p (e \vee x) \cdot b_\circ \cdot (e \vee y)\,.$$

Hereafter we may continue as follows:

First of all $\equiv$ is *reflexive* and *symmetric* by definition.

Next $\equiv$ is *transitive.* Suppose:

$$\begin{aligned} a &= (e \wedge x) \cdot a' \cdot (e \wedge y) \quad \& \quad b = (e \wedge x) \cdot b' \cdot (e \wedge y) \\ c &= (f \wedge u) \cdot c'' \cdot (f \wedge v) \quad \& \quad b = (f \wedge u) \cdot b'' \cdot (f \wedge v)\,. \end{aligned}$$

We may assume $e = f$ and in addition that $e\ (= f)$ is a unit of the meet $a' \wedge b' \wedge b'' \wedge c''$. This implies that suitable elements $p, q, r, s \in P$ satisfy:

$$\begin{aligned} a &= (e \wedge x \wedge u)p \cdot a' \cdot q(e \wedge y \wedge v) \\ b &= (e \wedge x \wedge u)p \cdot b' \cdot q(e \wedge y \wedge v) \\ b &= (e \wedge x \wedge u)r \cdot b'' \cdot s(e \wedge y \wedge v) \\ c &= (e \wedge x \wedge u)r \cdot c'' \cdot s(e \wedge y \wedge v) \\ &\leadsto \\ pa'q \equiv_p pb'q &= r \cdot b'' \cdot s \equiv_p rc''s\,, \end{aligned}$$

meaning $a \equiv c$. Hence $\equiv$ is also transitive.

Furthermore, by $(i) \iff (ii)$, $\equiv$ respects multiplication, because

$$\begin{array}{ccccc} a = xa_\circ y & & as = xa_\circ(ys) & & sa = (sx)a_\circ y \\ & \Longrightarrow & & \& & \\ b = xb_\circ y & & bs = xb_\circ(ys) & & sb = (sx)b_\circ y\,. \end{array}$$

It remains to verify

$$a \equiv b \Longrightarrow s \wedge a \equiv s \wedge b$$

To this end let $a \equiv b$ be defined in the sense of (ii) with a unit e of s, that is $es = s = se$.

Then there exist positive elements e', e'' with $(e \wedge x)e' = e = e''(e \wedge y)$. We put $\bar{s} := e' \cdot s \cdot e''$, and $s' := e \vee \bar{s}$. Then it results:

$$
\begin{aligned}
s &= (e \wedge x)\bar{s}(e \wedge y) \\
&= (e \wedge x)(e \wedge \bar{s})(e \vee \bar{s})(e \wedge y) \\
&= (e^2 \wedge e\bar{s} \wedge xe \wedge x\bar{s})(e \vee \bar{s})(e \wedge y) \\
&= (e \cdot e \wedge e\bar{s} \cdot e \wedge x \cdot e \wedge x\bar{s} \cdot e)(e \vee \bar{s})(e \wedge y) \\
&= ((e \wedge e\bar{s} \wedge x \wedge x\bar{s}) \cdot e \cdot (e \vee \bar{s})(e \wedge y) \\
&= (e \wedge z)s'(e \wedge y)
\end{aligned} \tag{5.3}
$$

with $z = e\bar{s} \wedge x \wedge x\bar{s}$ – recall $e(e \vee \bar{s}) = e \vee \bar{s}$.

In case of $(e \wedge z)r = e \wedge x$ with $r \in P$ for $r \cdot a_\circ \equiv_p r \cdot b_\circ$ this implies further:

$$
\begin{aligned}
a &= (e \wedge z)(r \cdot a_\circ)(e \wedge y) \\
\& \quad b &= (e \wedge z)(r \cdot b_\circ)(e \wedge y)\,,
\end{aligned}
$$

and consequently by applying (5.3) we get

$$
\begin{aligned}
s \wedge a &= (e \wedge z)(s' \wedge r \cdot a_\circ)(e \wedge y) \\
s \wedge b &= (e \wedge z)(s' \wedge r \cdot b_\circ)(e \wedge y)\,.
\end{aligned}
$$

But $s' \wedge r \cdot b_\circ$ is positive, since the components are positive, recall e is a unit of s and thereby of $\bar{s}$ and s', too. Moreover e is unit of $z\,, y$ and the inner components, as well.

Consequently, altogether, $\equiv$ respects $\wedge$, too. □

5. 1. 3 Lemma. *Let $\mathfrak{S}$ be a d-semigroup. If $\equiv$ is a congruence on $\mathfrak{S}$, then $\equiv$ extends uniquely from $\mathfrak{S}$ to $\mathfrak{S}^1$ via:*

$$\alpha \equiv_1 \beta \;:\Longleftrightarrow\; x \cdot \alpha \cdot y \;\equiv\; x \cdot \beta \cdot y \quad (\forall\, x, y \in S)\,.$$

PROOF. Observe $\alpha \in S^1 \Longrightarrow x\alpha, \alpha x \in S$ and axiom (A3). □

5. 1. 4 Corollary. *Let $\mathfrak{S}$ be a d-semigroup. If the congruence σ , ρ generate a subdirect decomposition of $\mathfrak{S}$, then their extensions σ_1 , ρ_1 provide a subdirect decomposition of $\mathfrak{S}^1$.*

5. 1. 5 Lemma. *Let $\mathfrak{S}$ be a d-semigroup. If $\equiv_1$ is a congruence on $\mathfrak{S}^1$, then $\equiv_1$ extends uniquely from $\mathfrak{S}^1$ to $\mathfrak{Q}$ via:*

$$\alpha \equiv_{_Q} \beta \;:\Longleftrightarrow\; x \cdot \alpha \cdot y \equiv_1 x \cdot \beta \cdot y \quad (\exists\, x, y \in C^{1+})\,.$$

PROOF. Recall first that $\alpha\,,\ \beta \in S^1$ implies $x\cdot\alpha\,,\ \beta\cdot y \in S^1$ and thereby $x\cdot\alpha\cdot y\,,\ x\cdot\beta\cdot y \in S^1$. We now turn to the proof:

Obviously it suffices to show that the relation, defined above, is a congruence relation.

By definition $\equiv_Q$ is reflexive and symmetric. Furthermore $\equiv_Q$ is transitive, since in case of positive and cancellable elements x, y, u, v we get:

$$\begin{array}{ccc} x\alpha y \equiv_1 x\beta y & \& & u\beta v \equiv_1 u\gamma v \\ & \Longrightarrow & \\ (x \vee u)\alpha(y \vee v) & \equiv_1 & (x \vee u)\beta(y \vee v)\,. \end{array}$$

Hence $\equiv_Q$ is an equivalence relation. But moreover, $\equiv_Q$ is even a congruence relation:

We start from some $\gamma = uv^{-1}$, where in particular v is positive and cancellable. Then it results:

$$\begin{array}{lcccc} & x\alpha y \equiv_1 x\beta y & \Longrightarrow & x(\alpha uv^{-1})vy & \equiv_1 \ x(\beta\,\cdot\,uv^{-1})vy \\ \text{and} & x\alpha y \equiv_1 x\beta y & \Longrightarrow & x(\alpha \wedge uv^{-1})vy & \equiv_1 \ x(\beta \wedge uv^{-1})vy\,. \end{array}$$

□

5. 1. 6 Corollary. *Let $\mathfrak{S}$ be a d-semigroup and let $\sigma_1\,,\ \rho_1$ provide a subdirect decomposition of $\mathfrak{S}^1$. Then $\sigma_Q\,,\ \rho_Q$ provide a subdirect decomposition of $\mathfrak{Q}$.*

Before continuing by the study of (most) concrete congruences we give one result on *left congruences.* Here by a left congruence we mean an equivalence, satisfying moreover:

$$\begin{array}{lccc} & a\ \theta\ b & \Longrightarrow & sa\ \theta\ sb \\ \text{and} & a\ \theta\ b & \Longrightarrow & s \wedge a\ \theta\ s \wedge b\,. \end{array}$$

Any left congruence on $\mathfrak{S}$ is, of course, a congruence on $(S, \wedge)$, but moreover we get:

5. 1. 7 Lemma. *Let $\mathfrak{S}$ be a d-semigroup. If $\equiv$ is a left congruence on $(S, \cdot, \wedge)$ and thereby a congruence on the semilattice $(S, \wedge)$, then $\equiv$ is even a congruence on the lattice $(S, \wedge, \vee)$.*

PROOF. First of all, choosing some suitable element b'', we get:

$$b \equiv a \vee b \Longrightarrow a \wedge b \equiv a \Longrightarrow b''(a \wedge b) \equiv b''a \Longrightarrow b \equiv a \vee b$$

and thereby $\overline{a} \leq \overline{b} \Longleftrightarrow a \equiv a \wedge b \Longleftrightarrow b \equiv a \vee b$. Hence it holds $\overline{a}, \overline{b} \leq \overline{a \vee b}$. So it suffices to verify: $\overline{a} \leq \overline{c}\ \&\ \overline{b} \leq \overline{c} \implies \overline{a \vee b} \leq \overline{c}$. But by

$$a \equiv b\ \&\ a = a''(a \wedge b) \Longrightarrow a \vee b = a''b \equiv a''(a \wedge b) = a$$

we get:

$$c \equiv a \vee c \equiv b \vee c \Longrightarrow a \vee (b \vee c) = (a \vee b) \vee (a \vee c) \equiv a \vee c \equiv c\,,$$

that is $\overline{a \vee b} \leq \overline{c}$. □

5.2 Concrete Congruences

In ℓ-groups congruences correspond uniquely to *convex normal divisors.* A similar correspondence does, of course, not hold in general, consider d-lattices. In spite of this there are particular congruences, providing fruitful insights, and, of course, these congruences are congruences as well in case of ℓ-groups, although not defined by normal divisors. In particular there are three *ideal oriented* congruences which will contribute essentially to clearing the d-semigroup structure. First of all three results, which are easily checked.

5. 2. 1 Proposition. *Let $\mathfrak{S}$ be a d-semigroup and let I be an m-Ideal of $\mathfrak{S}$. Then*

$$a \equiv b\ (I) \ :\Longleftrightarrow\ \exists\, e, f \in I : a \leq be\ \&\ b \leq af$$

defines a left congruence on $\mathfrak{S}$, which in case of $s \cdot I = I \cdot s$ is even a congruence.

5. 2. 2 Proposition. *Let $\mathfrak{S}$ be a d-semigroup and let C be a c-ideal of $\mathfrak{S}$. Then*

$$a \equiv b\ (C) \ :\Longleftrightarrow\ \exists\, e, f \in C : a \leq be\ \&\ b \leq af$$

defines a left congruence on $\mathfrak{S}$, which in case of $s \cdot C = C \cdot s$ is even a congruence.[1]

5. 2. 3 Corollary. *$a \equiv b$ according to 5.1.3 or 5.2.2 is equivalent to $ae = bf\ \ (e, f \in I, C)$,*

[1]Recall $a \leq be \Rightarrow ax = be\ \ (x \in S^+) \Rightarrow af = be\ \ (f = x \wedge e \in C)$. Similarly we would succeed below 5.2.1.

SINCE $a \leq be \;\&\; b \leq af \Longrightarrow ax = be \leq afe \Longrightarrow ax = a(x \wedge fe)\,.$

5. 2. 4 Proposition. *Let $\mathfrak{S}$ be a d-semigroup and let $\mathfrak{i}$ be a d-ideal of $\mathfrak{S}$. Then*

$$a \equiv b\ (\mathfrak{i}) \ \ :\Longleftrightarrow\ \ \exists x \in \mathfrak{i}\,:\, a \wedge x = b \wedge x$$

defines a congruence on $\mathfrak{S}$.

Apart from the particular substructures, presented sofar, there are interesting congruences, generated by subsets.

5. 2. 5 Lemma. *Let $\mathfrak{S}$ be a d-semigroup and let U be an arbitrary filter of $\mathfrak{S}$. Then*

$$a \equiv_U b \ \ :\Longleftrightarrow\ \ a \cdot U = b \cdot U$$

defines a left congruence on $\mathfrak{S}$, which in case of $s \cdot U = U \cdot s$ $(\forall s \in S)$ is even a congruence.

5. 2. 6 Proposition. *Let $\mathfrak{S}$ be a d-semigroup and let θ be a left congruence on $\mathfrak{S}$. Then*

$$a \equiv_\theta b \ \ :\Longleftrightarrow\ \ a \cdot \overline{x} = b \cdot \overline{x}\ \ (\forall\, \overline{x} \in S/\theta)$$

defines a congruence relation on $\mathfrak{S}$.

Suppose $u = u^2$. Then the set of all $x \leq u$ forms a p-ideal and the set $S \cdot u$ forms a d-ideal. Hence – according to 5.2.4 and 5.2.5 – any idempotent element provides two canonical congruences, denoted by σ_u and π_u. But, there holds much more.

5. 2. 7 Proposition. *Let $\mathfrak{S}$ be a d-semigroup and let $u \in S$ be idempotent. Then $(\sigma_u\,,\,\pi_u)$ with*

$$\begin{aligned} a\ \sigma_u\ b \ \ &:\Longleftrightarrow\ \ \exists\, su : a \wedge su = b \wedge su \\ a\ \pi_u\ b \ \ &:\Longleftrightarrow\ \ au = bu \end{aligned}$$

define a congruence pair generating a subdirect decomposition $(S/\sigma_u)\otimes(S/\pi_u)$ of $\mathfrak{S}$.

PROOF. The congruence character of σ_u and π_u follows from the results developed so far and from the fact that idempotents are *central.* Furthermore we get:

$$\begin{array}{rcl} a \wedge su & = & b \wedge su \\ & \& & \\ au & = & bu \end{array} \quad \Longrightarrow \quad \begin{array}{rcl} su \wedge a & = & su \wedge b \\ & \& & \\ su \vee a & = & su \vee b\,. \end{array}$$

Observe: by $su \leq su \vee x$ it holds $su \vee a = u(su \vee a) = u(su \vee b) = su \vee b$. This leads to the assertion since the lattice $(S, \wedge, \vee)$ is distributive. $\square$

Furthermore, as an immediate consequence of (2.19) we get

5. 2. 8 Lemma. *Let $\mathfrak{S}$ be a positive d-semigroup. Then $a \equiv_x b :\Longleftrightarrow x \wedge a = x \wedge b$ is a congruence relation.*

Provided, $\mathfrak{S}$ is even complementary, things change, of course, but also in this case it holds:

5. 2. 9 Lemma. *Let $\mathfrak{S}$ be a complementary d-semigroup. Then $a \longmapsto u \cdot a$ provides a homomorphism also w. r. t. residuation.*

PROOF. $(au) \cdot (xu) \geq bu \Longrightarrow a \cdot xu \geq b$ and $au \cdot (a * b)u \geq bu.$ $\square$

5.3 Finest Congruences

In this section we are concerned with *finest congruence relations,* this topic will be taken up again under 17.2.7. In particular we will characterize the *finest cancellative* congruence and *the finest idempotent* congruence. This will enable us to characterize the subdirect products of cancellative and idempotent d-semigroups.

In this context positive elements play a central role. Hence, recall again that positive means $a = a^+$.

5. 3. 1 Proposition. *Let $\mathfrak{S}$ be a d-semigroup. Then the finest cancellative congruence on $\mathfrak{S}$ is characterized by:*

$$a \,\kappa\, b \;:\Longleftrightarrow\; \exists\, x \in S : xax = xbx\,.$$

PROOF. First of all we see that the relation κ is equivalent to $\exists x, y : xay = xby$ and also with $\exists x^+ : x^+ax^+ = x^+bx^+$, multiply one time to $x \vee y$, and another time to x^+.

This provides immediately that κ is cancellative, and we see furthermore that there are no finer cancellative congruences than κ, if κ, at all, is a congruence relation.

We see that κ is reflexive and symmetric by definition and also without any problem we verify transitivity of κ by multiplying.

So, it remains to verify that κ respects the operations $\cdot$ and $\wedge$. But the latter requirement follows immediately. So we may restrict ourselves to multiplication.

To this end we suppose $a\,\kappa\,b$ and consider as and bs. Supposing that e is a common positive unit of s and x, we start from $x^+ax^+ = x^+bx^+$ and decompose s into $(e \vee s)(e \wedge s)$. Let now $(e \wedge s)e^* = e$ be satisfied. Then there exists some positive u satisfying $x^+u = e^*x^+$. And this implies:

$$\begin{aligned} x^+asx^+u &= x^+as^+(e \wedge s)x^+u \\ &= x^+as^+(e \wedge s)e^*x^+ \\ &= x^+as^+ex^+ \\ &= x^+ax^+t \ \ (\exists\ t) \\ &= x^+bx^+t \\ &= x^+bsx^+u\,. \end{aligned}$$

□

In addition the preceding proof provides:

5. 3. 2 Corollary. *Let $\mathfrak{S}$ be a positive d-semigroup. Then we get the finest congruence under which x becomes cancellable is κ, defined by the equivalence $a\,\kappa_x\,b :\Longleftrightarrow xax = xbx$, and the finest congruence under which all elements of a given $\cdot$ - and $\vee$ - closed subset $X \subseteq S$ are cancellable is κ, defined by the equivalence $a\,\kappa_X\,b :\Longleftrightarrow xax = xbx \ \ (\exists x \in X)$.*

This remark will be of interest whenever we will try to restore cancellation property as well as possible. We now turn to *archimedean congruences.*

5. 3. 3 Definition. Let $\mathfrak{S}$ be a d-semigroup. Two elements a, b are called *archimedean equivalent*, symbolized by $a \approx b$, if there exists a suitable exponent $n \in \mathbf{N}$ satisfying $a \leq b^n$ & $b \leq a^n$.

5. 3. 4 Lemma. *Let $\mathfrak{S}$ be a positive d-semigroup. Then $\approx$ is the finest idempotent congruence on $\mathfrak{S}$.*

PROOF. *Straightforward(ly).* $\square$

5. 3. 5 Lemma. *Let $\mathfrak{S}$ be a d-semigroup and let $\equiv$ be a congruence generating an idempotent $\mathfrak{P}/\!\equiv$. Then also $\overline{\mathfrak{S}} := \mathfrak{S}/\!\equiv$ is idempotent.*

PROOF. Assuming $ea = a = ae$ we get $a = (e \wedge a)(e \vee a)$ and $ax = e \vee a$ $(x \in P)$. Then it results $\bar{x}^2 = \bar{x}$, and thereby $(\overline{e \vee a})\bar{x} = \overline{e \vee a}$, leading to $\bar{a}\bar{x} = \bar{a} = \bar{e} \vee \bar{a}$, whence $\bar{a}$ is positive, satisfying $\bar{a} \cdot \bar{a} = \bar{a}$. $\square$

5. 3. 6 Proposition. *Let $\mathfrak{S}$ be a d-semigroup. Then the congruence $\equiv$, generated on $\mathfrak{S}$ by $\approx$, is the finest idempotent congruence on $\mathfrak{S}$, whence $\mathfrak{S}/\!\equiv$ is the largest idempotent homomorphic image of $\mathfrak{S}$.*

PROOF. According to 5.3.4 and 5.3.5 the image $\mathfrak{S}/\!\equiv$ is idempotent. Consider now another idempotent image S/η and let e be a positive unit of $a \wedge b$. Then with $e''(e \wedge a) = e = (e \wedge b)e'$ it follows:

$$\begin{aligned} a\,\eta\,b &\Longrightarrow (e \wedge a)(e \wedge a)(e \vee a)(e \wedge b)\,\eta\,(e \wedge a)(e \vee b)(e \wedge b)(e \wedge b) \\ &\Longrightarrow (e \wedge a)(e \wedge a)(e \vee a)(e \wedge b) \equiv (e \wedge a)(e \vee b)(e \wedge b)(e \wedge b) \\ &\Longrightarrow e''(e \wedge a)(e \wedge a)(e \vee a)(e \wedge b)e' \equiv e''(e \wedge a)(e \vee b)(e \wedge b)(e \wedge b)e' \\ &\Longrightarrow a \equiv b\,. \end{aligned}$$

$\square$

5. 3. 7 Proposition. *Let $\mathfrak{S}$ be a d-semigroup. Then $\mathfrak{S}$ is a subdirect product of some cancellative and some idempotent d-semigroup iff it satisfies $\kappa \cap \eta = \iota$.*

We want to simplify 5.3.7. To this end we give:

5. 3. 8 Lemma. *Let $\mathfrak{S}$ be a d-monoid. Then $\kappa \cap \eta = \iota$ holds in $\mathfrak{S}$ if and only if $\kappa \cap \eta = \iota$ holds in $\mathfrak{P}$.*

PROOF. Put $a^* := (1 \wedge a)^{-1}$ & $b^* := (1 \wedge b)^{-1}$, then any congruence $\equiv$ fulfills $a \equiv b \Longleftrightarrow a^+ \equiv b^+$ & $a^* \equiv b^*$. $\square$

5. 3. 9 Lemma. *Let $\mathfrak{S}$ be a d-semigroup. Then $\kappa \cap \eta = \iota$ is satisfied in $\mathfrak{S}$ if and only if $\kappa \cap \eta = \iota$ is satisfied in $\mathfrak{S}^1$.*

PROOF. Let $\alpha, \beta \in \Sigma^+$ satisfy $\alpha \approx \beta$ and suppose $\gamma\alpha\delta = \gamma\beta\delta$. Then together with e also $e\gamma =: s$ and $\delta e =: t$ belong to S and any $u \in S^+$ satisfies $su = vs$ $(\exists v \in S)$. This leads to $s \cdot u\alpha \cdot t = s \cdot u\beta \cdot t$ and to $u\alpha \approx u\beta$, and thereby to $u\alpha = u\beta$ $(\forall\, u \in S^+)$. This completes the proof, recall lemma 3.1. 10. □

Next we show:

5. 3. 10 Proposition. *Let $\mathfrak{S}$ be a d-semigroup. Then $\mathfrak{S}$ is a* subdirect product *of some cancellative and some idempotent* d-semigroup *iff:*

$$\begin{array}{rcl} (a^+ \wedge b^+)^n \geq a^+ \vee b^+ & \& & s(a^+ \wedge b^+)t = s(a^+ \vee b^+)t \\ & \Rightarrow & \\ a^+ & = & b^+\,. \end{array}$$

PROOF.
$$\begin{array}{rcl} (a^+ \wedge b^+)^n \geq a^+ \vee b^+ & \Longrightarrow & (a^+)^n \geq b^+ \;\&\; (b^+)^n \geq a^+ \\ & \Longrightarrow & a^+ \,\eta\, b^+ \\ & \& & \\ s(a^+ \wedge b^+)t = s(a^+ \vee b^+)t & \Longrightarrow & sa^+t = sb^+t\,, \\ & \Longrightarrow & a^+ \,\kappa\, b^+\,. \end{array}$$
□

5.4 Subdirectly irreducible d-semigroups

In later chapters on *representable* and *hyper-archimedean* d-semigroups *subdirectly irreducible* d-semigroups will play a central role. There is only little known about subdirectly irreducible d-semigroups in general but in the finite case things are more convenient.

First of all we recall the proposition 5.2.7 and get:

5. 4. 1 Proposition. *Any subdirectly irreducible d-semigroup $\mathfrak{S}$ has at most two idempotents.*

PROOF. Let a, b be a critical pair.

CASE 1. There exists some $u = u^2$ satisfying $ua \neq ub$. Then $u =: 1$ is the identity element of $\mathfrak{S}$.

Suppose now $v^2 = v$. Then v generates a subdirect decomposition of $\mathfrak{S}$, but since $\mathfrak{S}$ is subdirectly irreducible, one of the two factors must collapse, and this must be $\mathfrak{S}/\phi_u$, since this factor doesn't separate a and b.

So we get $sv = v \ \ (\forall s \in S)$, that is $v = 0$. $\square$

Observe that the preceding proposition has various applications, in particular for inverse and for locally finite (any $\{a^n \mid (n \in Z)\}$ is finite), *d*-semigroups, as will be elaborated later on.

For the sake of generality we continue by studying arbitrary *cdl*-semigroup.

5. 4. 2 Definition. Let $\mathfrak{S}$ be a *cdl*-semigroup and let θ be a *left congruence*. Then by a *critical pair* w. r. t. θ we mean any a, b which is separated by θ but collapses w. r. t. any proper subcongruence of θ.

Of course, in lattice ordered structures a, b is a critical pair iff $a \wedge b$, $a \vee b$ is a critical pair. Hence we may always start from $a < b$.

5. 4. 3 Proposition. *Let $\mathfrak{S}$ be a cdl-semigroup (cdl-semigroup) and let $\mathfrak{S}/\theta$ be subdirectly irreducible. Then θ is generated by an irreducible filter and thereby dually by an irreducible ideal.*

PROOF. Let $\overline{a} < \overline{b}$ be a critical pair. We choose some regular filter $\overline{F}$ of $\overline{\mathfrak{S}} := \mathfrak{S}/\theta$, *containing* $\overline{b}$, but avoiding $\overline{a}$, with inverse image F in $\mathfrak{S}$. Then F is irreducible in $\mathfrak{S}$, since $\overline{F}$ is regular in $\overline{\mathfrak{S}}$. Furthermore

$$\begin{aligned} \overline{x} \equiv \overline{y} &\iff \overline{s} \cdot \overline{x} \cdot \overline{t} \in \overline{F} \\ &\iff \overline{s} \cdot \overline{y} \cdot \overline{t} \in \overline{F} \end{aligned}$$

defines a congruence relation on $\overline{\mathfrak{S}}$, which is the diagonal since $\overline{\mathfrak{S}}$ is subdirectly irreducible. On the other hand it holds

$$\begin{array}{rcl} \overline{s} \cdot \overline{x} \cdot \overline{t} \in \overline{F} & \iff & \overline{s} \cdot \overline{y} \cdot \overline{t} \in \overline{F} \\ & \iff & \\ s \cdot x \cdot t \in F & \iff & s \cdot y \cdot t \in F \\ & \rightsquigarrow & \\ x \ \theta \ y & \iff & x \equiv y \ (F). \end{array}$$ $\square$

We now turn to the positive case:

5. 4. 4 Proposition. *Let $\mathfrak{S}$ be a positive subdirectly irreducible cdl-semigroup. Then $\mathfrak{S}$ contains a maximum* 0 *and a uniquely determined hyper-atom (co-atom) h, which together with* 0 *forms a critical pair.*

PROOF. Let $h < b$ be a critical pair. Then it holds:

$$x < b \;\&\; x \not\leq h \implies x \wedge h < x = x \wedge b\,,$$

whence h and b are separated according to 5.2.8. So, b must have the zero property and it must hold $x < b \Longrightarrow x \leq h$. □

Applying 5.4.4 in the d-semigroup case we get:

5. 4. 5 Proposition. *Let $\mathfrak{S}$ be a positive subdirectly irreducible d-semigroup. Then $\mathfrak{S}$ is a normal d-monoid, and the set R of right units of the hyperatom h and the set L of left units of h, as well, form prime c-ideals.*

PROOF. Because $hx = h \vee hx = 0$ it is easily seen that R, and dually L, form prime c-ideals.

Furthermore, since any right unit e of h generates an h, 0 separating congruence, namely $x \equiv y \Longleftrightarrow xe = ye$, and since any right cancellative c satisfies $hc \neq 0c$, which leads to $hc = h$, we see that any right unit e of h is right cancellable and that conversely any right cancellable element is a right unit of h.

So, any unit e of h is cancellable,whence $\mathfrak{S}$ is even a monoid.

Consequently the proof is complete if $\mathfrak{S}$ is linearly ordered, since any linearly ordered d-monoid is normal. Otherwise let the elements u and v be incomparable and suppose

$$\begin{gathered} u, v \leq a\,,\ (u \wedge v)u' = u, (u \wedge v)v' = v, \\ u^*(u' \wedge v') = u'\,,\ v^*(u' \wedge v') = v'\,. \end{gathered}$$

Then it results: $$(u^* \wedge v^*)(u' \wedge v') = u' \wedge v'$$

with $(u \wedge v)u^* = (u \wedge v)u^*(u' \wedge v') = u$ and $(u \wedge v)v^* = v$, by duality. Consequently $u^* \wedge v^* \in L \cap R$. This means $u^* \wedge v^* = 1$. So, again by duality, $\mathfrak{S}$ is normal also in the second case. □

Now we are in the position to prove:

5. 4. 6 Proposition. *Any d-semigroup $\mathfrak{S}$ admits an embedding in a normal d-monoid.*

PROOF. We extend $\mathfrak{S}$ to $\mathfrak{S}^1$ and decompose $\mathfrak{S}^{1^+}$ subdirectly into subdirectly irreducible components. These components are normal, hence also their direct product Δ is normal.

However, it might be that cancellable elements of $\mathfrak{S}$ are no longer cancellable in Δ.

We overcome this situation by changing to a homomorphic image $\overline{\Delta} := \Delta/{\equiv_C}$ with $a \equiv_C b :\Longleftrightarrow \exists c \in C \subseteq S \, : \, c \cdot \alpha \cdot c = c \cdot \beta \cdot c$. As Δ is positive $\equiv_C$ is a congruence, which is easily seen, making all elements of $\mathfrak{S}$ cancellable in $\overline{\Delta}$ and separating any $a \neq b$ of S, as is easily seen. Consequently the quotient hull of $\overline{\Delta}$ verifies our assertion, by

$$(c^{-1}a \wedge c^{-1}b)x = c^{-1}b \Longleftrightarrow (a \wedge b)x = b\,.$$

Thus the proof is complete. □

5. 4. 7 Definition. Given a positive subdirectly d-semigroup $\mathfrak{S}$ with hyperatom h, henceforth we will write $R(h) := R$ and $L(h) := L$, and $E(h) := R(h) \cap L(H)$.

Below 5.4.3 it was shown that subdirectly irreducible images of *cdl*-semigroups are generated by regular filters. In the positive case we even obtain:

5. 4. 8 Proposition. *Let $\mathfrak{S}$ be a positive cdl-semigroup. Then the subdirectly irreducible homomorphic images of $\mathfrak{S}$ correspond uniquely with the regular filters of $\mathfrak{S}$ and thereby* a fortiori *also with the co-regular ideals.*

PROOF. We have – still – to show that regular filters generate a subdirectly irreducible image. So, let J be *co*-regular w. r. t. h and let b be not contained in J. Then $\overline{h}$ is a uniquely determined hyperatom in $\overline{\mathfrak{S}} := \mathfrak{S}/J$, since otherwise $S \setminus J$ would not be maximal w. r. t. not containing h.

Now we consider some subdirectly irreducible homomorphic image $\overline{\overline{\mathfrak{S}}}$ with $\overline{\overline{h}} \neq \overline{\overline{0}}$. Here $\{\overline{\overline{0}}\}$ is the image of $\{\overline{0}\}$ and both, $\{\overline{0}\}$ and $\{\overline{\overline{0}}\}$ are regular filters w. r. t. the corresponding hyperatoms. This means $\overline{\overline{\mathfrak{S}}} \cong \mathfrak{S}/J \cong \overline{\mathfrak{S}}$. Consequently $\mathfrak{S}/J$ is subdirectly irreducible. □

5. 4. 9 Proposition. *Let $\mathfrak{S}$ be a commutative subdirectly irreducible d-semigroup. Then $\mathfrak{S}$ is linearly ordered and* 0*-cancellative.*

PROOF. According to 6.1.2 the relation $\equiv (P)$ provides a linearly ordered image.

Let now $a < b$ be a critical pair. If a is cancellable, then outside $C(S)$ only one element is possible, and this element must be equal to 0.

Otherwise all cancellable elements are smaller than or equal to a, and above a there can lie only $b = 0$.

Hence, it remains to verify that all $c \leq a$ are *conditionally cancellable,* meaning $ux = uy \leq a \Longrightarrow x = y$. To this end recall that $E(c)$ with $c \leq a$ is an ideal satisfying $E(c) \subseteq E(a)$, and that by assumption it holds, of course, $E(a) = \{1\}$. Hence, in case of $R(x, y, x', y')$ we get:

$$\begin{aligned} cx = cy \neq 0 \;&\Longrightarrow\; a(x \wedge y)x' = a(x \wedge y) = a(x \wedge y)y' \\ &\Longrightarrow\; x' = 1 = y' \Longrightarrow x = y\,. \end{aligned}$$ □

Applying the preceding proposition we get:

5. 4. 10 Proposition. *Any commutative d-semigroup $\mathfrak{S}$ is embedded in some hypernormal d-monoid.*

PROOF. We extend $\mathfrak{S}$ to a d-monoid, adjoin a zero 0 and construct the corresponding quotient hull. Now we form the direct product of all subdirectly irreducible images. □

In case that $\mathfrak{S}$ is not commutative, 5.4.9 does not hold. But – as shown below 6.1.1 – any subdirectly irreducible d-semigroup satisfying

(O) $$xay \wedge ubv \;\leq\; xby \vee uav\,.$$

is linearly ordered.

The results presented here concern subdirectly irreducible *cdl*-semigroups in general. In later chapters we will get further insights, for instance when considering archimedean subdirectly irreducible d-semigroups ($a^n \leq b \ \ (\forall\, n \in \mathbf{N}) \Longrightarrow ab, ba \leq b$), and thereby in particular *real d-semigroups*, cf. 9.3.8.

Chapter 6

Representation

6.1 Starting from l-ideals

6. 1. 1 Proposition. *Let $\mathfrak{S}$ be a d-semigroup and let P be an irreducible l-ideal. Then*

$$a \equiv b\ (P)\ \ :\Longleftrightarrow\ \ sa \in P \Longleftrightarrow sb \in P$$

defines a left congruence on $\mathfrak{S}$, and by analogy

$$a \equiv b\ (P)\ \ :\Longleftrightarrow\ \ \forall\, x, y : xay \in P \Longleftrightarrow xby \in P$$

defines even a congruence.

PROOF. Let P be a prime ideal. Then it is easily seen that the relation defined above is an equivalence relation, respecting multiplication from the left. So, it remains to verify that it also respects meet.

We write $\equiv$ instead of $\equiv(P)$ and start from $a \equiv b$. Then it follows:

$$\begin{array}{rcl} a \equiv b\ \&\ s(c \wedge a) \in P & \Longrightarrow & sc \in P \vee sa \in P \\ & \Longrightarrow & sc \in P \vee sb \in P \\ & \Longrightarrow & s(c \wedge b) \in P \\ & \leadsto & \\ c \wedge a & \equiv & c \wedge b \end{array}$$

Let now the second equivalence be satisfied, too. Then we succeed by analogy. $\square$

Sofar it is shown that irreducible ideals provide left congruences. But it has not yet been exhibited their particular meaning.

6.1.2 Proposition. *Let $\mathfrak{S}$ be a d-semigroup, let P be an irreducible l-ideal of $\mathfrak{S}$ and let $\equiv$ be the left congruence of* 6.1.1*. Then $\equiv$ is* linear, *meaning that the corresponding homomorphic image of $(S, \wedge, \vee)$ is a* chain.

PROOF. First we get $\overline{a} \leq \overline{b}$ iff $sb \in P \Longrightarrow sa \in P$ is satisfied. For, this condition implies:

$$\begin{aligned} s(a \wedge b) \in P &\Longrightarrow sa \wedge sb \in P \\ &\Longrightarrow sa \in P \vee sb \in P \\ &\Longrightarrow sa \in P\,, \end{aligned}$$

and $a \equiv a \wedge b$ implies:

$$sb \in P \;\Longrightarrow\; s(a \wedge b) \in P \Longrightarrow sa \in P\,.$$

Suppose now that $(S, \wedge)/\!\equiv$ is not linear. Then there exist elements $a, b, u, v \in S$ satisfying:

$$\begin{array}{lcl} ua \in P & \& & ub \notin P \\ va \notin P & \& & vb \in P\,. \end{array}$$

But this leads to

$$va \wedge ub \notin P \quad \& \quad va \wedge ub \leq vb \vee ua \in P\,,$$

a contradiction w.r.t. lemma 2.3.2. □

As is easily seen the preceding proof carries over to the both side case whenever

$$\text{(O)} \qquad xay \wedge ubv \;\leq\; xby \vee uav$$

is satisfied. This means that a d-semigroup is *representable,* i.e. admits a subdirect decomposition into linearly ordered factors, iff it satisfies condition (O). This condition is symptomatical for representability in general, as will turn out in context with studying *ordered algebraic structures.* Here we give the fundamental result:

6.1.3 Proposition. *Let $\mathfrak{S}$ be a d-semigroup and let P be an irreducible (lattice-)ideal. Then*

$$\text{(6.2)} \qquad ax \in P \;\&\; a \cdot x \equiv a \cdot y \Longrightarrow x \equiv y\,.$$

PROOF. Observe first that together with p also all elements equivalent to p belong to P. Hence, according to $ax \in P$, also $ay \in P$ is satisfied, which leads to

$$sx \in P \Longleftrightarrow (s \vee a)x \in P \Longleftrightarrow (s \vee a)y \in P \Longleftrightarrow sy \in P\,. \qquad \square$$

We now turn to operators acting on chains. They will prove to be of central importance.

6. 1. 4 Proposition. *Any d-semigroup $\mathfrak{S}$ admits a subdirect decomposition whose factors admit an embedding into some r-semigroup.*

PROOF. We start from 6.1.1 and 6.1.2 and consider the set R of all elements with $ax \equiv ay \Longrightarrow x \equiv y$. As shown above all elements of P have this property, but also all elements ca with cancellable c. Observe $cax \equiv cay \Longrightarrow c^{-1}cax \equiv c^{-1}$. Furthermore $w \leq r \in R \Longrightarrow w \in R$ since $xw = r$ & $wy \equiv wz \Longrightarrow ry = xwy \equiv xwz = rz$. Let now $sw \equiv cp \in R$. Then $w \leq s^+w \equiv (1 \wedge s)^{-1}cp$, whence $w \in R$. In other words: $W := S \backslash R$ satisfies $SW \subseteq W$ whence W is an $\equiv$-class.

On the set of all classes of $\equiv$ we define mappings ϕ_x by $\overline{s}\,\phi_x := \overline{xs}$. These functions provide *lattice endomorphisms* of $(\overline{S}, \wedge, \vee)$ satisfying moreover $sW \in W$, as just shown.

We consider $\{\phi_x \,|\, x \in S\}$. Obviously we get:

$$\phi_x \circ \phi_y = \phi_{yx} \quad \text{and} \quad \phi_x \wedge \phi_y = \phi_{x \wedge y}\,. \tag{6.3}$$

Now we consider the chain $\overline{T} := \{\overline{x}, x \notin W\}$. It follows first:

$$\begin{array}{rcl} \overline{s}\,\phi_x \in \overline{T} \;\&\; \overline{r} \leq \overline{s} & \Longrightarrow & \overline{r}\,\phi_x \in \overline{T} \\ & \& & \\ \overline{t}\,\phi_x \leq \overline{v} & \Longrightarrow & \exists\, \overline{u}:\; \overline{u}\,\phi_x = \overline{v}\,. \end{array}$$

OBSERVE: From $\overline{r} \leq \overline{s}$ it follows $\overline{s} = \overline{r \vee s}$, which means $x\overline{r} \leq x\overline{s}$, and from $\overline{xt} \leq \overline{u}$ it follows $\overline{u} = \overline{xt \vee u}$, from which results $\overline{u} = \overline{xv} = \overline{v}\,\phi_x$, for some suitable v.

Thus any $x \in S$ is mapped to an ideal/filter isomorphism ϕ_x of $\overline{T}$, and these $\phi_x : \overline{T} \longrightarrow \overline{T}$ satisfy the homomorphism conditions above.

So, it remains to verify that any pair $a < b$ of S is separated by at least one image:

By 4.1.3 there exists some prime ideal $P_{a,b}$ satisfying $a \in P_{a,b}$ & $b \notin P_{a,b}$. Hence the left congruence, generated by $P_{a,b}$, separates a and b, and this means in case of $(a \wedge b)e = a \wedge b$, that ϕ_a and ϕ_b produce different images of $\overline{e}$. □

Of course, dually w. r. t. irreducible ideals there exist the corresponding congruences w. r. t. irreducible filters. But, observe that the congruences *modulo* P and *modulo* $(S \backslash P)$ coincide.

6.2 Starting from c-ideals

In this section we will give an alternative proof of Theorem 6.1.4 by the rules of c-ideals. c-ideals are the adequate structure tool in ℓ-group theory.

In the following let $\mathfrak{S}$ always be an arbitrary d-semigroup. Let furthermore a, b be different, positive and fixed. We shall consider left congruences w. r. t. certain c-ideals, briefly *c-congruences.*

6. 2. 1 Lemma. *Under the above assumptions the set K_0 of all right units of $a \wedge b$ forms a c-ideal with $a \not\equiv b \ (K_0)$.*

PROOF. First of all K_0 is not empty, because of (A4), and moreover K_0 is multiplication closed, by evidence.

Suppose now $|\,f\,| \leq |\,e\,|$ & $e \in K_0$ and let g be a positive unit of $e \wedge f \wedge a \wedge b$. Then it holds $a(g \vee e) = a$ and we get $ae = a \rightsquigarrow a(g \wedge e) = a$ and thereby $ag = a = a(g \wedge e)g^* = ag^*$, that is $|\,e\,| = (g \vee e)g^* \in K_0$.

Hence, also $|\,f\,|$ belongs to K_0 and thereby also $f \vee g$ and any positive $f^{\because}$ with $f^{\because} \cdot (g \wedge f) = g$ belongs to K_0. This leads next to $af^{\because} = a \rightsquigarrow a = a(g \wedge f)$. Hence $f = (g \vee f)(g \wedge f) \in K_0$. □

6. 2. 2 Lemma. *The set of c-ideals K_i with $a \not\equiv b \ (K_i)$ contains a maximal K, and this K is prime.*

PROOF. Let $K_i \ (i \in I)$ be an ascending chain of c-ideals of the considered type. Then, also the union K of these $K_i \ (i \in I)$ is a c-ideal, separating the elements a and b, since

$$\begin{array}{rcl} a & \equiv & b\ (K) \\ & \rightsquigarrow & \\ a \leq be\ \ (\exists e \in K_j) & \& & b \leq af\ \ (\exists f \in K_j) \\ & \rightsquigarrow & \\ a \leq (a \wedge b)ef & \& & b \leq (a \wedge b)ef \\ & \rightsquigarrow & \\ a \vee b & \leq & (a \wedge b)ef \\ & \rightsquigarrow & \\ a & \equiv & b\ (K_j) \quad (\exists j \in I)\,. \end{array}$$

Hence there exists a maximal c-ideal K of the considered type. And moreover this K is prime, which is shown as follows:

Suppose $K = E \cap F$ with $E \neq K \neq F$. Then $a \equiv b\ (E)$ and $a \equiv b\ (F)$ would imply $a \leq be\ (e \in E)$ and $a \leq bf\ (f \in F)$, that is $a \leq b(e \wedge f)$ with $e \wedge f \in E \cap F = K$, meaning – by duality – $a \equiv a \wedge b \equiv b\ (K)$. □

We fix the maximal K of 6.2.2 and denote the corresponding left congruence by $\equiv$, and its classes $x\equiv$ by $\overline{x}$. Furthermore we term the residue structure $\mathfrak{S}/\equiv\ =\ \mathfrak{S}/K$ by $\overline{\mathfrak{S}}$.

6. 2. 3 Lemma. *Suppose $\overline{x} \leq \overline{y}$ and $u \in P$. Then it follows:*

$$\overline{xu} = \overline{x} \implies \overline{yu} = \overline{y}\,.$$

PROOF. We give two proofs (a) and (b), avoiding sups in the first case and left factors in the second case. Moreover suppose $y''(x \wedge y) = y$. Then we succeed by

$$\begin{array}{rrcl} \text{(a)} & x \equiv xu\ \&\ \overline{x} = \overline{x \wedge y} & \Longrightarrow & y = y''(x \wedge y) \equiv y''x \equiv y''xu \\ & & \Longrightarrow & \exists\ f \in K\ :\ yu \leq y''xu \leq yf \\ & & \Longrightarrow & yu \equiv y\ . \\[1ex] \text{(b)} & xu \leq xe\ \ (\exists\ e \in K) & \Longrightarrow & (x \vee y)u \leq (x \vee y)e \\ & & \Longrightarrow & yu \leq (x \vee y)u \equiv x \vee y \equiv y \\ & & \Longrightarrow & yu \leq (x \vee y)e \leq yfe \\ & & & (\exists\, e, f \in K) \\ & & \Longrightarrow & yu \equiv y\ . \end{array}$$ □

In particular – according to 6.2.3 – we get,

$$x \equiv y\ \&\ xu \equiv x \implies yu \equiv y\,. \tag{6.4}$$

6. 2. 4 Lemma. *Suppose* $\overline{x} \leq \overline{y}$ *and* $u \in P$. *Then it follows:*

$$\overline{yu} = \overline{y} \implies \overline{xu} \leq \overline{y}\,.$$

PROOF. First of all, for a suitable $e \in K$, we get $x \leq ye$, and therefore, because $yu \equiv y \Longrightarrow yeu \equiv ye$ we get furthermore $xu \leq yeu \equiv ye \equiv y$, that is $\overline{xu} \leq \overline{y}$. □

6. 2. 5 Lemma. *Suppose* $\overline{a \wedge b} \leq \overline{x} < \overline{a \vee b}$,. *Then the set* K_x *of all elements* e *with* $xe \equiv x$ *is equal to the fixed c-ideal* K.

PROOF. According to 4.2.3 it suffices to show, that K_x^+ and K^+ are equal. Furthermore by 6.2.3 we get $K^+ \subseteq K_x^+$.

Let now u, v belong to K_x. Then, according to 6.2.3 in a similar manner as below 6.2.1 we get

$$\begin{aligned} xu \equiv x \ \&\ xv \equiv x &\implies xu \equiv xuv \\ &\implies x \equiv x \cdot uv\,. \end{aligned}$$

Thus K_x is sup-c-ideal of K.

Let next u belong to ${K_x}^+$. Then it results $xu \equiv x$ whence for each $e_1, ..., e_n \in K_0$ successively $x \equiv xue_1ue_2...ue_nu \equiv x$ is obtained. This means – according to 4.2.4 and again according to 6.2.4 – that a and b are not separated by $(K, u)^c$ that is that $(K, u)^c = K$ and thereby $u \in K^+$, that is $K^+ \supseteq K_x^+$. This completes the proof. □

Furthermore we get:

6. 2. 6 Lemma. *In* $\overline{\mathfrak{S}}$ *the classes* $\overline{a}$ *and* $\overline{b}$ *are comparable.*

PROOF.
$$\begin{aligned} (a \wedge b)(a' \wedge b') = a \wedge b &\implies a' \wedge b' \in K \\ &\implies a' \in K \vee b' \in K \\ &\implies \overline{a} \leq \overline{b} \vee \overline{b} \leq \overline{a}\,, \end{aligned}$$
□

Start now – w. l. o. g. – from $\overline{a} < \overline{b}$.

6. 2. 7 Lemma. *In* $\overline{\mathfrak{S}}$ *each* $\overline{x} \leq \overline{b}$ *is comparable with each* $\overline{s}$.

PROOF. (i) First of all we consider the classes $\overline{x} \leq \overline{a}$. Here we get:

$$\begin{aligned} (x \wedge s)(x' \wedge s') = x \wedge s &\implies a(x' \wedge s') \equiv a \\ &\implies x' \wedge s' \in K_a = K \\ &\implies x' \in K \vee s' \in K \\ &\implies \overline{x} \leq \overline{s} \vee \overline{s} \leq \overline{x}\,. \end{aligned}$$

(*ii*) Let now $\overline{x} \leq \overline{b}$ be satisfied. Then in case of $\overline{x \wedge s} < \overline{b}$, we may argue in analogy with (*i*).

If, however, it holds $\overline{x \wedge s} = \overline{b}$, then $\overline{x} = \overline{b} = \overline{x \wedge s}$, that is $\overline{x} \leq \overline{s}$. □

Next we define

$$\text{(T)} \qquad T := \left\{ u \,\middle|\, \overline{tu} = \overline{t} \;\&\; u \in P \Longrightarrow u \in K \right\} .$$

6. 2. 8 Lemma. *T contains all $\overline{x} < \overline{b}$ and all $\overline{x}$ with $x \in C$.*

PROOF. In case of $\overline{x} < \overline{b}$ & $\overline{xu} = \overline{x}$, we get:

$$\begin{aligned} \overline{xu} = \overline{x} &\Longrightarrow \overline{(a \vee x)u} = \overline{a \vee x} \\ &\Longrightarrow u \in K_{a \vee x} = K . \end{aligned}$$

And, in case of $c \in C$ & $\overline{cu} = \overline{c}$, we find some suitable pair $e \in K, v \in P$ satisfying

$$cu \leq ce \;\&\; cuv = ce \Longrightarrow uv = e \Longrightarrow u \in K . \qquad \square$$

6. 2. 9 Proposition. *The system $\overline{T}$ satisfies:*

$$\begin{array}{lrcl} (1) & e \in K & \Longrightarrow & e \in T = \{t \,|\, \overline{t} \in \overline{T}\} \\ (2) & \overline{t_1} \leq \overline{t_2} \in \overline{T} & \Longrightarrow & \overline{t_1} \in \overline{T} \\ (3) & t \in T \;\&\; s \in S & \Longrightarrow & \overline{t} \leq \overline{s} \;\vee\; \overline{s} \leq \overline{t} \\ (4) & \overline{st} \in \overline{T} & \Longrightarrow & \overline{t} \in \overline{T} \\ (5) & c \wedge d \in T & \Longrightarrow & c \in T \;\vee\; d \in T . \end{array}$$

PROOF. Throughout the proof we assume that u, v, w are positive. Then it follows:

Ad (1): $e \in K$ & $\overline{eu} = \overline{e}$ & $eu \leq ef \;\; (f \in K)$ implies $u \leq eu \leq ef \in K \rightsquigarrow u \in K$.

Ad (2): $\overline{t_1} \leq \overline{t_2}$ & $\overline{t_1 u} = \overline{t_1}$ – according to 6.2.3 – implies $\overline{t_2 u} = \overline{t_2}$, that is $u \in K$.

Ad (3): $t \in T$ & $s \in S$ & $R(s,t,s',t')$ & $\overline{t} \in \overline{T}$ implies by (Ad (2)) $\overline{s \wedge t} \in \overline{T}$, from which results:

$$\begin{aligned} (s \wedge t)(s' \wedge t') = s \wedge t &\Longrightarrow s' \in K \vee t' \in K \\ &\Longrightarrow \overline{s} \leq \overline{t} \vee \overline{t} \leq \overline{s} . \end{aligned}$$

Ad (4): $\overline{st} \in \overline{T}$ & $\overline{tu} = \overline{t}$ implies $\overline{stu} = \overline{st} \Longrightarrow u \in K$.

Ad (5): $\overline{c} \wedge \overline{d} \in \overline{T}$ & $\overline{cu} = \overline{c}$ & $\overline{dv} = \overline{d}$ implies first

$$\left.\begin{array}{c} \overline{c(u \wedge v)} = \overline{c} \\ \\ \overline{d(u \wedge v)} = \overline{d} \end{array}\right. \rightsquigarrow \overline{(c \wedge d)(u \wedge v)} = \overline{(c \wedge d)}$$

and thereby $u \wedge v \in K$ because $c \wedge d \in T$, that is $u \in K \vee v \in K$.

Suppose now w. l. o. g. $\overline{c} \notin \overline{T}$. Then there exists an element u with $\overline{cu} = \overline{c}$, but $u \notin K$. By the implication above this leads to $v \in K$ for all v with $\overline{dv} = \overline{d}$. Therefore in this case it must hold $\overline{d} \in \overline{T}$. □

Now we are in the position to prove:

6. 2. 10 Proposition. *Let D be the intersection of all b and T containing m-ideals with $x \equiv g \in I \Longrightarrow x \in I$. Then each $\overline{d}$ $(d \in D)$ is comparable with each $\overline{s}$ $(s \in S)$, and it is $S \backslash D$ in any case* closed w. r. t. multiples. *If moreover $D/\!\equiv$ has no maximum, then $S \backslash D$ is even a d-ideal.*

PROOF. Suppose $\overline{x} \leq \overline{g} \in \overline{T}$. Then according to 6.2.9 (2) also $\overline{x}$ belongs to $\overline{T}$, meaning that each s satisfies $\overline{x} \leq \overline{s}$ or $\overline{s} \leq \overline{x}$. Hence, if $\overline{x}$ and $\overline{s}$ are incomparable, then neither $\overline{x}$ nor $\overline{s}$ can belong to $\overline{T}$.

Let now $\overline{x}$, $\overline{s}$ be incomparable and therefore $x, s \notin T$. Then for all $\overline{g} \in \overline{T} \cup \{\overline{b}\}$ it holds $\overline{g} \leq \overline{x}$ and $\overline{g} \leq \overline{s}$, as well, which implies $\overline{x} = \overline{g \vee x}$ and $\overline{s} = \overline{g \vee s}$. Therefore, due to $K \subseteq T$, we may start from positive elements x, s, in order to prove $x, s \notin D$, thus constructing a contradiction which leads to the fact, that each $\overline{d}$ $(d \in D)$ is comparable with each $\overline{s}$ $(s \in S)$.

So let's start from $x, s \in P$ and $R(x, s, x', s')$ with positive elements x', s'. Then we get first $\overline{g} \leq \overline{x' \wedge s'}$, since together with x, s also the elements x', s' are incomparable This leads further to

$$\begin{array}{rcl} g & \leq & (x' \wedge s')e \ \ (e \in K) \\ & \rightsquigarrow & \\ (x \wedge s)g & \leq & (x \wedge s)(x' \wedge s')e \\ & = & (x \wedge s)e \ , \\ & \rightsquigarrow & \\ \overline{(x \wedge s)g} & \leq & \overline{x \wedge s}\,. \end{array}$$

But, the set U of all u with $\overline{(x \wedge s)u} \leq \overline{x \wedge s}$ is an m-ideal, which contributes to D, which is shown as follows: : Put $x \wedge s =: z$. Then it results:

$$\begin{array}{rcl} \overline{zu} \leq \overline{z} \ \&\ \overline{zv} \leq \overline{z} & \Longrightarrow & \overline{z(u \vee v)} \leq \overline{z} \\ & \& & \\ v \leq u \ \&\ \overline{zu} = \overline{z} & \Longrightarrow & \overline{zv} \leq \overline{zu} \leq \overline{z}\,, \end{array}$$

whence U is a lattice ideal. But U is moreover multiplication closed. Observe, in case of

$$\begin{array}{lccc} & \overline{zu} \leq \overline{z} & \& & \overline{zv} \leq \overline{z} \\ \text{with} & zu \leq ze & \& & zv \leq zf \quad (e, f \in K)\,, \end{array}$$

it follows for some suitable positive element e'

$$\begin{array}{rcl} zuv & \leq & zev = e'zv \leq e'zf = zef \\ & \rightsquigarrow & \\ \overline{zuv} & \leq & \overline{z}\,. \end{array}$$

Hence U is also multiplication closed, whence U is even an m-ideal that contributes to D, that is satisfies $U \supseteq D$.

Now, by verifying $x \notin U \ \&\ s \notin U$ we show, that x and s do not belong to D. To this end consider – by example – $\overline{(x \wedge s)x} \leq \overline{x \wedge s}$. Then, since x and s are positive, it results $\overline{x} = \overline{x \wedge s}$ and thereby $\overline{x} \leq \overline{s}$, a contradiction!

So far we got that all classes $\overline{d}$ $(d \in D)$ are comparable with all classes $\overline{s}$ $(s \in S)$. It remains to verify, that

(a) $S \backslash D$ is closed w. r. t. multiples in any case, and
(b) that $S \backslash D$ forms even a d-ideal, if D has no maximum.

Ad (a). Consider:

$$(i) \quad sg \in D \ \&\ g \notin D \ \text{ and } \ (ii) \quad gs \in D \ \&\ g \notin D\,.$$

Ad (i): Let e be a unit of s and suppose $e''(e \wedge s) = e = (e \wedge s)e'$ with positive elements e', e''. Then, in case that e is chosen adequately small, it results $(e \wedge s)e' \in T$, and thereby $e' \in T \subseteq D$. Hence ee' belongs to D and consequently – choose some suitable positive element r – also $e''e = re''$ belongs to D. But, according to 6.2.9 (4) this provides the contradiction $g \leq re''sg = rs^+g \in D \rightsquigarrow g \in D$.

Ad (ii): Let e be a unit of s and suppose $(e \wedge s)e' = e$ with some positive e'. Then, choosing like above, we get $(e \wedge s)e' = e \in T$ and thereby, due to 6.2. 9 (2), $g \leq gs^+ = gse' \in D$, again a contradiction!

Ad (b). Recalling that $D/\!\equiv$ is linearly ordered, and that any $\overline{d}$ satisfies $\overline{d} \leq \overline{x}$ for any $x \notin D$ we get:

$$\overline{c} \wedge \overline{d} \in \overline{D} \ \&\ c, d \notin D \implies \overline{c} \wedge \overline{d} = \max(\overline{x}) \ \ (x \in D)\,. \qquad \square$$

Before continuing we recall the notion of an r-semigroup, and repeat 6.1.4 in a certain manner as part 1 of a main theorem on the interplay between d-semigroups and r-semigroups.

6. 2. 11 Proposition. *Any d-semigroup $\mathfrak{S}$ has a subdirect decomposition into semigroups of ideal/filter isomorphisms of the special chains $\overline{\mathcal{T}}$, constructed above.* [1)]

PROOF. We give a *self contained* proof. This provides additional insights, based on some repetitions:

We choose the structure elements an denotations of proposition 6.2.10 and consider 6.2.11 as continuation of 6.2.10 . So, let D and T be given in the sense of 6.2.10.

We define ϕ_x *via* $\overline{s}\,\phi_x := \overline{xs}$. These mappings are lattice endomorphisms of $(\overline{S}, \wedge, \vee)$ – satisfying moreover $s \in O := S \backslash D \Longrightarrow \overline{s}\,\phi_x \subseteq O$.

Next we consider $\{\phi_x \mid x \in S\}$. Obviously it holds

$$\phi_x \circ \phi_y = \phi_{yx} \ \text{ and } \ \phi_x \wedge \phi_y = \phi_{x \wedge y}\,, \tag{6.6}$$

and moreover the chain *chain* $\overline{T}$ satisfies:

$$\begin{array}{rcl} \overline{s}\,\phi_x \in \overline{T} \ \&\ \overline{r} \leq \overline{s} & \Longrightarrow & \overline{r}\,\phi_x \in \overline{T} \\ & \& & \\ \overline{t}\,\phi_x \leq \overline{v} & \Longrightarrow & \exists\, \overline{u}:\ \overline{u}\,\phi_x = \overline{v}\,. \end{array}$$

FOR: $\overline{r} \leq \overline{s}$ implies $\overline{s} = \overline{r \vee s}$, that is $\overline{xr} \leq \overline{xs}$, and $\overline{xt} \leq \overline{v}$ implies $\overline{v} = \overline{xt \vee v}$, that is $\overline{v} = \overline{xu} = \overline{u}\,\phi_x$ for some suitable u .

[1)] Of course, by 6.1.4 it has already developed such a subdirect decomposition along different lines, but that method does not respect the cancellation property and the method of proof given here works already in weaker than d-semigroup situations.

Now we show, that the order endomorphisms ϕ_x induce even ideal/ filter isomorphisms on the chains $\mathcal{T}$. To this end we assume $\overline{s}\,\phi_x = \overline{t}\,\phi_x$. Then there are elements $s', t' \in P$ satisfying:

$$\begin{array}{cccc} & \overline{s}\,\phi_x & = & \overline{t}\,\phi_x \in \overline{T} \\ & & \Longrightarrow & \\ & \overline{x(s \wedge t)s'} & = \overline{x(s \wedge t)} = & \overline{x(s \wedge t)t'} \\ & & \Longrightarrow & \\ \leadsto & s' \in K & \& & t' \in K \\ \leadsto & \overline{s} & = & \overline{t}\,. \end{array}$$

Thus any $x \in S$ is mapped on an induced ideal/filter isomorphism ϕ_x of $\overline{T}$, and moreover, these $\phi_x : \overline{T} \longrightarrow \overline{T}$ satisfy equation (6.6).

It remains to verify that any pair $a \neq b$ is separated in at least one component. So, let's start from

$$e(a \wedge b) = \ (a \wedge b) \ = (a \wedge b)e$$

with positive e. Then there exist positive elements u, v satisfying

$$(e \wedge a \wedge b) \cdot u = e \wedge a \ \& \ (e \wedge a \wedge b) \cdot v = b\,,$$

that is with:

$$\begin{array}{ccc} (e \wedge a \wedge b) \cdot u(e \vee a) = a & \& & b = (e \wedge a \wedge b) \cdot v \\ & \leadsto & \\ P \ni u(e \vee a) & \neq & v(e \vee b) \in P\,. \end{array}$$

So each $u(e \vee a) \neq v(e \vee b)$ is separated, whence all $a \neq b$ are separated: Suppose $w(e \wedge a \wedge b) = e$, and multiply $\overline{a}$ and $\overline{b}$ from the left with w. $\square$

6. 2. 12 Corollary. *Proposition 6.2.11 remains valid even in cdl-monoids $\mathfrak{S}$ satisfying the conditions:*

(A4') $$a \leq b \implies \exists x : \ ax = b$$

(A4") $$ax = ay \implies (a \vee b)x = (a \vee b)y\,.$$

PROOF. This is verified by checking step by step. $\square$

That an identity element 1 is relevant is shown by the right zero case. However this condition may be slightly weakened along the lines of the proof given in this section.

6.3 r-Semigroups

The results of this chapter give rise to the question which way d- and r-semigroups interact. Already in the introduction it was mentioned, that r-semigroups always satisfy the axioms (A1) through (A3) and moreover many rules of divisibility arithmetic, however not in any case also axiom (A4) is valid. In order to verify this we consider $\mathbf{Q}$. Here, for instance 0 and $\sqrt{2}$ generate isomorphic order filters $\{x \mid x > 0\}$ and $\{x \mid x > \sqrt{2}\}$ but non isomorphic corresponding order ideals $\{x \mid x \leq 0\}$ and $\{x \mid x \leq \sqrt{2}\}$. This shows easily that axiom (A4) fails to be satisfied.

On the other hand, the r-semigroup of the *real axis* does satisfy axiom (A4). Thus the r-semigroup of $\mathbf{Q}$ is embedded in the r-semigroup of $\mathbf{R}$, which is a d-semigroup.

This suggests the conjecture that any r-semigroup can be extended to a d-semigroup of ideal/filter isomorphisms, by extending the chain under consideration. And, in fact, we will succeed by an extension method due to Harzheim, cf. [59].

To this end we start from a chain $(T, \leq) =: \mathcal{T}$ and define

(1) $A < B :\Longleftrightarrow a < b \ \ (\forall a \in A, b \in B)$,

(2) $\mathcal{A}(C) := \{x \mid x \leq c \ \ (\exists c \in C)\}$,

(3) $\mathcal{E}(C) := \{x \mid x \geq c \ \ (\exists c \in C)\}$.

Next we call *cut* of $\mathcal{T}$ any pair $A < B$ with $A \cup B = T$, and we denote the set of all cuts of $\mathcal{T}$ by $\mathcal{S}(\mathcal{T})$. Let now $A \mid B$ and $C \mid D$ be two cuts of $\mathcal{T}$. We put $A \mid B < C \mid D$ iff $A \subseteq C$ is satisfied. Furthermore, if $a \in T$ and $C \mid D \in \mathcal{S}(\mathcal{T})$, we put $a < C \mid D$ iff $a \in C$ is satisfied, and we put $C \mid D < a$ iff $a \in D$ is satisfied. This provides an extension of the order of $\mathcal{T}$ to $T \cup \mathcal{S}(\mathcal{T})$ and generates a chain $\overline{\mathcal{S}}(\mathcal{T})$.

In the following it will be helpful to think of $A \mid B$ as of a tag between A and B.

Finally, if ω_M is the *order type* of the chain $\mathcal{M} = (M, <)$ we introduce the notion ω_M^* for the *order type* of $\mathcal{M} = (M, >)$.

6. 3. 1 Definition. Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be chains, such that $T_1 \subseteq T_2$ and such that $a \leq b$ in $\mathcal{T}_1$ implies $a \leq b$ in $\mathcal{T}_2$. Then we put $\mathcal{T}_1 \trianglelefteq \mathcal{T}_2$.

Let $\mathcal{K}$ be a chain and let $\mathcal{T}_\kappa$ $(\kappa \in K)$ be a family of chains, such that $\kappa_1 \leq \kappa_2 \Longrightarrow \mathcal{T}_{\kappa_1} \trianglelefteq \mathcal{T}_{\kappa_2}$. Then by $\sum\limits_{\kappa\in K} \mathcal{T}_\kappa$ $(\kappa \in K)$ we mean $\bigcup\limits_{\kappa\in K} T_\kappa$ considered w. r. t. $a \leq b$ iff $a \leq b$ in one $\mathcal{T}_\kappa$ and thereby in all $\mathcal{T}_\kappa$ with $a, b \in\ T_\kappa$.

Finally, recall that an ordered set $\mathcal{C} \trianglelefteq \mathcal{T}$ is said to be coinitial in $\mathcal{T}$ if for every $t \in T$ there exists an element $c \in C$ with $t < c$, and that dually an ordered set $\mathcal{C} \trianglelefteq \mathcal{T}$ is said to be cofinal in $\mathcal{T}$ if for every $t \in T$ there exists an element $c \in C$ with $c < t$.

6. 3. 2 Definition. Let λ be an *ordinal number.* We put

$$\begin{aligned} \mathcal{S}(1) &:= \quad \mathcal{S}(\emptyset) \\ \mathcal{S}(\nu) &:= \begin{cases} \sum\limits_{\kappa<\nu} \mathcal{S}\,(\kappa) \ \ (\kappa < \nu), & \text{if } \nu \text{ is a } \textit{limes} \\ \overline{\mathcal{S}}\,(\mathcal{S}\,(\nu-1)) & \text{otherwise.} \end{cases} \end{aligned}$$

Then it results nearly immediately:

6. 3. 3 Lemma. *Let $\mathcal{T} = (T, <)$ be a chain, and let λ be the initial ordinal of the cardinality of the* power set T^* *of T. Then the chain $\mathcal{T}$ is embedded in some $\mathcal{S}(\alpha)$ $(\alpha < \lambda)$. In particular, if we well order T by $\ll$ (what way ever), then $(T, \ll)$ represents an ordinal $\beta < \lambda$.*

Moreover the convex hull $\mathcal{C}(T) =: \mathcal{C}$ *of $\mathcal{T}$ in $\mathcal{S}(\lambda)$ and any interval $\{x \mid A < x < B\}$ determined by some cut $A \mid B$ of $\mathcal{T}$ as well as any ideal $\{x \mid x \in \mathcal{S}(\lambda)\ \&\ x < T\}$ and any filter $\{x \mid x \in \mathcal{S}(\lambda)\ \&\ x > T\}$ are similar to $\mathcal{S}(\lambda)$.*

PROOF. Let T be well ordered of type $\beta < \lambda$. We choose successively $f(t_\nu) =: s_\nu \in S(\nu)$ $(\nu \leq \lambda)$ in a similar constellation w. r. t. $\{s_\kappa \mid \kappa < \nu\}$ as the constellation of t_ν is w. r. t. $\{t_\kappa \mid \kappa < \nu\}$ in $\mathcal{T}$.

After this embedding of $\mathcal{T}$ in $\mathcal{S}(\alpha)$, since λ as limes is indecomposable, there remain λ many cut extensions towards $\mathcal{S}(\lambda)$ to be realized. This means, that in fact any interval $\{x \mid A < x < B\}$ determined by some cut $A \mid B$ of $\mathcal{T}$ as well as any ideal $\{x \mid x \in \mathcal{S}(\lambda)\ \&\ x < T\}$ and any filter $\{x \mid x \in \mathcal{S}(\lambda)\ \&\ x > T\}$ of are similar to $\mathcal{S}(\lambda)$. $\square$

The next result is crucial.

6. 3. 4 Proposition. *Let λ be a limes and let S be a convex subset of $\mathcal{S}(\lambda)$, such that there exists an inductively well ordered subset $\mathcal{C}_e$ of ordinal number β with $0 < \beta < \lambda$ which is coinitial in $\mathcal{A}(S)$, and such that there exists an inductively well ordered subset $\mathcal{C}_e$ of ordinal number γ^* with $0 < \gamma < \lambda$, which is cofinal in $\mathcal{E}(S)$. Then $\mathcal{S}$ is similar to $\mathcal{S}(\lambda)$.*

PROOF. Put $\alpha := \max(\beta, \gamma)$. Then, since λ is a limes any $\kappa < \lambda$ satisfies even $\kappa + \alpha < \lambda$.

Now we choose the first μ' with $S \cap \mathcal{S}(\mu') \neq \emptyset$. By assumption, this μ' has the predecessor $\mu = \mu' - 1$, and by construction there is only one $s \in S(\mu')$ belonging to S, since the existence of two different elements $s_1 \neq s_2 \in S$ requires that (already) $\mathcal{S}_\mu$ contains an element of S, recall S is convex in $S(\lambda)$.

Next we will "extract" successively subsets of cuts out of $\mathcal{S}$ such that finally $\mathcal{S}$ is exhausted. First of all we put:

$$\mathcal{N}(1) \;:=\; \mathcal{S}(\mu + 1) \cap \mathcal{S}\,.$$

By our above demonstration it holds

$$\begin{array}{lccc} & \mathcal{S}(\mu + 1 + 0) \cap \mathcal{S} \;\subseteq\; \mathcal{N}(1) \;\subseteq\; \mathcal{S}(\mu + 1 + \alpha + 0) \cap \mathcal{S} & & \\ \text{with} & \mathcal{S}(0) \quad \sim \quad \mathcal{N}(1) & & (\text{by } f_0)\,. \end{array}$$

Hence we may suppose that already each κ with $1 \leq \kappa < \nu < \lambda$ is associated with some $\mathcal{N}(\kappa + 1)$ in such a way that it holds

$$\begin{array}{lccl} & \multicolumn{3}{c}{\mathcal{S}(\mu + 1 + 0 + \kappa) \cap \mathcal{S} \;\subseteq\; \mathcal{N}(\kappa + 1) \;\subseteq\; \mathcal{S}(\mu + 1 + \alpha + \kappa) \cap \mathcal{S}} \\ \text{with} & \mathcal{S}(\kappa) & \sim & \mathcal{N}(\kappa + 1) \quad (\text{by } f_\kappa) \\ \text{and} & \kappa_1 \leq \kappa_2 & \Longrightarrow & \mathcal{N}(\kappa_1) \subseteq \mathcal{N}(\kappa_2) \\ & & \& & f_{\kappa_1} \subseteq f_{\kappa_2}\,. \end{array}$$

We will show that this construction finally "arrives" at λ. To this end we consider w. r. t. ν the limes and the non limes case.

CASE 1. Let ν be a limes. We put:

$$\mathcal{N}(\nu) \;:=\; \bigcup \mathcal{N}(\kappa) \; (\kappa < \nu)$$

seeing immediately that this set satisfies the induction condition for ν.

CASE 2. Let now ν be no limes. Then $\nu - 1$ exists, hence $\mathcal{N}(\nu - 1)$ is defined, and moreover any cut of $\mathcal{N}(\nu - 1)$ induces uniquely a cut of $\mathcal{S}(\nu - 1)$. But this means that $\mathcal{N}(\nu)$ and $\mathcal{S}(\nu)$ fulfill the induction condition for ν.

Thus, on the one hand the induction condition is carried over and on the other hand, since λ is a limes, that is $\mu' + \lambda' = \lambda \Longrightarrow \lambda' = \lambda$, we obtain $\mathcal{S} \sim \mathcal{S}(\lambda)$.

This completes the proof. □

In addition it has been proven that in convex hulls $\mathcal{C}(T)$ with $|\,T\,| < |\,S(\lambda)\,|$ all order filters, isomorphic with some order ideal of $\mathcal{C}(T)$, and all order ideals, isomorphic with some order filter of $\mathcal{C}(T)$, have complements of type $\mathcal{S}(\lambda)$, and it holds by analogy that any cut of $\mathcal{C}(T)$ generates an interval of type $\mathcal{S}(\lambda)$. This leads to

6. 3. 5 Theorem. *Any r-semigroup admits an embedding into a d-semigroup of order/filter isomorphisms.*

PROOF. Let $\mathcal{T}$ be given and let λ be an initial ordinal of T^*. We embed $\mathcal{T}$ into $\mathcal{S}(\lambda)$ – according to 6.3.3.

Then for each cut $A\,|\,B$ of $\mathcal{T}$ the added elements produce a uniquely determined convex subset C of $\mathcal{S}(\lambda)$ with $A < C < B$ & $A \cup B = T$, similar to $\mathcal{S}(\lambda)$, and it holds for any ideal/filter isomorphism ϕ of $\mathcal{S}(\lambda)$ the proper inequality $A\,\phi < C\,\phi < B\phi$.

Now we consider the convex hull $\mathcal{K} := \mathcal{C}(T)$ of $\mathcal{T}$ in $\mathcal{S}(\lambda)$.

Then there exists some well ordered set of some even fixed well order type $\alpha < \lambda$, coinitial in $\mathcal{K}$ and thereby also in any filter $K - A\,\phi$ with ideal A of $\mathcal{K}$, whence the ideals $\{x\,|\,x < \phi(A)\}$ are similar to $\mathcal{S}(\lambda)$ – and whence by duality also the filters $\{x\,|\,x > A\}$ are similar to $\mathcal{S}(\lambda)$.

We now choose and fix some $\mathcal{S}$ of the class $\mathcal{S}_i$ $(i \in I)$ of all subsets, order isomorphic to $\mathcal{S}(\lambda)$, pick one isomorphism $\phi_i : \mathcal{S}_i \longrightarrow \mathcal{S}$ for each $\mathcal{S}_i$, in order to define afterwards for each $\mathcal{S}_i$, $\mathcal{S}_j$ an isomorphism $\mathcal{S}_i \longrightarrow \mathcal{S}_j$ *via*

$$\phi_{i,j} : \mathcal{S}_i \longrightarrow \mathcal{S}_j := \phi_i \circ \phi_j^{\ -1}.$$

Then any ideal/filter isomorphism ϕ_T of $\mathcal{T}$ w. r. t. the definition of $\phi_{i,j}$ in a canonical manner generates an ideal/filter isomorphism ϕ_K of the *convex hull*

$\mathcal{K}$ of $\mathcal{T}$, such that composition and pointwise minimum are carried over and above all it turns out that the r-semigroup of $\mathcal{K}$ is a d-semigroup.

ASSUME NOW $\phi \leq \psi$, that is $x\phi \leq x\psi$ for all x of dom(ϕ).

Then – as is easily seen – there exists a right quotient w. r. t. ϕ and ψ – send $x\phi$ to $x\psi$ and extend this relation in case of $K\phi \neq K$, and thereby $K\psi \neq K$, by a similar mapping of $\mathcal{K} - \mathcal{K}(\phi)$ onto $\mathcal{K} - \mathcal{K}(\psi)$, which is possible according to 6.3.4. Thus, summarizing we get: $\phi \leq \psi \Longrightarrow \phi \,|_l\, \psi$.

NEXT we construct the corresponding left quotients. To this end we consider the *relation* $\psi \circ \phi^{-1}$ in three steps.

1. Obviously dom $(\psi \circ \phi^{-1}) =$ dom (ψ) and moreover the elements of dom(ψ) satisfy $((x\psi)\phi^{-1})\phi = x\psi$, that is $(\psi \circ \phi^{-1}) \circ \phi = \psi$.

So, if in addition rg$(\psi \circ \phi^{-1})$ is a filter, then $\psi \circ \phi^{-1}$ is an ideal/filter isomorphism, and we are through.

2. If however neither rg$(\psi \circ \phi^{-1})$ is a filter nor dom$(\psi \circ \phi^{-1})$ is (the whole) K, then – according to 6.3.4 – we are in the position to complete the relation $\psi \circ \phi^{-1}$ to some ideal/filter isomorphism with the required properties.

3. Finally, if dom$(\psi \circ \phi^{-1}) = K$, implying dom$(\psi) =$ dom$(\phi) = K$, then rg$(\psi \circ \phi^{-1})$ is a filter and thereby $\psi \circ \phi^{-1}$ is an ideal/filter isomorphism, satisfying $(\psi \circ \phi^{-1}) \circ \phi = \psi$, for:

Suppose dom$(\phi) =$ dom$(\psi) = K$ and $y \geq x \in$ rg$(\psi \circ \phi^{-1})$. Then it results $y\phi \geq x\phi \in$ rg(ψ), and thereby $y\phi \in$ rg(ψ), that is $y \in$ rg$(\psi \circ \phi^{-1})$, whence $\psi \circ \phi^{-1}$ is an ideal/filter isomorphism satisfying $(\psi \circ \phi^{-1}) \circ \phi = \psi$ and thereby $\phi \leq \psi \Longrightarrow \phi \,|_r\, \psi$, that is all at all

$$\phi \leq \psi \Longrightarrow \phi \,\Big|\, \psi\,. \tag{6.9}$$ □

Next we present a proposition, due to Holland [65], that will afterwards be carried over to d-semigroups.

6. 3. 6 Proposition. *Let $\mathcal{T}$ be a chain whose closed intervals are order isomorphic. Then the ℓ-group $\mathfrak{A}$ of all order automorphisms of $\mathcal{T}$ is* divisible, *that is, then in $\mathfrak{A}$ any $x^n \doteq a$ has a solution.*

PROOF. We give a slightly modified verification here:

Let α be an order automorphism of $\mathcal{T}$ and let n be a natural number. We are looking for some χ satisfying $\chi^n = \phi$. Obviously an ℓ-group is divisible iff its positive cone is divisible. Consequently, we may assume that all $x \in T$ satisfy $x \leq x\phi$. Furthermore, by assumption $\mathcal{T}$ is dense. Now, in order to construct such a χ we call *equivalent* any two elements x, y with the property that $\{z \,|\, z = y\phi^n \ (n \in \mathbf{Z})\}$ and $\{z \,|\, z = x\phi^n \ (n \in \mathbf{Z})\}$ generate the same *convex hull*. Obviously this is the case iff y belongs to the convex hull of $\{z \,|\, z = x\phi^n \ (n \in \mathbf{Z})\}$ and x belongs to the convex hull of $\{z \,|\, z = y\phi^n \ (n \in \mathbf{Z})\}$, and it is easily checked that an equivalence class is a singleton iff it is generated by a *fixpoint* and thereby that an equivalence class, containing at least one non fixpoint, satisfies $z < z\phi$ for all z.

Let now $[\,x\,]$ be some equivalence class and let $x < x\phi$. Then, since $\mathcal{T}$ is dense, the interval $[\,x\,,\,x\phi\,]$ can be decomposed into n intervals by choosing some

$$x = x_0 < x_1 < x_2 < ... < x_{n-1} < x_n = x\phi\,,$$

and by assumption the intervals $(x_k, x_{k+1}]$ are isomorphic. Hence an order automorphism χ can be constructed by generating a mapping in such a way that in the classes with non empty *support* any $(x_k, x_{k+1}]$ $(k+1 < n)$ is mapped onto $(x_{k+1}, x_{k+2}]$ whereas fixpoints remain fix. □

Now we are in the position to prove

6. 3. 7 Proposition. *Any r-semigroup admits an embedding into a* divisible *d-semigroup.*

PROOF. We start from the setting of 6.3.5 with $\mathcal{N} := \mathcal{S}(\lambda)$. Then, any positive ideal/filter isomorphism ${\phi_K}^+$ admits an extension to an order automorphism ϕ_N of the chain $\mathcal{N}$.

So, putting

$$\begin{aligned} x{\phi_N}^+ &:= x\phi_N && \text{in case of} && x \leq x\phi_N \\ x{\phi_N}^+ &:= x && \text{in case of} && x \geq x\phi_N\,, \end{aligned}$$

we get a positive order automorphism of $\mathcal{N}$, inducing the ideal/filter isomorphism ${\phi_K}^+$ of $\mathcal{K}$.

Conversely it is easily checked that any positive order automorphism ϕ^+ of $\mathcal{N}$ induces some positive ideal/filter isomorphism ${\phi_K}^+$ of $\mathcal{K}$, respecting composition and pointwise minimum.

Hence the ℓ-semigroup $\mathfrak{R}^+(\mathcal{K})$ of all positive ideal/filter isomorphisms of $\mathcal{K}$ is a positive divisible d-semigroup.

Now we show that the r-semigroup of $\mathcal{T}$ is embedded in the quotient hull of $\mathfrak{R}^+(\mathcal{K})$.

To this end let ϕ_T be an arbitrary ideal/filter isomorphism of $\mathcal{T}$ and let ϕ_S be some of its extensions to $\mathcal{N}$. Then ϕ_K admits a splitting into

$$\phi_K{}^+ \circ \psi_K{}^- = \psi_K{}^- \circ \phi_K{}^+$$
$$via$$
$$x\phi_K{}^+ = x\phi_K \quad \text{and} \quad x\psi_K{}^- = x \quad \text{in case of} \quad x \leq x\phi_S$$
$$x\psi_K{}^- = x\phi_K \quad \text{and} \quad x\phi_K{}^+ = x \quad \text{in case of} \quad x \geq x\phi_S\,.$$

Here, by definition, $\psi_K{}^-$ is an order automorphism of $\mathcal{K}$, inverse to some positive order automorphism of $\mathcal{K}$. But then $\phi_K = \phi_K{}^+ \circ \psi_K{}^-$ belongs to the quotient hull of $\mathfrak{R}^+(\mathcal{K})$, which is divisible. $\square$

Finally we remark: The preceding results entail

6. 3. 8 Corollary. *Any positive d-monoid is embedded in a homomorphic image of some ℓ-group cone.*

PROOF. We consider the above presented situation of $\mathcal{K}$ in $\mathcal{S}(\lambda)$. Here any positive order automorphism α of $\mathcal{S}(\lambda)$ in a uniquely manner generates an ideal/filter isomorphism $h(\alpha)$ of $\mathcal{K}$, and it is easily seen that h respects meet and multiplication. $\square$

6.4 Further Consequences

The preceding section provides – as consequences – several most classical corollaries

6. 4. 1 Corollary. *Any commutative d-semigroup $\mathfrak{S}$ is a subdirect product of* 0*-cancellative linearly ordered components.*

PROOF. Consider the c-ideal K of 6.2.2. Here by commutativity, this ideal is *invariant*, that is, it satisfies $K \cdot x = x \cdot K$.

We suppose first that D/K has a maximum and thereby necessarily an idempotent element $\overline{u}$. Here we put $\overline{0} := \{x \,|\, \overline{x} \geq \overline{u}\}$ and define $\overline{a} \cdot \overline{0} = \overline{0} = \overline{0} \cdot \overline{a}$ and $\overline{0} \wedge \overline{a} = \overline{a}$.

Finally, in the remaining case $\overline{0} := \{x \,|\, x \notin D\}$ produces a residue class image. □

6. 4. 2 Corollary. *Any positive commutative d-semigroup $\mathfrak{S}$ admits an embedding in a brick.*

PROOF.We may start from a d-monoid. Then we get a 0-cancellative homomorphic image $\overline{\mathfrak{S}}$ of $\mathfrak{S}/K$ by putting $\overline{0} := \{x \,|\, \overline{x} \geq \overline{b}\}$ in $\mathfrak{S}/K$.

Now we form the lexicographical product of $\overline{\mathfrak{S}}$ and $(\mathbf{Z}\,,+\,,\min)$ and consider the substructure of all elements above $(\overline{1} \,|\, 0)$. Then it is easily checked that this is a positive d-semigroup. Next we define $O := \{(\overline{x} \,|\, u) \,|\, (\overline{x} \,|\, u) \geq (\overline{a} \,|\, 1)\}$ thus getting a homomorphic image, containing the starting model as a substructure. □

6. 4. 3 Corollary. *Let $\mathfrak{S}$ be* locally finite, *that is let any element $a \in S$ have only finitely many powers. Then $\mathfrak{S}$ is a subdirect product of strictly archimedean, cf. definition 9.3.1, linearly ordered d-semigroups.*

PROOF. Assume for instance $a \in S$ and $a^n = a^n \cdot a^k$. Then it results $a^{nk} = (a^{nk})^2$, whence on the one hand any element a has an idempotent unit and on the other hand any c-ideal is invariant, as is easily seen. Consequently – according to 5.4.1 – any subdirectly irreducible model $\mathfrak{S}$ of this type is a d-monoid with zero . Furthermore, since any $1 \wedge a$ has only finitely many powers, it must hold in general $1 \wedge a = 1 \leadsto 1 \leq a$, whence $\mathfrak{S}$ is positive.

So, $\mathfrak{S}$ is strictly archimedean. □

But recall: The preceding proposition is, of course, also an immediate consequence of 5.2.7.

6. 4. 4 Corollary. *Any finite d-semigroup is a subdirect product of components of type $S_n = (\{0, 1, ..., n\},\ a \cdot b := \min(a + b, n),\ a \wedge b := \min(a, b))$.*

PROOF. This is an immediate consequence of 6.4.3. □

We now turn to historical theorems on ℓ-groups and lattices, which are first formulated simultaneously and then discussed simultaneously.

6. 4. 5 (A. H. Clifford). *Any abelian ℓ-group is representable, that is has a subdirect decomposition into linearly ordered groups.*

6. 4. 6 (W. Ch. Holland). *Any ℓ-group is embedded in an order automorphism group of some chain.*

6. 4. 7 (Lorenzen & Šik). *An ℓ-group is a subdirect product of linearly ordered groups iff it satisfies:*

$$\text{(LS)} \qquad (1 \vee a^{-1}b) \wedge x^{-1}(1 \vee b^{-1}a)x = 1\,.$$

6. 4. 8 (G. Birkhoff). *Any d-lattice may be considered as a ring of sets.*

6. 4. 9 (M. H, Stone). *Any boolean lattice may be considered as a field of sets.*

Each of the preceding corollaries results from the representation theorem, if one recalls that any $0, 1$-*series* may be considered as a subset of its index set. Only 6.4.7 needs some explanation:

Obviously (LS) is necessary, but (LS) is also sufficient, since by (LS) it follows:

$$a \wedge b = 1 \implies a \wedge x^{-1}bx = 1\,,$$

whence the essential steps of the representation theorem carry over, if we work with invariant c-ideals, that is *convex normal divisors,* instead of arbitrary c-ideals.

Chapter 7

Complete d-semigroups

7.1 Completeness and Cone

We turn to d-semigroups, satisfying certain completeness conditions.

7. 1. 1 Definition. A lattice is called *conditionally complete* if it has no *gaps,* that is if any upper bounded subset is upper limited, that is has a least upper bound. A conditionally complete lattice is called $\vee$-*distributive,* here, if it satisfies:

(D$\vee$) $$s = \bigwedge a_i \ \ (i \in I) \implies x \vee s = \bigwedge (x \vee a_i) \ \ (i \in I)\,.$$

Dually the notion of a conditionally complete $\wedge$-*distributive* lattice and the axiom (D$\wedge$), respectively, are defined.

Furthermore a conditionally complete lattice is called *infinitely distributive* if for existing limits the following two equations are satisfied:

(DV1) $$\bigwedge_C \Big[\bigvee_{A_\gamma} a_{\gamma,\alpha}\Big] \ = \ \bigvee_\Phi \Big[\bigwedge_C a_{\gamma,\phi(\gamma)}\Big]$$

(DV2) $$\bigvee_C \Big[\bigwedge_{A_\gamma} a_{\gamma,\alpha}\Big] \ = \ \bigwedge_\Phi \Big[\bigvee_C a_{\gamma,\phi(\gamma)}\Big]\ ,$$

where γ runs through the set C and Φ runs through the set of all mappings ϕ of C into the union of all A_γ with $\phi(\gamma) \in A_\gamma$.

Obviously any conditionally complete *chain* is infinitely distributive, and thereby also $\vee$- and $\wedge$-distributive.

Recall, opposite to the finite case (D$\vee$) and (D$\wedge$) are independent. Consider f.i. the system of all closed subsets of the *Euclidean space and define as* $\bigvee A$

the hull of A. Here the set C of all points $(x|y)$ satisfying $x^2+y^2=1$, w.r.t. the sets C_k of type $x^2+y^2 \leq 1-k^{-2}$ $(k \in \mathbf{N})$ – in the lattice of all closed subsets of the plane – provides the inequality $C \cap \bigvee C_k = C \neq \emptyset = \bigvee (C \cap C_k)$.

7. 1. 2 Definition. A d-semigroup $\mathfrak{S}$ is called *conditionally complete* if its lattice is conditionally complete.

A d-semigroup is called *complete,* if its lattice is conditionally complete and if moreover it holds:

(DW) $$s = \bigwedge a_i \ \ (i \in I) \implies xsy = \bigwedge xa_iy \, (i \in I)\,.$$

Instead of complete we also will say $\bigwedge$-*complete*, and we dually define axiom (DV) and the notion $\bigvee$-*complete.*

Let $\mathfrak{S}$ be conditionally complete and assume that moreover the equations (DW) and (DV) are valid. Then $\mathfrak{S}$ is called *continuous*, here. By analogy we define *inf-continuous* and *sup-continuous.*

As a first result we get – compare 2.8.6 –

7. 1. 3 Proposition. *Let* $\mathfrak{B}$ *be a brick with complete lattice* $(B, \leq)$. *Then* $\mathfrak{B}$ *considered as d-semigroup is even continuous.*

Furthermore we get:

7. 1. 4 Proposition. *A d-semigroup* $\mathfrak{S}$ *is* (*already*) *conditionally complete if its cone is conditionally complete.*

PROOF. We show that lower bounded families (a_i) $(i \in I)$ are inf-bounded. To this end let s be a lower bound of (a_i) $(i \in I)$ and let e be a positive unit of s. Then we get in $\mathfrak{S}$ and $\mathfrak{S}^1$, respectively:

$$\begin{array}{rrcl} & (i) \quad \big(\bigwedge(e \vee a_i)\big)\, e & = & \bigwedge(e \vee a_i) \ =: d \\ \text{and} & (ii) \quad {a_i}' := e(1 \wedge a_i)^{-1} & \leq & e(1 \wedge s)^{-1} =: s'\,. \end{array}$$

Observe: (i) results by into-multiplying e and (ii) results since e commutes with $1 \wedge s$ and e and $1 \wedge a_i$ and because all elements of type $u(1 \wedge v)^{-1}$ $(u \in S)$ belong to S. Furthermore we may assume that in (ii) all elements ${a_i}'$ are positive, and thereby that also the element s' is positive.

We put $a' := \bigvee a'_i$. Then a' is a left divisor of e. Furthermore, if f is a positive unit of e, it follows $s'(1 \wedge s)f = e(1 \wedge s)^{-1}(1 \wedge s)f = ef = e$, and it holds $e^2 = e(1 \wedge s)(1 \wedge s)^{-1}e = (e \wedge s)s'$ with $s' \geq a'$, that is $e^2 = ta'$.

Consequently we may suppose that $e = a'y$ with $y \geq 1 \wedge s$ and $e^2 = ta'$.

We will show, that

$$g := dy = de^2y = dta'y$$

satisfies the conditions of $\inf(a_i)$. To this end observe that

$$s = (1 \vee s)(1 \wedge s) \leq dy = g$$

is satisfied, and that furthermore any fixed $a_j \ (j \in I)$ satisfies

$$\begin{aligned} a'y &= e \leq e^2 \\ &= e(1 \wedge a_j)^{-1} \cdot (1 \wedge a_j)e \\ &\leq a' \cdot (e \wedge a_j) \end{aligned}$$

Hence it results next:

$$\begin{aligned} g &= dta'y \\ &\leq dta'(e \wedge a_i) \\ &= d(e \wedge a_i) \\ &\leq (e \vee a_i) \cdot (e \wedge a_i) \\ &= a_i \ (\forall i \in I)\,. \end{aligned}$$

Recall now, that d, a', and t are exclusively determined by the unit e and the family $(a_i) \ (i \in I)$. This means that $u \leq a_i \ (i \in I)$ implies $u \vee s \leq a_i \ (i \in I)$ and $e(u \vee s) = u \vee s = (u \vee s)e$. Hence, starting from $u \vee s$ instead from s we get the same dy and thereby $u \vee s \leq g$. But this means $u \leq g$, that is $g = \inf(a_i) \ (i \in I)$. □

By 7.1.4 the natural question arises how far the distributivity laws above are carried over to "the whole". Here we obtain

7. 1. 5 Proposition. *If $\mathfrak{S}$ is conditionally complete, then each of the D-laws above is carried over from the cone to the "whole".*

PROOF. We prove by example, studying the case of completeness. First it holds: If $s = \bigwedge a_i \ (i \in I)$ then it results $s = \bigwedge(a_i)$ in $\mathfrak{S}^1$, since together with x also all αx belong to S. Moreover for all invertible elements α and all $i \in I$ we get $y \leq \alpha a_i \Longleftrightarrow \alpha^{-1} y \leq a_i$, that is $\alpha \bigwedge a_i = \bigwedge \alpha a_i$. But putting $\alpha := (1 \wedge x \wedge s)^{-1}$ this implies:

$$\begin{aligned} x \bigwedge a_i &= \alpha^{-1}(\alpha x \bigwedge a_i)\alpha\alpha^{-1} \quad (i \in I) \\ &= \alpha^{-1}(\bigwedge \alpha x a_i \alpha)\alpha^{-1} \\ &= \bigwedge(\alpha^{-1}\alpha x a_i \alpha\alpha^{-1}) \\ &= \bigwedge x a_i \ (i \in I)\ , \end{aligned}$$

recall $a_i\alpha \in S^+$ and $\alpha x \in S^+$. So, we are finished w. r. t. (DW) by right/left duality.

In the same manner we succeed in the remaining cases. □

7.2 Continuous d-Semigroups

The main structure of this section will be that of a *continuous d-semigroup.*

7. 2. 1 Definition. By an inf-continuous d-semigroup we mean a conditionally complete d-semigroup, satisfying (D1$\wedge$),..., (D4$\wedge$), and accordingly by a sup-continuous d-semigroup we mean a conditionally complete d-semigroup, satisfying (D1$\vee$),..., (D4$\vee$).

A d-semigroup is called continuous if it is both, inf- and sup-continuous.

The main theorem of this section tells:

Continuous d-Semigroups are commutative.

7. 2. 2 Definition. A d-semigroup is called *archimedean*, if it satisfies:

(A) $$a^n \leq b \ \ (\forall\, n \in \mathbf{N}) \implies ab\,,\, ba \leq b\,.$$

7. 2. 3 Proposition. *A d-semigroup is* (*already*) *archimedean, if the implication holds:*

(A$^+$) $$a^{+^n} \leq b^+ \ \ (\forall\, n \in \mathbf{N}) \implies a^+b^+ = b^+ = b^+a^+\,.$$

PROOF. Obviously (A) implies (A^+) and if (A^+) is satisfied in case of $ea = a = ae$ it results in a first step $eb = b = be$, that is by 2.2.4 even $a^n \leq b \Longrightarrow e^n \cdot a^n \leq e^n \vee b = e \vee b$ and thereby

$$\begin{aligned} a^n \leq b \ (\forall n \in \mathbf{N}) &\Longrightarrow (e \vee a)^n \leq e \vee b \ (\forall n \in \mathbf{N}) \\ &\Longrightarrow (e \vee a)(e \vee b) = e \vee b \\ &\Longrightarrow (e \vee a)b = (e \vee b)(e \wedge b) = b \\ &\Longrightarrow ab \leq b \qquad (\& \, ba \leq b)\,. \end{aligned}$$ □

7.2.3 entails next:

7. 2. 4 Proposition. *If $\mathfrak{S}$ is archimedean then also the identity extension and the quotient extension of $\mathfrak{S}$ are archimedean.*

PROOF. As to the identity extension we have to refer (in advance) to 8.3. 2, but with respect to the quotient hull the equation: $(a \cdot b^{-1})^n \leq c \Longrightarrow a^n \leq c \cdot b^n \Longrightarrow a^n \leq c\,.$ □

Next two crucial results:

7. 2. 5 Proposition. *Complete – recall, that is $\bigwedge$-complete – d-semigroups are archimedean.*

PROOF. Let $a^n \leq b$ $(\forall\, n \in \mathbf{N})$ be satisfied, where a, b are positive, and suppose $a^n c_n = b$ $(n \in \mathbf{N})$. Then in a first step we replace c_n by $c_0 \wedge \ldots \wedge c_n =: d_n$ and afterwards in a second step we replace this d_n by $a \vee d_n =: a_n$. In particular thus we get $c_0 = b$ and $a_0 = b$, and it results furthermore that the chosen elements satisfy $a_{n+1} \leq a_n$. Consequently we may start from

$$a_n = a_{n+1} \cdot x_{n+1}$$

and thereby from

$$\begin{aligned} a \cdot b &= a \cdot a^n \cdot a_n \\ &= a^{n+1} \cdot a_{n+1} \cdot x_{n+1} \\ &= b \cdot x_{n+1}\,. \end{aligned}$$

Putting

$$x := \bigwedge x_n \ (n \in \mathbf{N})$$

we get next

$$a \cdot b = b \cdot x\,.$$

Now we choose elements v_n satisfying

$$x_{n+1} = v_{n+1} \cdot x\,,$$

in order to show $\quad b \cdot x = b\,.$

To this end we define

$$\begin{aligned} b_0 &:= a_1 \cdot v_1 \cdot x \\ &= a_1 \cdot x_1 = a_0 \cdot 1 = b \\ b_1 &:= a_1 \cdot v_1 \end{aligned}$$

and assume that a chain $\quad b_0 \geq b_1 \geq \ldots \geq b_n$

is constructed, satisfying

$$\begin{aligned} b_i &= a_i \cdot z_i \qquad (0 \leq i \leq n) \\ b_i &= b_{i+1} \cdot x \quad (0 \leq i \leq n-1)\,. \end{aligned}$$

Then we get:

$$\begin{aligned} a_n &= a_{n+1} \cdot x_{n+1} \\ &\rightsquigarrow \\ b_n &= a_{n+1} \cdot v_{n+1} \cdot x \cdot z_n \\ &= (a_{n+1} \cdot v_{n+1} \cdot {z_n}') \cdot x\,. \end{aligned}$$

Put now $v_{n+1} \cdot {z_n}' =: z_{n+1}$ and define $b_{n+1} := a_{n+1} \cdot z_{n+1}$. Then it results

$$\begin{aligned} b_{n+1} &\leq b_n \\ b_{n+1} &= a_{n+1} \cdot z_{n+1} \\ &\& \\ b_n &= b_{n+1} \cdot x\,. \end{aligned}$$

But by

$$\begin{aligned} (\bigwedge_{n \in N} b_n) \cdot x &= \bigwedge (b_n \cdot x) \\ &= \bigwedge b_{n-1} = \bigwedge b_n \leq b \end{aligned}$$

this leads to $\quad a \cdot b = b \cdot x = b\,.$

Hence by duality it results:

$$a \cdot b = b = b \cdot a$$

which completes the general proof. □

7. 2. 6 Proposition. $\bigvee$-*complete d-semigroups are archimedean.*

PROOF. Let $a^n \leq b$ $(\forall n \in \mathbf{N})$ be satisfied. Then it holds $\bigvee a^n \leq b$ and $a \bigvee a^n = \bigvee a^n$, which means $ab \leq b$, and by duality we get $ba \leq b$. □

The proof of 7.2.6 is trivial. This leads to the conjecture that even weaker conditions than $\bigvee$-completeness imply the archimedean property. In fact – this is true.

7. 2. 7 Proposition. *Let $\mathfrak{S}$ be a conditionally complete d-semigroup $\mathfrak{S}$ with maximal right and maximal left units for all $a \in S$. Then $\mathfrak{S}$ is archimedean.*

PROOF. Let u be a maximal and thereby the maximal right unit and let v be the maximal left unit of b. Then u and v are positive and thereby idempotent, that is in particular central elements. So they are equal.

Let now w. l. o. g. $\mathfrak{S}$ be positive and suppose that $a^n \leq c$ $(\forall n \in \mathbf{N})$ is valid and that u is the maximal unit of c. Then it holds also $(au)^n \leq c$ $(\forall n \in \mathbf{N})$, whence we may start from $a = au$.

Furthermore for each pair $x \neq y$ with $xu = x$ & $yu = y$ and thereby also with $(x \wedge y)u = x \wedge y$ it holds the conditional cancellation law $sx = sy \leq c \Longrightarrow x = y$. Recall that in case of $R(x, y, x', y')$ it results $sx = s(x \wedge y) = sy$, that is $s(x \wedge y)x' = s(x \wedge y)$, whence by assumption x' and thereby y' as well are right units of c below u, that is satisfying $ux' = u = uy'$. Consequently we obtain $x = (x \wedge y)x' = (x \wedge y)ux' = (x \wedge y)uy' = (x \wedge y)y' = y$.

Let now b be the LUB of $(au)^n$ and suppose $(au)^n \cdot x_n = b$ $(n \in \mathbf{N})$. Then by conditional cancellation we get $x_n = (au) \cdot x_{n+1}$, which means $x_1 \geq \bigvee (au)^n$, that is $x_1 \geq b$ and thereby $b = (au)x_1 \geq (au)b \geq ub \geq b \leq c$, that is $au \cdot c = c \rightsquigarrow ac = c$.

The rest follows by right/left duality. $\square$

It is nearly immediately seen, that 7.2.6 results from 7.2.7.

As a special case w.r.t. the preceding proposition we present:

7. 2. 8 Lemma. *Let $\mathfrak{S}$ be totally ordered, dense and conditionally complete. Then $\mathfrak{S}$ is $\bigvee$-complete. In particular in this case any $a \in S$ has a maximal left unit l and a maximal right unit r.*

PROOF. We consider the positive case and suppose $\bigvee(ab_i) < a \cdot \bigvee b_i$. Then by density there exists some c strictly between $\bigvee(ab_i)$ and $a \cdot \bigvee b_i$, satisfying $c = au$. But then u is an upper bound of $\{b_i\}$, whence it results $c = \bigvee b_i$, a contradiction.

The rest follows by duality. $\square$

The requirement of density is necessary. For adjoin the elements $p \neq p^2$ to the set $\mathbf{N}^0$ and define $n \leq p, p^2, np = p = pn, np^2 = pp = p^2 = p^2 n$. Thus an archimedean, commutative and complete totally ordered d-monoid is generated in which there doesn't exist a maximal (right) unit of p. And moreover the example under consideration is not $\bigvee$-complete.

By the way, linear conditionally complete d-semigroups need not be $\bigwedge$-complete, as will be shown under 9.4.4. However, contrary, dense linear conditionally complete d-semigroups are $\bigwedge$-complete – which is shown by analogy to the proof of 7.2.8.

AND OBSERVE associativity is not required, neither here nor under 7.2.8 HOWEVER:

7. 2. 9 Proposition. *Any conditionally complete linear d-semigroup $\mathfrak{S}$ is archimedean.*

PROOF. Let $1 \leq a \leq S := \bigvee\limits_{n \in N} a^n \leq b$. Then there exists some $s \leq S$ with $as = S$.

In case of $s = S$ we are through. Otherwise we conclude $s < S \leq b$ and $a^k \leq s < a^{k+1} \leq S \leq b \ \ (\exists\, k \in \mathbf{N})$, leading to

$$aSa = a \cdot as \cdot a \leq a \cdot a^{k+1} \cdot a \leq S \Longrightarrow a \cdot S = S = S \cdot a \Longrightarrow ab = b = ba\,. \ \Box$$

Completeness and the archimedean property have in common that in case of $a^n \,|\, b \ \ (\forall n \in \mathbf{N})$ they guarantee a smallest u among all elements x satisfying $ba = bx$, that is the existence of $b * ba =: u$ and dually of $ab : b =: v$. Starting from this property we get:

7. 2. 10 Proposition. *A conditionally complete d-semigroup satisfying that $a^n \,|\, b \ \ (\forall n \in \mathbf{N})$ implies the existence of $b * ba =: u$ and $ab : b =: v$ is archimedean if in addition right units are left units and vice versa.*

PROOF. Let $a^n \,|\, b \ \ (\forall n \in \mathbf{N})$ and $u = b{*}ba$, that is in particular $u^n{*}u^n{\cdot}u = u$. Then we get $u \cdot c = \bigvee u^n \Longrightarrow \bigvee u^n \mid c \Longrightarrow \bigvee u^n = c \Longrightarrow u \cdot c = c \Longrightarrow u \cdot b = b = b \cdot u$, that is $ab = b = ba$. $\Box$

OBSERVE: In the commutative case the preceding proof offers a valuable abbreviation of the proof under 7.2.5.

We now turn to the commutativity proof for complete d-semigroups. It will be based on special congruences. In particular decompositions by idempotents and decompositions of positive d-semigroups by some a^d, will turn out to be crucial.

First of all we get nearly immediately:

7. 2. 11 Lemma. *Let $\mathfrak{S}$ be a conditionally complete d-semigroup, and let $u = u^2$. Then $\mathfrak{S} \cdot u$ is conditionally complete, too, even more, then* $\inf(a_i \cdot u)$ *and* $\sup(a_i \cdot u)$ *in $\mathfrak{S}$ and $\mathfrak{S} \cdot u$ coincide.*

So, if moreover $\mathfrak{S}$ is $\bigwedge$- or $\bigvee$-complete then any homomorphism $\mathfrak{S} \longrightarrow \mathfrak{S} \cdot u$ maps LUBs to LUBs and GLBs to GLBs.

Hence in particular a continuous $\mathfrak{S}$ has a continuous image $\mathfrak{S} \cdot u$.

7. 2. 12 Proposition. *Any continuous d-semigroup has a limit respecting decomposition into continuous d-monoids.*

PROOF. Suppose that $a \neq b$ and that u is the maximum of all units of $a \wedge b$. Then $u = u^2$ is the identity of $\mathfrak{S} \cdot u$ and $\mathfrak{S} \cdot u$ separates the elements $a = au, b = bu$. □

Now we consider special situations.

7. 2. 13 Proposition. *Let $\mathfrak{S}$ be a sup-continuous d-semigroup. Then any pair x, y of incomparable elements produces at least one pair of x, y separating homomorphic images $\overline{\mathfrak{S}}, \overline{\overline{\mathfrak{S}}}$ with*

$$\overline{x} \leq \overline{y} \ \&\ \overline{\overline{y}} \leq \overline{\overline{x}} \quad \textit{and} \quad \overline{y\,'} \neq \overline{1} \ \&\ \overline{\overline{x\,'}} \neq \overline{\overline{1}}\,.$$

PROOF. We shall show that idempotent elements u, v do exist such that $\mathfrak{S} \cdot u, \mathfrak{S} \cdot v$ separate x, y .

So, let x, y be incomparable with $R(x, y, x\,' \geq 1, y\,' \geq 1)$. Then the set U of all positive u_i $(i \in I)$ satisfying $(x \wedge y)(x\,' \wedge u_i) = x \wedge y$ is not empty, since $y\,'$ belongs to U. We put $\bigvee u_i$ $(i \in I) =: u$. Then it follows

$$\begin{aligned} (x \wedge y)(x\,' \wedge u) &= (x \wedge y) \bigvee (x\,' \wedge u_i) \\ &= \bigvee ((x \wedge y)(x\,' \wedge u_i)) \\ &= x \wedge y\ , \end{aligned}$$

that is $u \in U$.

But, it holds $x\,' \wedge u^2 \leq (x\,' \wedge u)^2$. Hence, u^2 belongs to U as well. This entails $u^2 = u \geq u_i$ $(i \in I)$.

Now we consider the set V of all positive v_i $(i \in I)$ satisfying the identity $(x \wedge y)(v_i \wedge u) = x \wedge y$. Then by analogy V contains an idempotent maximum v, say, and it follows by construction

$$x\,' \leq v \quad \& \quad y\,' \leq u\,,$$

that is
$$\begin{array}{rrcl} & xv & = & (x \wedge y)x'v \\ & & = & xv \wedge yv \\ \rightsquigarrow & xv & \leq & yv \end{array}$$
and dually
$$xu \geq yu \,.$$

Suppose now
$$xu = yu \quad \text{and} \quad xv = yv \,,$$

and thereby
$$(x \wedge y)(u \wedge v) = x \wedge y \,.$$

Then it results:
$$\begin{array}{rcl} x = x(u \wedge v) & = & xu \wedge xv \\ & = & yu \wedge yv = y(u \wedge v) = y \,, \end{array}$$

a contradiction! So – putting $\mathfrak{S} \cdot v =: \overline{\mathfrak{S}}$ and $\mathfrak{S} \cdot u =: \overline{\overline{\mathfrak{S}}}$ – the first part is proven.

But it holds $x' \not\leq u$ and $y' \not\leq v$, since for instance $x' \leq u$ leads to $x' \leq u \wedge v$ and thereby to $x = (x \wedge y)x' \leq (x \wedge y)(u \wedge v) = x \wedge y$, that is to $x \leq y$, again a contradiction! Thus, by left/right duality we are through. $\square$

In the remainder of this section we will denote the homomorphic image of $\mathfrak{S}$ w. r. t. the principal ideal a^d by $\mathfrak{S}_a$.

7. 2. 14 Lemma. *Let $\mathfrak{S}$ be a conditionally complete positive d-semigroup. Then each $\mathfrak{S}_a$ is conditionally complete, too. Let now ϕ_a be the corresponding homomorphism. Then ϕ_a in any case maps GLBs onto GLBs, and if $\mathfrak{S}$ satisfies in addition $(D\wedge)$, then it maps in addition LUBs onto LUBs.*

Now we are in the position to prove:

7. 2. 15 Proposition. *Any continuous d-semigroup is commutative.*

PROOF. We show step by step:

(i) If there exists a non commutative continuous d-semigroup, then there exists even a positive non commutative continuous d-monoid with zero element 0, satisfying for at least one pair p, q
$$1 < p < q < pq < qp = 0$$
and having in addition 1 as maximal unit e_{pq} of pq.

(*ii*) If there exists a non commutative continuous d-semigroup, then there exists even a model satisfying the conditions of (*i*) and in addition for at least one pair a, b :

$$1 < s := ab * ba \le a < b < ab < ba = 0 \text{ and } e_{ab} = 1$$

and for at least one element x and suitable natural numbers $k,\ \ell,\ m$:

(1) $x^k \le s \le x^{k+1}$

(2) $x^\ell \le a \le x^{\ell+1}$

(3) $x^m \le b \le x^{m+1}$.

(*iii*) The pair s, x of (*ii*) satisfies $s < x^2$.

(*iv*) The pair s, x of (*ii*) may be assumed in addition to satisfy $x^2 \le s$.

Thus according to (*iii*) and (*iv*) a contradiction is constructed.

A Remark: In what follows at many places we will consider endomorphisms of type $a \longmapsto a \cdot e$ with idempotent e. So, the reader should recall, that these endomorphisms provide *continuous archimedean images* and that they are moreover – according to 5.2.9 – also $*$, $:$-homomorphisms.

Furthermore we mention that in archimedean d-monoids the elements a, b, ab, ba are even pairwise different, if only the elements ab and ba are different.

Clearly $ab \ne ba \Longrightarrow a \ne b$, but $a = ab$ is impossible, too, in case of $ab \ne ba$, since the archimedean property would imply $ab = bab = ba$, whence by duality we are through.

Now we start proving (*i*) through (*iv*).

Ad (*i*). **First of all** according to 2.4.2 and according to our remark above there exists a positive model with at least one $1 < p < q$ and $pq \ne qp$. This provides – again by our remark above and by 7.2.13 – a starting model $\mathfrak{T}$ with

$$1 < p < q < pq < qp \qquad \text{or} \qquad 1 < p < q < qp < pq\ .$$

Suppose now $qp < pq$. Then we turn to the left/right dual model by $x \circ y := yx$. Thus – in any case – we get a model $\mathfrak{T}_1$, satisfying the first part of the assertion.

Now we form $(\mathfrak{T}_1)_{pq}$. This way, by continuity and by 7.2.14 we are led from $\mathfrak{T}_1$ to a homomorphic model $\overline{\mathfrak{T}}$, satisfying in addition $\overline{pq} = \overline{0}$.

Furthermore by sup-continuity $\overline{pq}$ has a maximum unit in $\overline{\mathfrak{T}}$, say $\overline{e}$. in $\overline{\mathfrak{T}}$ This entails $\overline{pq}\cdot\overline{e} \neq \overline{qp}\cdot\overline{e}$. Hence $\overline{\mathfrak{T}}\cdot\overline{e}$ is a model according to (i).

Ad (ii). **Next** we consider a d-monoid $\mathfrak{T}$, constructed along the lines of (i) and replace $\overline{x}$ generously by x. Moreover we start from some y satisfying $1 < y \leq s$. Then, if $y^k \leq s \leq y^{k+1}$ $(\exists k \in \mathbf{N})$, y in the role of x satisfies condition (1).

Otherwise, by the archimedean property and condition $e_{pq} = 1$ there must exist some k with:

$$y^k \leq s \text{ and } s \not\leq y^{k+1} \ \& \ y^{k+1} \not\leq s\,,$$

whence by 7.2.13 we are led to a homomorphic image with $\overline{y}^k \leq \overline{s} \leq \overline{y}^{k+1}$. But the homomorphism under consideration is a $*$-homomorphism, too, satisfying $\overline{s} * \overline{y}^{k+1} \neq \overline{1}$, recall 7.2.13. Hence the elements pq and qp remain separated, because $1 \neq s * y^{k+1} \leq y^k * y^{k+1} \leq y \leq s$. Consequently we get moreover:

$$\overline{1} < \overline{y}^k \leq \overline{s} = \overline{pq} * \overline{qp} \leq \overline{y}^{k+1} \ \& \ \overline{s} \leq \overline{p} < \overline{q} < \overline{pq} < \overline{qp} = \overline{0}\,.$$

If in addition $\overline{y}^{k+1} \geq \overline{p}$ is satisfied, we are through w. r. t. $\overline{p}$. Otherwise there exists some ℓ, satisfying $\overline{y}^{\ell} \leq \overline{p}$ and $\overline{y}^{\ell+1} \not\leq \overline{p}$ & $\overline{p} \not\leq \overline{y}^{\ell+1}$. Consequently we are in the position to continue the procedure until next $\overline{p}$ is "captured" and finally also $\overline{q}$ and $\overline{pq}$ are "captured".

Ad (iii). **Let now $\mathfrak{S}$ be the model**, constructed below (ii).

We show, as announced, that in this model $s < x^2$ must be satisfied, which results as follows:

If a or b is a power of x, then for some suitable n it holds

$$x^n \leq ab \leq x^{n+1} \quad \& \quad x^n \leq ba \leq x^{n+1}\,,$$

that is $s = ab * ba \leq x$. Because $x = x^2 \Longrightarrow x^n = x^{n+1} \Longrightarrow ab = ba$ this entails $x < x^2$ and thereby $s < x^2$.

$$\begin{array}{lrcl} \text{Otherwise we obtain} & b & = & x^m(x^m * b) \\ \text{with} & x & \geq & x^m * x^{m+1} \geq x^m * b \\ \text{and} & x^2 & = & (x^m * b)((x^m * b) * x^2)\,. \end{array}$$

But putting $y := (x^m * b) * x^2 \leq x^2$ this implies:

$$\begin{array}{rcl} aby & = & ax^m(x^m * b)((x^m * b) * x^2) \\ & = & ax^m x^2 \\ & \geq & x^\ell x^m x^2 \\ & = & x^{m+1}x^{\ell+1} \\ & \geq & ba \end{array}$$

and thereby:
$$s = ab * ba \;\leq\; y \leq x^2 \,.$$

Suppose now $s = x^2$. Then by $x \leq a < b$ it follows first $ab \geq x^2$ which in case of $y = x^2$ leads to the contradiction:

$$\begin{array}{lrcl} & (x^m * b)x^2 & = & (x^m * b)y = x^2 \\ \rightsquigarrow & (x^m * b)ab & = & ab \\ \rightsquigarrow & x^m * b & = & 1 \\ \rightsquigarrow & x^m & \geq & b \\ \rightsquigarrow & x^m & = & b\,. \end{array}$$

So, in any case it must hold $s < x^2$.

Ad (*iv*). **Finally**, let again $\mathfrak{S}$ be the model of (*ii*). We show that in this model $x^2 \leq s$ is possible. To this end it suffices, of course, to construct, starting from $\mathfrak{S}$, a model, satisfying for some element z the $\leq, <$-relation $1 < z^2 \leq s := ab * ba$, since in this case we could choose exactly this element z in the role of x. But in $\mathfrak{S}$ we have $ab \neq ba$. Hence a and b cannot together be powers of x. Hence it must hold

$$(7.7) \qquad 1 < x^\ell * a < x \qquad \text{or} \qquad 1 < x^m * b < x\,.$$

For $1 = x^\ell * a$ implies $x^\ell \geq a$, that is $a = x^\ell$, and $x^\ell * a = x$ would imply $a = x^{\ell+1}$. This proves (7.7), by symmetry.

Thus in any case there exists some z with $1 < z < x \leq s$, say for instance w. l. o. g. $z = x^\ell * a$. Provided, now, it holds $z^2 \leq s$, then we are through.

Otherwise we consider $r := z \wedge z * x$. It holds $r^2 \leq x$ and in case of $r \neq 1$, we are through again.

In the remaining case it holds $r = 1$, that is the elements z and $z * x$ are coprime, whence also the elements z^2 and $z * x$ are coprime. But this means, recall $1 < z * x \leq s$,

$$z^2 \not\leq s \;\;\&\;\; s \not\leq z^2\,.$$

Now we decompose $\mathfrak{S}$ in the sense of 7.2.13 w.r.t. the elements $z^2\,, s$.

Here we may assume $\overline{z}^2 \leq \overline{s}$ and $\overline{s} \neq \overline{1}$, by $\overline{z}^2 * \overline{s} \neq \overline{1}$. Therefore by our remark it results $\overline{1} < \overline{s} = \overline{ab} * \overline{ba} \leq \overline{a} < \overline{b} < \overline{ab} < \overline{ba}$. So, we may stop if $\overline{z} \neq \overline{1}$.

Otherwise it holds $\overline{z} = \overline{x}^\ell * \overline{a} = \overline{1}$, that is $\overline{a} = \overline{x}^\ell$, and $\overline{a} \cdot \overline{b} \neq \overline{b} \cdot \overline{a}$. So, there exists a model with

$$1 = x^\ell * a < x \quad \text{and} \quad 1 < x^m * b < x\ .$$

But this means, that repeating the procedure by starting from $\overline{z} = \overline{x}^m * \overline{b}$ leads to a model of the desired type. $\square$

Chapter 8

Archimedean d-semigroups

8.1 Commutativity

In this chapter it is shown, that any archimedean d-semigroup is commutative. This will be done by leading back the general situation to the special situation of the preceding chapter. Moreover, according to 2.4.2, we may restrict our attention to positive d-semigroups and thereby to positive d-monoids. So, let in this section $\mathfrak{S} := (S, \cdot, \wedge)$ be always a d-monoid.

8. 1. 1 Definition. Let 0 be an arbitrary element of S. Then by $E(0)$ we mean the set of all right units of 0.

Obviously $E(0)$ is always a c-ideal, however, not necessarily invariant, that is of type $E(0) \cdot S_0 = S_0 \cdot E(0)$ w. r. t. $S_0 := \{x \mid x \leq 0\}$.

In the positive case the d-ideal congruence $a \equiv b\ (0)$ is equivalent to $0 \wedge a = 0 \wedge b$. Hence $a \circ b := 0 \wedge ab$ defines a d-semigroup on S_0.

8. 1. 2 Proposition. *Let* 0 *belong to* S, *suppose that any right unit of* 0 *and also any left unit of* 0 *is even a unit of* 0 [1]. *Finally let* $E(0)$ *be an ideal of* $\mathfrak{S}_0$. *Then* $\overline{\mathfrak{S}}_0 := \mathfrak{S}_0/E(0)$ *is a brick.*

PROOF. We prove first, that $\overline{\mathfrak{S}}_0$ is complementary, that is we show that there is always a smallest $\overline{x}$ satisfying $(\overline{a} \wedge \overline{b}) \circ \overline{x} = \overline{b}$, denoted by $\overline{a} * \overline{b}$, and dually a smallest $\overline{z}$ satisfying $\overline{z} \circ (\overline{a} \wedge \overline{b}) = \overline{b}$, denoted by $\overline{b} : \overline{a}$. To this end

[1] This is, of course, the case, if $\mathfrak{S}$ is archimedean.

suppose $(a \wedge b)x = b \leq 0$ and $\overline{a} \circ \overline{y} \geq \overline{b}$. Then it results:

$$\begin{array}{rrcll}
 & (a \wedge b)x & \leq & 0 \wedge (a \wedge b)ye & (\, e \in E(0)\,) \\
\Longrightarrow & (a \wedge b)x & = & (a \wedge b)(ye \wedge x)x' & (\,(ye \wedge x)x' = x\,) \\
\Longrightarrow & b & = & bx' & \\
\Longrightarrow & 0 & = & 0x' & \\
\Longrightarrow & x' & \in & E(0) & \\
\Longrightarrow & \overline{x} & \leq & \overline{y}\,. &
\end{array}$$

Hence under the above assumptions $\overline{x}$ is the right complement of $\overline{a}$ in $\overline{b}$. So by duality $\overline{\mathfrak{S}}$ is complementary.

Moreover we got $\overline{a} \cdot \overline{u} = \overline{a} \Longrightarrow \overline{u} = \overline{1}$, that is in general

$$\overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{y} \neq \overline{0} \Longrightarrow \overline{a}(\overline{x} \wedge \overline{y}) = \overline{a}(\overline{x} \wedge \overline{y}) \cdot \overline{x'} \Longrightarrow \overline{x'} = \overline{1} \Longrightarrow \overline{x} \leq \overline{y}\,.$$

and thereby

$$\overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{y} \neq \overline{0} \Longrightarrow \overline{x} = \overline{y}\,. \tag{8.1}$$

And this entails

$$\overline{a} : (\overline{b} * \overline{a}) = (\overline{b} : \overline{a}) * \overline{b} \tag{8.2}$$

since by the 0-cancellation property it results

$$(\overline{a} \wedge \overline{b}) \cdot (\overline{b} * \overline{a}) = \overline{a} \Longrightarrow \overline{a} : (\overline{b} * \overline{a}) = \overline{a} \wedge \overline{b}\,, \tag{8.3}$$

and thereby in general (8.2) . □

8. 1. 3 Lemma. *Let $\mathfrak{S}$ be archimedean, then $E(0)$ is invariant in $\mathfrak{S}_0$.*

PROOF. Let 0 belong to S and assume $0e = 0$. Then, according to the archimedean property of $\mathfrak{S}$, for all $x \leq 0$ we get both, $ex \leq 0$ and $xe \leq 0$. But in case of $xe = fx \leq 0$ this implies – for some suitable $y \in S$ –

$$0 = yxe = yfx = yfxe = yf^2x = yf^nx \implies f \in E(0)\,.$$

This completes the proof by duality. □

8. 1. 4 Lemma. *Let $\mathfrak{S}$ be archimedean. Then any $\overline{\mathfrak{S}}_0$ is integrally closed.*

PROOF. Suppose $\overline{a} \leq \overline{0}$ and $\overline{1} \neq \overline{t} \in \overline{S}_0$, in particular suppose that $t^n \leq 0$ $(\forall n \in \mathbf{N})$ is not valid. Then there is a highest exponent $m \in \mathbf{N}$, satisfying $t^m \leq 0$ in $\mathfrak{S}$, meaning that in $\mathfrak{S}_0$ there exists a highest $n \in \mathbf{N}$, satisfying $t^n \leq ae$ $(\exists\, e \in E(0))$, say with $t^n \cdot x = ae$. So $\overline{t} \not\leq \overline{x}$ since otherwise in $\mathfrak{S}$ we would get $t \leq xf$ $(f \in E(0))$ and thereby $t^{n+1} \leq aef$. Hence by $\overline{t}^n * \overline{a} \leq \overline{x}$ we get also $\overline{t} \not\leq \overline{t}^n * \overline{a}$. Thus the proof is complete by duality. □

8. 1. 5 Lemma. *An archimedean $\mathfrak{S}$ is commutative iff any $\overline{\mathfrak{S}}_0$ $(0 \in S)$ is commutative.*

PROOF. According to 2.4.2 we may start from some $a \leq b$. If then in $\mathfrak{S}$ ax equals b and in $\overline{\mathfrak{S}}_{ba}$ $\overline{a} \circ \overline{x}$ equals $\overline{x} \circ \overline{a}$, then $ax \leq ba \geq xa$ with $0 := ba$ leads to:

$$\begin{array}{rrcll} \overline{a} \circ \overline{x} = \overline{x} \circ \overline{a} & \Longrightarrow \quad ax & \equiv & xa & \qquad (E(0)) \\ & \Longrightarrow \quad axe & \overset{5.2.3}{=} & xaf & \quad (e, f \in E(0)) \\ & \Longrightarrow \quad aaxe & = & axaf & \\ & \Longrightarrow \quad abe & = & ba = 0 & \\ & \Longrightarrow \quad ab & \leq & ba\,. & \end{array}$$

Now replace ab by ba and operate "from the left. Then we obtain next $ba \leq ab$, which leads finally to $ab = ba$. □

Sofar it seems likely that commutativity depends on commutativity of completely integrally closed bricks. Moreover, according to theorem 7.2.15 any continuous d-semigroup is commutative. This means that we are through, once we can show that any completely integrally closed brick admits an embedding into some complete brick, since complete bricks are continuous, recall 2.8.6.

The proof under consideration will be given in two steps. In a first step we shall verify that the v-ideal structure $\mathfrak{V}$ of a completely integrally closed brick satisfies

(M) $$\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \circ \mathfrak{x} = \mathfrak{b} = \mathfrak{y} \circ \mathfrak{a} \quad (\exists : \mathfrak{x}, \mathfrak{y})$$

whence this ideal semigroup, say $\mathfrak{A}$, is complementary. Then, in a second step we shall show, that $\mathfrak{A}$ is even a brick. To this end we start with:

8. 1. 6 Proposition. *Let $\mathfrak{B}$ be an integrally closed brick, and let $\mathfrak{V}$ be its v-ideal structure. Then $\mathfrak{V}$ satisfies condition*

(M) $$\mathfrak{a} \supseteq b \Longrightarrow \mathfrak{a} \,\Big|_{\ell}\, \mathfrak{b} \;\&\; \mathfrak{a} \,\Big|_{r}\, \mathfrak{b}\,.$$

PROOF. Let $\mathfrak{a}$ contain $\mathfrak{b}$. We have to show $\mathfrak{a} \circ (\mathfrak{a} * \mathfrak{b}) = \mathfrak{b} = (\mathfrak{b} : \mathfrak{a}) \circ \mathfrak{a}$.

Let first $\mathfrak{b}$ be a principal ideal b. We may suppose that all elements $a \in A$ divide b, choose $A = \{a \wedge b \,|\, a \in A\}$.

We put $\mathfrak{a} * \mathsf{b} =: \mathfrak{c} =: C^v$. Then it holds $\mathfrak{a} \circ \mathfrak{c} \subseteq \mathsf{b}$. Suppose now, that there exists some $\mathfrak{a} \circ \mathfrak{c} \neq \mathsf{b}$, then there exists some t satisfying

$$t \leq AC \quad \& \quad t \not\leq b\,,$$

and thereby also $$b < \ t \vee b \ =: d\,.$$

But this would entail

$$AC \geq d \ \rightsquigarrow \ a * d \leq c \ (\forall : a \in A,\, c \in C)\,,$$

whence we would get:

$$1 \neq b * d \ \leq \ a * d \leq c \ (\forall a \in A)\,.$$

But from $b * a = 1$ and $a * b \leq a * d \leq c \ (\forall a \in A)$ it results:

$$\begin{aligned} a * b &= (a * d) : ((a * b) * (a * d)) \\ &= (a * d) : ((b * a) * (b * d)) \\ &= (a * d) : (b * d) \\ &\leq c : (b * d) \qquad (\forall\, c \in C). \end{aligned}$$

So, for any $a \in A$ we would get $a(c : (b * d)) \geq a(a * b) \geq b$ & $c \in C$ and thereby $c : (b * d) \in \mathfrak{c}$, whence $a(c : (b * d)) \geq d \ (\forall a \in A)$ would be satisfied.

So we could continue the procedure up to $b * d \leq c : (b * d)^n$, a contradiction w. r. t. the fact, that $\mathfrak{B}$ was presumed to be completely integrally closed. Hence it results $b * d = 1$ and thereby $d \leq AC \Longrightarrow d \leq b$, that is $\mathfrak{a} \circ \mathfrak{c} = \mathsf{b}$.

Let $\mathfrak{b}$ now be arbitrary. Then $\mathfrak{x} = X^v$ with $X := \bigcup(\mathfrak{a} * \mathsf{b}) \ (b \in \mathfrak{b})$ entails $\mathfrak{a} \circ \mathfrak{x} = \mathfrak{b}$, that is $\mathfrak{a} \,|_{\,\ell}\, \mathfrak{b}$. This completes the proof by $*, :$ $-$duality. $\square$

8. 1. 7 Proposition. *Let $\mathfrak{B}$ be a completely integrally closed brick. Then $\mathfrak{B}$ satisfies:*

(Q) $$\mathfrak{a} : (\mathfrak{b} * \mathfrak{a}) \ = \ (\mathfrak{b} : \mathfrak{a}) * \mathfrak{b}\,.$$

PROOF. It holds $\mathfrak{a} : (\mathfrak{b} * \mathfrak{a}) \supseteq \mathfrak{a}, \mathfrak{b}$ and thereby $(\mathfrak{a} : (\mathfrak{b} * \mathfrak{a})) * \mathfrak{a} \subseteq \mathfrak{b} * \mathfrak{a}$. Hence we obtain:

$$\begin{aligned}(\mathfrak{a} : (\mathfrak{b} * \mathfrak{a})) * \mathfrak{a} &= \mathfrak{b} * \mathfrak{a}\,,\\ (\mathfrak{a} + \mathfrak{b}) * \mathfrak{a} &= \mathfrak{b} * \mathfrak{a}\\ \mathfrak{a} : (\mathfrak{b} * \mathfrak{a}) &\supseteq \mathfrak{a} + \mathfrak{b}\,.\end{aligned}$$

Now we show

$$\begin{aligned}\mathfrak{x} \supseteq \mathfrak{y} \supseteq \mathfrak{z} \quad &\& \quad \mathfrak{x} * \mathfrak{z} = \mathfrak{y} * \mathfrak{z}\\ &\Longrightarrow\\ \mathfrak{x} \quad &= \quad \mathfrak{y}\,.\end{aligned}$$

First, by 8.1.6 the premise implies:

$$\begin{aligned}\mathfrak{x} * \mathfrak{o} &= (\mathfrak{x} * \mathfrak{z}) \circ (\mathfrak{z} * \mathfrak{o})\\ &= (\mathfrak{y} * \mathfrak{z}) \circ (\mathfrak{z} * \mathfrak{o})\\ &= (\mathfrak{y} * \mathfrak{o}) =: \mathfrak{w}\,.\end{aligned}$$

Suppose now $\mathfrak{x} \supset \mathfrak{y}$. Then there exists an $s \in B$ with $s \not\leq X$ but $s \leq Y$, and thereby also an element $t \in B$ with

$$1 \neq t \;\&\; \mathsf{t} \leq \mathfrak{x} * s \;\supseteq\; \mathfrak{x} * \mathfrak{y} \supseteq \mathfrak{x} * \mathfrak{o}\,.$$

This relation then would yield for the v-ideal $\mathfrak{x} * \mathfrak{o} = \mathfrak{w}$:

$$\begin{aligned}\mathfrak{y} \circ (\mathsf{t} * \mathfrak{w}) &= \mathfrak{x} \circ (\mathfrak{x} * \mathfrak{y}) \circ (\mathsf{t} * \mathfrak{w})\\ &\subseteq \mathfrak{x} \circ \mathsf{t} \circ (\mathsf{t} * \mathfrak{w})\\ &= \mathfrak{x} \circ \mathfrak{w}\\ &= \mathfrak{o}\,.\end{aligned}$$

Hence it would follow $\quad \mathsf{t} * \mathfrak{w} \subseteq \mathfrak{w}$ and $\mathfrak{w} \subseteq \mathsf{t} * \mathfrak{w}$,

that is

$$\mathsf{t} * \mathfrak{w} = \mathfrak{w} = \mathsf{t}^n * \mathfrak{w} \quad (\forall n \in \mathbf{N})$$

and thereby

$$\begin{aligned}1 \neq t \leq \mathfrak{w} \quad &= \quad \mathsf{t}^n * \mathfrak{w} \supseteq \mathsf{t}^{\mathfrak{n}} * \mathfrak{o}\\ &\rightsquigarrow\\ 1 \neq t \quad &\leq \quad t^n * 0 \quad (\forall n \in \mathbf{N})\,,\end{aligned}$$

a contradiction. Thus we are led to

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{a} : (\mathfrak{b} * \mathfrak{a})\,.$$

This completes the proof by duality. □

Summarizing we get:

8. 1. 8 Theorem. *Any archimedean d-semigroup $\mathfrak{S}$ is commutative.*

PROOF. Apply 2.8.6, 7.2.15, 8.1.2 through 8.1.6 and 4.3.3. □

8.2 Appendix

Below 8.1.6 it is shown that the v-ideals of any brick satisfy the condition $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \,|\, \mathfrak{b}$. In fact this holds already on weaker assumptions.

8. 2. 1 Proposition. *Let $\mathfrak{S}$ be an archimedean complementary semigroup. Then the v-ideals of $\mathfrak{S}$ satisfy:*

$$\text{(M)} \qquad \mathfrak{a} \supseteq b \implies \mathfrak{a} \,|_{\ell}\, \mathfrak{b} \;\&\; \mathfrak{a} \,|_{r}\, \mathfrak{b} \,.$$

PROOF. First of all we exhibit that in a complementary semigroup according to $s \,|\, At \Longrightarrow s : t \,|\, A \Longrightarrow (s : t)t \,|\, At$ the v-ideal , generated by A , is equal to the set of all common multiples of all common divisors of A .

Next we show that in complementary semigroups any finitely generated v-ideal satisfies condition (M).

To this end assume $\mathfrak{a} = (a_i)^v \ (1 \leq i \leq n)$ and $b \in \mathfrak{a}$. Then $\mathfrak{a} * \mathbf{b}$ is equal to $(\bigvee(a_i * b) \ (1 \leq i \leq n))^v$, and we get for $c := \bigvee \ (a_i * b) \ (1 \leq i \leq n)$

$$d \,|\, Ac \Longrightarrow c \,|\, b \vee d \ \ =: \ g \,|\, Ac \Longrightarrow g : c \,|\, A \,.$$

This means $g : c \leq b,$, say $(g : c)y = b$. and thereby $Ay \geq b$, that is $y \geq c$. Hence we get further:

$$g = (g : c)c \ \leq \ (g : c)y = b \,,$$

that is $b = g = b \vee d \rightsquigarrow d \,|\, b$.

Next we show that together with $\mathfrak{S}$ also the d-monoid of finitely generated v-ideals is archimedean.

To this end we start like above from $\mathfrak{a}$ and b. If here for all $n \in \mathbf{N}$ it holds $\mathfrak{a}^n \supseteq \mathsf{b}$, then it follows:

$$\begin{array}{rrcl} t \leq \mathfrak{a}\mathsf{b} \implies & t & \leq & a_i b \ \ (1 \leq i \leq n) \\ \implies & t : b & \leq & a_i \\ \implies & (t : b)^n & \leq & b \ \ (\forall n \in \mathbf{N}) \\ \implies & t & = & (t : b)((t : b) * t) \\ & & \leq & (t : b)b = b \ . \end{array}$$

Thus, in particular any archimedean complementary semigroup is commutative.

Now we are in the position to prove the principal assertion:

Here we start from $\mathfrak{a}\mathsf{b} \subseteq \mathsf{b}$ and $\mathfrak{x} := \mathfrak{a} * \mathsf{b}$. Then in case of $c \leq AX$ it holds $d = b \vee c \leq AX$, whence it results $b \in \mathfrak{a} \cap \mathsf{b} \subseteq \mathfrak{x}$ for all a, x with $a \in \mathfrak{a}$, $x \in \mathfrak{x}$

$$b * d \leq x \quad \& \quad b * d \leq a \, .$$

From this, however, we get for any a, x under consideration:

$$\begin{array}{rl} & (b * d)((b * d) * a)(b * d)((b * d) * x) \\ \geq & (b * d)((b * d) * b)(b * d) \\ \implies & ((b * d) * a)(b * d)((b * d) * x) \\ \geq & ((b * d) * b)(b * d) \\ \implies & a((b * d) * x) \\ \geq & b \ . \end{array}$$

Consequently, together with any x also $(b * d)x$ belongs to $\mathfrak{x}$. This leads to $(b * d)\mathfrak{x} = \mathfrak{x}$ and thereby in general to $(b * d)^n \mathfrak{x} = \mathfrak{x}$. But $\mathfrak{S}$ is archimedean, so it results $b = (b * d)b = b \vee d$, that is $c \leq b$.

Thus we are through, since the assumption of $\mathfrak{b}$ being some principal ideal b is easily generalized, as seen above. □

8. 2. 2 Corollary. *Any archimedean complementary semigroup admits an $|$-respecting embedding into some complete complementary semigroup, such that any α of the extension is the GCD of some subset of S.*

That not any d-semigroup satisfying the archimedean property or even the archimedean property for v-ideals admits a complete extension, will turn out in the later chapter on real d-semigroups.

8.3 The Identity Extension

Let in this section $\mathfrak{S}$ be always a d-semigroup without identity and $\mathfrak{S}^1$ its identity extension with carrier Σ. We denote the elements of $\mathfrak{S}^1$ by lower case Greek letters except for situations in which we wish to emphasize that the elements under consideration belong to S. Since $\mathfrak{S}$ is assumed not to contain an identity, there can't either exist some cancellative element. On the other hand, embedding $\mathfrak{S}$ into $\mathfrak{S}^1$ means adjoining elements of type 1, type $1 \wedge a$, type $(1 \wedge b)^{-1}$, or type $(1 \wedge a)(1 \wedge b)^{-1}$ (with $a, b \in S$). Hence S contains exactly the non cancellable elements, whereas $\Sigma \backslash S$ contains exactly the cancellable elements of Σ, compare Chapter 3.

We start with:

8. 3. 1 Lemma. $\tau \leq x \in S^+ \ \ (\forall\, x \in S^+)$ *implies* $\tau \leq 1$.

PROOF. Because $x \leq a \in S^+ \Longrightarrow 1 \vee x \leq a$ we may restrict our attention to positive elements τ. We consider the cases:

(*i*) τ is of type $(1 \wedge b)^{-1}$

(*ii*) τ is of type $(1 \wedge a)(1 \wedge b)^{-1}$.

Ad (*i*). Assume $\tau = (1 \wedge b)^{-1}$ and let e be a positive unit of b. Then by assumption τ satisfies:

$$\begin{aligned} \tau = (1 \wedge b)^{-1} \leq e &\Longrightarrow 1 \leq e \wedge b \\ &\Longrightarrow 1 \leq b \\ &\Longrightarrow \tau = 1\,. \end{aligned}$$

Ad (*ii*). If, however, it holds $\tau = (1 \wedge a)(1 \wedge b)^{-1}$, then there exists a positive $e \in S^+$ with $e(a \wedge b) = a \wedge b = (a \wedge b)e$ and $b = (e \vee b)(e \wedge b)$. Furthermore there exists a positive unit f with $\tau \leq f$, whence by $\tau \geq 1$ we get $e\tau = e$ and thereby $e \wedge a = e \wedge b$. This entails:

$$\begin{aligned} 1 \vee b &= e \vee b \\ &= e(e \vee b)(1 \wedge a)(1 \wedge a)^{-1} \\ &= (e \vee b)e(1 \wedge a)(1 \wedge a)^{-1} \\ &= (e \vee b)(e \wedge a)(1 \wedge a)^{-1} \\ &= (e \vee b)(e \wedge b)(1 \wedge a)^{-1} \\ &= b(1 \wedge a)^{-1}\ , \end{aligned}$$

leading to:

$$\begin{aligned}
\tau^{-1} &= (1 \wedge b)(1 \wedge a)^{-1} \\
&= (1 \wedge a)^{-1} \wedge b(1 \wedge a)^{-1} \\
&= (1 \wedge a)^{-1} \wedge (1 \vee b) \\
&= ((1 \wedge a)^{-1} \wedge 1) \vee ((1 \wedge a)^{-1} \wedge b) \\
&= 1 \vee ((1 \wedge a)^{-1} \wedge b) \\
&\geq 1 \\
&\rightsquigarrow \\
\tau &= 1\,.
\end{aligned}$$

This completes the proof □

As a fundamental consequence we get:

8. 3. 2 Proposition. *If $\mathfrak{S}$ is archimedean, then $\mathfrak{S}^1$ is archimedean, too.*

PROOF. Suppose $1 \leq \tau^n \leq a \in S$ $(\forall\, n \in \mathbf{N})$ and let e be a positive unit of a in $\mathfrak{S}$. Then it follows

$$\begin{aligned}
1 \leq \tau^n \leq a &\Longrightarrow 1 \leq (\tau e)^n \leq a e^n = a \\
&\Longrightarrow \tau e a = a \\
&\Longrightarrow \tau a = a\ .
\end{aligned}$$

If, however, it holds $1 \leq \tau^n \leq \alpha \in \Sigma \backslash S$ $(\forall n \in \mathbf{N})$, then α is cancellable, and according to the first part of the proof each $x \in S^+$ satisfies:

$$\begin{aligned}
1 \leq \tau^n \leq \alpha x &\Longrightarrow \tau \alpha x = \alpha x \\
&\Longrightarrow \tau x = x\ .
\end{aligned}$$

Thus we get $\tau = 1$ meaning $\tau\alpha = \alpha$. □

We now turn to the identity extension $\mathfrak{S}^1$ in case that $\mathfrak{S}$ is a complete d-semigroup: By $\{B\}$ we will mean the v-ideal, generated by B in $\mathfrak{S}^1$. Observe, that the v-ideals, generated by B in $\mathfrak{S}$ and $\mathfrak{S}^1$, respectively, may be different. As a first result we get:

8. 3. 3 Lemma. *The v-ideal, generated by S^+ in ${\mathfrak{S}^1}^+$, is equal to $\{1\}^v$.*

PROOF. We consider the cases $\tau \in S^+$ and $\tau \in \tau \in {\mathfrak{S}^1}^+ \backslash S^+$

If $\tau = t \in S^+$ and $\sigma | a \cdot t$ $(\forall a \in S^+)$, then from $et = t$ $(\exists\, e)$ it results $\sigma \,|\, et = 1 \cdot t = 1 \cdot \tau$.

And if $\tau \in \mathfrak{S}^{1^+}\backslash S^+$ with $\sigma \,|\, a\cdot\tau$ $(\forall a \in S^+)$ according to 8.3.1 we get $\sigma\tau^{-1} \leq 1$ and thereby $\sigma \,|\, \tau = 1 \cdot \tau$.

Hence 1 is element of the v-ideal generated by S^+ in $\mathfrak{S}^1$ and consequently $\{S^+\} = \{1\}$. $\square$

Furthermore we get:

8. 3. 4 Proposition. *Let $\mathfrak{S}$ be a complete d-semigroup and let $\mathfrak{A}$ and $\mathfrak{B}$ be two v-ideals of $\mathfrak{S}^{1^+}$ with $\mathfrak{A} \supseteq \mathfrak{B}$. Then it even holds $\mathfrak{A} \,|\, \mathfrak{B}$.*

PROOF. We may restrict our attention to the case of $\mathfrak{B} = \{\beta\}$, and have to discuss the cases $\beta \in S$ and $\beta \in \Sigma\backslash S$.

To begin with, we suppose $\beta \in S^+$, that is $\beta = b \in S$, and assume that e is a positive unit of b. Then $\mathfrak{A} = \{\alpha_i\}$ with $\alpha_i \leq b$ implies $\alpha_i e \in S^+$ and $e \leq \alpha_i e$ for all $i \in I$, whence in $\mathfrak{S}^+$ there exists $\inf\{\alpha_i e\}$, say a.

Next because $a \leq be = b$ it results $a \,|\, b$, say $ax = b$ with $x \in S^+$. But this leads to

$$\{\alpha_i\}\{ex\} \;=\; \{b\}\,.$$

OBSERVE: $\sigma \,|\, \alpha_i ex \cdot \tau$ with $\tau = t \in S^+$ implies

$$\begin{aligned}
\sigma \,|\, \alpha_i ex\cdot t \iff \sigma f \;&|\; \alpha_i ex \cdot t \qquad\qquad (af = a, i \in I)\\
\iff \sigma f \;&|\; (\textstyle\bigwedge(\alpha_i ex))\cdot t\\
\iff \sigma \;&|\; (\textstyle\bigwedge(\alpha_i e))\cdot xt\\
\iff \sigma \;&|\; axt\\
\iff \sigma \;&|\; bt\,.
\end{aligned}$$

And $\tau \in \Sigma^+\backslash S^+$ in case of $(\sigma\wedge\tau)\sigma' = \sigma$ and $(\sigma\wedge\tau)\tau' = \tau$ implies:

$$\begin{aligned}
\sigma \,|\, \alpha_i ex\cdot t \iff \sigma' \;&|\; \alpha_i ex \cdot \tau' \qquad\qquad (af = a, i \in I)\\
\iff \sigma' f \;&|\; \alpha_i ex\\
\iff \sigma' f \;&|\; (\textstyle\bigwedge(\alpha_i ex))\\
\iff \sigma' \;&|\; (\textstyle\bigwedge(\alpha_i e))x\cdot\tau'\\
\iff \sigma \;&|\; ax\cdot\tau\\
\iff \sigma \;&|\; b\cdot\tau\,.
\end{aligned}$$

Thus, in case of $\beta \in S$ it is shown $\mathfrak{A} \,|\, \{\beta\}$.

Suppose now $\beta \in \Sigma^+ \backslash S^+$. Then for each $x \in S^+$ there exists some $\mathfrak{A}_x$ with $\mathfrak{A} \circ \mathfrak{A}_x = \{\beta x\}$. This leads to $\{\mathfrak{A}\mathfrak{A}_x\} = \{\beta x\}$ $(x \in S^+)$, and hence – by lemma 8.3.3 – to $\{\mathfrak{A}\mathfrak{A}_x\} = \{\beta\}\{S^+\} = \{\beta\}\{1\} = \{\beta\}$. □

As a consequence of the preceding theorem we get that $\mathfrak{S}^+$ admits a complete extension with identity 1. But it remained open, wether the existing infima and suprema are carried over from $\mathfrak{S}$ to the extension. Here we get first:

8. 3. 5 Lemma. *Let a be* $\inf(a_i)$ $(i \in I)$ *in* $\mathfrak{S}^+$*. Then* $\{a\}$ *is infimum of the principal ideals* $\{a_i\}$ *belonging to the v-ideal structure* $\mathfrak{V}^+$ *of* $\mathfrak{S}^{1^+}$.

Let a be $\sup(a_i)$ $(i \in I)$ *in* S^+*. Then* $\{a\}$ *is supreme the of the principal ideals* $\{a_i\}$ *in the principal ideal structure* $\mathfrak{V}^+$ *of* $\mathfrak{S}^{1^+}$.

PROOF. Assume $A \subseteq S^+$, $a = \bigwedge(a_i)$ $(a_i \in A)$ in $\mathfrak{S}^+$ and $ae = a$ with positive element e. If then $\mathfrak{X} \supseteq \{a_i\}$ $(a_i \in A)$ is satisfied, in case of $\mathfrak{X} \in \mathfrak{V}^+$, we get:

$$\sigma \,|\, \mathfrak{X}\tau \Longrightarrow \sigma e \,|\, a_i e\tau \Longrightarrow \sigma e \,|\, ae\tau \Longrightarrow \sigma \,|\, a\tau \rightsquigarrow a \in \mathfrak{X} \rightsquigarrow \mathfrak{X} \,|\, \{a\}\,.$$

Let now $a = \sup(a_i)$ $(a_i \in A \subseteq S^+)$ and $\{a_i\} \supseteq \mathfrak{X}$ be satisfied. Then, by $x \geq a_i \in S^+ \implies x \in S^+$ it follows $a \leq x \in \mathfrak{X}$ and thereby $\{a\} \,|\, \mathfrak{X}$. □

Finally we have to mention:

8. 3. 6 Proposition. *Together with* $\mathfrak{S}$ *also* $\mathfrak{V}^+$ *is a continuous d-semigroup.*

PROOF. We start from $x \in S^+$ and $xe = x$ $(e \in S^+)$. Then it follows

$$\mathfrak{A} \circ \bigcap \mathfrak{B}_{\mathsf{i}} \supseteq \mathsf{x} \circ (\mathfrak{A} \circ \bigcap \mathfrak{B}_i) \circ \mathsf{e} = \bigcap \mathsf{x} \circ \mathfrak{A} \circ \mathfrak{B}_i \supseteq \mathsf{x} \circ \bigcap \mathfrak{A} \circ \mathfrak{B}_i \quad (i \in I)\,.$$

Consequently, according to lemma 8.3.3, we get $\bigcap$-continuity, and $\sum$-continuity is verified in a similar manner. □

8. 3. 7 Lemma. *If ρ is cancellable in* $\mathfrak{S}^1$*, then* $\{\rho\}$ *is cancellable in* $\mathfrak{V}^+$*, too.*

PROOF. By assumption $\{\rho\}\mathfrak{A} = \{\rho\}\mathfrak{B}$ implies:

$$\sigma \,|\, \mathfrak{A}\tau \iff \rho\sigma \,|\, \rho\mathfrak{A}\tau \iff \rho\sigma \,|\, \rho\mathfrak{B}\tau \iff \sigma \,|\, \mathfrak{B}\tau \rightsquigarrow \mathfrak{A} = \mathfrak{B}\,. \qquad \square$$

Now we are in the position to show:

8. 3. 8 Proposition. *Let $\mathfrak{S}$ be a complete d-semigroup. Then $\mathfrak{S}$ admits a complete extension with identity.*

Let $\mathfrak{S}$ be inf - and sup - continuous then $\mathfrak{V}$ is inf- and sup- continuous, as well.

PROOF. This follows from the preceding results by 7.1.5. $\square$

Chapter 9

Linear d-monoids

In this chapter we are interested in *archimedean linear d-semigroups*, that is totally ordered archimedean d-semigroups. Since the negative cone is completely determined by the *positive cone,* we may restrict ourselves to studying *positive archimedean d-semigroups.* To this end we will start with an introduction to *complete chains.*

Linear ordered semigroups play an important role in *measure theory* and its applications, but our focus excludes applications and is that of d-smigroups "living" in the real unit interval $[0,1]$. The reader, interested in the large field of linear ordered semigroups and their applications is referred to the contribution [64] of Hofmann & Mislove. There he will find a most readable introduction and survey, as well, including hints to the elements of Euclid, [52], and the first paper on semigroups ever by Nils Henrik Abel, [1], and Bourbaki's contribution to the field in [37].

Moreover he will find a most valuable list of references, in particular concerning topological aspects as *one parameter semigroups.*

9.1 Dense Chains

We rely on Karl Doerge, who relied on Felix Hausdorff, [60], [61]. Nowadays one has to study Egbert Harzheim, [59], a most readable and valuable contribution to the theory of ordered sets.[1)]

[1)] But, of cause, each of them relies on Georg Cantor's fundamental ideas and work.

9. 1. 1 Definition. A *partially ordered set* $(P, \leq) =: \mathfrak{P}$ is called *totally ordered*, or synonymously *linearly ordered*, or synonymously a *chain* iff for all $a, b, c \in P$ in P it holds:

$$(i) \quad a \not< a\,,$$
$$(ii) \quad a \leq b \;\&\; b \leq c \Longrightarrow a \leq c\,,$$
$$(iii) \quad a \neq b \Longrightarrow a < b \text{ aut } b < a\,.$$

Hence forth we will write $A \leq s$ if $a \leq s \;\; (\forall a \in A)$.

9. 1. 2 Definition. Let $\mathfrak{C}$ be a chain. We say that z it *lies between* a and b iff $a < z < b$. Let moreover $B \subseteq C$. We say that B lies *dense in* $\mathfrak{C}$ if between any two different elements of C there lies at least one element of B. In particular we call $\mathfrak{C}$ *dense (in itself), if C is dense in $\mathfrak{C}$.*

For instance $\mathbf{R}$ and $\mathbf{Q}$ are dense in $\mathbf{R}$.

9. 1. 3 Definition. Let $\mathfrak{C}$ be a chain with $B \subseteq C$. Then m *is called maximum* of A if $m \in A$ and $A \leq m$. Dually the notion *minimum* is defined.

The notions *upper* and *lower bound* are defined as usual, that is u is an upper bound of A if $A \leq u$ and l is a lower bound of A if $l \leq A$.

If S is the lowest upper bound, i.e. the minimum of all upper bounds, of A, then s is called the supremum of A, denoted by $\sup(A)$, also by $\Omega(A)$.

If L is the greatest lower bound, i.e. the maximum of all lower bounds, of A, then L is called the infimum of A, denoted by $\inf(A)$, also by $\omega(A)$

9. 1. 4 Definition. Let $\mathfrak{C}$ be as chain. We say that $\mathfrak{C}$ is *continuous* if $\mathfrak{C}$ is dense and any upper bounded $A \subseteq C$ has a supremum.

Obviously, in a continuous ordered set any lower bounded subset B has an infimum.

9. 1. 5 Definition. Two chains $\mathfrak{A} := (A, <_A)$ and $\mathfrak{B} : = (B, <_B)$ are called *(order-)similar*, if they are isomorphic w.r.t. their order.

9. 1. 6 Definition. Let $\mathfrak{C}$ be a chain. By an *open interval* (a, b) we mean the set $\{\, x \,|\, a < x < b \,\}$, and by a *closed interval* $[\, a, b\,]$ we mean the set $\{\, x \,|\, a \leq x \leq b \,\}$.

Furthermore by the *left open, right closed* interval $(a, b\,]$ we mean the set $\{\, x \,|\, a < x \leq b \,\}$, etc. Finally, a chain is called *right-* respectively *left-bordered,* if it has a *left-, right endpoint,* respectively, and, of course, if it has both, a left and a right endpoint, it is called *bordered.*

Recall, the chain of rationals is countable (folk). Hence the rational intervals $[\,0,1\,]$, $(0,1\,]$, $[\,0,1)$, $(0,1)$ are countable, too.

In fact it holds more

9. 1. 7 Proposition. *Any countable, dense chain $\mathfrak{C}$ is similar to one of the above presented intervals.*

PROOF. Obviously we are through, once it is shown that any *unbordered* countable dense chain is similar to the ordered set of rationals $\mathfrak{Q} := (Q, \leq)$.

So let's start with a countable unbordered chain $\mathfrak{C}$ and $\mathfrak{Q}$, both considered as sequences, say:

$$C = \{\, a_1\,,\, a_2\,,\, a_3\,, \ldots,\, a_n,\, \ldots \} \tag{9.1}$$

$$Q = \{\, b_1\,,\; b_2\,,\; b_3\,, \ldots\,, b_n,\, \ldots \}\,. \tag{9.2}$$

We map:

a_1 to b_1, b_2 to the first element of $C - \{a_1\}$ in a similar position w.r.t. a_1 as b_2 w.r.t. b_1, next the first element of $C - \{a_1, a_2\}$ to the first element of $Q - \{b_1, b_2\}$ in a similar position w.r.t. $\{b_1, b_2\}$ etc.

Since $\mathfrak{C}$ is assumed to be dense and unbordered, we finally arrive at a bijection, since any element of Q and also any element of C is taken into account. □

9. 1. 8 Definition. Let $\mathfrak{C}$ be a chain. A pair $(A|B)$ is called a cut of $\mathfrak{C}$ if

- (i) $A \cup B = K$
- (ii) $A \cap B = \emptyset$
- (iii) $a < b$ for all $a \in A, b \in B$

More precisely a cut is called a *jump* if A has a last element and B has a first element, and it is called a *gap*, if neither A has a last element nor B has a first element. In addition we call $(C\,|\,\emptyset)$ a *right cut* and $(\emptyset\,|\,C)$ a *left cut.*

For instance π generates a jump in $\mathfrak{Z}$ and a gap in $\mathfrak{Q}$.

Moreover it is clear that any *irrational number* generates a uniquely determined gap in $\mathfrak{Q}$, denoted as *cut number*, and, *vice versa*, any rational number defines gap in the set of all irrational numbers.

And, by the way, we see nearly immediately that any countable totally ordered set admits an isomorph bijection into $\mathfrak{Q}$ – fill the jumps by pairwise disjoint countable dense totally ordered sets.

9. 1. 9 Proposition. *Let $\mathfrak{C}$ be a continuous unbordered chain with a countable subset B, dense in $\mathfrak{C}$. Then $\mathfrak{C}$ is similar to $\mathfrak{R} := (\mathbf{R}, \leq)$.*

PROOF. Generate an *order isomorphism* between $\mathfrak{Q}$ and $\mathfrak{B}$. Then any $\alpha \notin B$ defines a cut in $(B, \leq)$ and thereby a uniquely defined cut number of $\mathfrak{Q}$, and moreover this mapping is bijective □

9. 1. 10 Corollary. *Let $\mathfrak{C}$ be a continuous unbordered chain with a countable subset B, dense in $\mathfrak{C}$. Then $\mathfrak{C}$ is similar to $\mathfrak{R} := (\mathbf{R}, \leq)$.*

9.2 Continuous Chains

The most classical example of a continuous chain is the *real unit interval* $\mathbf{E} := [0, 1]$.

9. 2. 1 Definition. Let $\mathfrak{C}$ be a chain and (a_n) a *sequence of elements* of C. As usual in analysis we say that (a_n) converges to a, in symbols

$$(a_n) \longrightarrow a \quad \text{ or alternately } \quad lim\ a_n = a\,,$$

if (a_n) *ends* in any *open interval* $I \ni a$, that is if a whole *end* $a_N, a_{N+1}, a_{N+2}...$ belongs to I.

9. 2. 2 Definition. Let $\mathfrak{C}$ be a *chain.* $a \in C$ is a *cluster point* of $B \subseteq C$ if any open interval $I \ni a$ of a contains one element of B, different from a – and thereby infinitely many elements of B.

9. 2. 3 Definition. Let $\mathfrak{C}_1, \mathfrak{C}_2$ be chains, not necessarily different and f a function $C_1 \longmapsto C_2$. Then f is called *continuous* at $x_o \in C_1$ if

$$x_n \longrightarrow x_0 \Longrightarrow f(x_n) \longrightarrow f(x_0)\,,$$

or equivalently if for any open interval $C_2 \supseteq U_2 \ni f(x_0)$ there exists an open interval $C_1 \supseteq U_1 \ni x_0$ with $f(U_1) \subseteq U_2$.

Continuous chains have strong properties, w.r.t. **R** well known to any graduate student. Never the less we include here some central and fundamental results that apply to *interval d-semigroups*, which will be considered in the next section.

9. 2. 4 Theorem. *Let $\mathfrak{C}$ be a dense chain*[2]*. Then the following are pairwise equivalent:*

(AS) The Axiom of Supremum: *Any not empty upper bounded subset of C has a supremum $(C, \leq)$, say is upper limited.*

(HB) The Theorem of Heine Borel: *Any family (a_i, b_i) $(i \in I)$ of open intervals that covers the closed interval $[\,a, b\,]$ contains a finite subfamily of open intervals $(a_{i_1}, b_{i_1}), \ldots, (a_{i_n}, b_{i_n})$, covering $[\,a, b\,]$.*

(CD) The Theorem of Cantor: *Any intersection empty family of closed intervals $[\,a_i, b_i\,]$ $(a_i \neq b_i\,,\; i \in I)$ contains at least two disjoint intervals.*

(SM) The Maximum Theorem: *Any continuous mapping of $[\,a, b\,]$ has a maximum.*

(ZS) The Intermediate Value Theorem: *Any continuous mapping of $[\,a, b\,]$ takes each value between $f(a)$ and $f(a)$.*

(MT) The Mapping Theorem: *Continuous functions map closed intervals an closed intervals.*

(BW) The Theorem of Bolzano-Weierstraß: *Any bounded infinite subset of C contains at least one cluster point.*

PROOF.

(AS) $\Longleftrightarrow$ **(HB)**:

[2] Observe, we do not assume that $\mathfrak{C}$ has a countable subset, dense in $\mathfrak{C}$.

($\Longrightarrow$) We define

$$X := \{\, x \,|\, [\, a, x\,] \text{ is (already) covered by a finite subfamily.}$$

Then there exists at least one x properly between a and b, belonging to X, choose some $(a_k, b_k) \ni a$, and moreover it holds $\Omega(X) := \Omega \leq b$. Choose now some interval $(a_\ell, b_\ell) \ni \Omega$. Then in this interval (a_ℓ, b_ℓ) on the left of Ω there lies at least one element x of X. Consequently Ω must be equal to b, since otherwise also strictly right of Ω would lie a further element of X. This proves ($\Longrightarrow$).

($\Longleftarrow$) $\mathfrak{C}$ is free of gaps $A|B$, since otherwise we could choose elements $a' < a \in A$ and $b' > b \in B$, such that the set of all (a', a_i) with $a_i \in A \cap [\, a, b\,]$ and the set of all (b_i, b') with $b_i \in [\, a, b\,] \cap B$ would provide an open covering of $[\, a, b\,]$ which would not contain a finite subcover of $[\, a, b\,]$, a contradiction.

Hence any upper bounded subset of $\mathfrak{C}$ has a supremum.

(AS) $\Longleftrightarrow$ **(CD)**:

($\Longrightarrow$) If there wouldn't exist a pair

$$[\, a_i, b_i\,] \cap [\, a_j, b_j\,] \;=\; \emptyset\,,$$

any a_i would lie left of any b_j. But this would mean

$$sup\{a_i\} \;\leq\; \inf\{b_j\} \;\; (i, j \in I)$$

and thereby a contradiction, since $sup\{a_i\}$ would belong to the intersection of all considered intervals.

($\Longleftarrow$) Assume now that $B \subseteq C$ is upper bounded, however without a supremum. Then the set of all intervals $[\, a_i, b_i\,]$ with $a_i \in B$, $B < b_i$ forms a family $\mathfrak{F}$ of intervals with an empty section (left to the reader). Hence there must exist two disjoint intervals in $\mathfrak{F}$, a contradiction.

(AS) $\Longleftrightarrow$ **(SM)**:

($\Longrightarrow$) Let $f(a)$ or $f(b)$ be the maximum of $W := f[\, a, b\,]$. Then there is nothing to show.

Otherwise, consider the set X of all $x \in [\, a, b\,]$ with the property that $[\, a, x\,]$ is bounded. This set is not empty since a belongs to X. Moreover it is upper bounded, for instance by b, with a supremum, say $\Omega \leq b$. Since f is continuous, it results immediately $\Omega = b$ and thereby that f is upper bounded on $[a, b]$, whence $W := f([a, b])$ has a supremum, say G.

We consider the set U of all $u \in [a, b]$ with $\mathrm{Sup} f([a, u]) < \mathrm{Sup} f([a, b])$ and the upper limit S of U. We obtain $S < b$, since otherwise we could choose an open interval $I \subseteq [a, b] \ni S$, whose function values would lie properly below G, a contradiction

Furthermore it must hold $f(S) = G$, since $f(S) > G$ would lead to contradiction.

Consequently $f(S)$ is maximum of W.

($\Longleftarrow$) Assume that $A|B$ is a gap. Then we are in the position to define a continuous mapping f on C by

$$f(x) := \begin{cases} x & \text{if } x \in A \\ a & \text{otherwise} \end{cases}$$

with a fix $a \in A$. This function is continuous but does not take a maximum value. Thus ($\Longleftarrow$) is proven.

(**AS**) $\Longleftrightarrow$ (**IV**):

($\Longrightarrow$) Suppose $f(a) < z < f(b)$. We define $X := \{ x \mid f([a, x]) < z \}$ and consider the supremum $\Omega(X) =: \Omega$. Then $f(\Omega) = z$, since by construction and continuity $f(\Omega) < z$ and $f(\Omega) > z$, as well, lead to a contradiction.

($\Longleftarrow$ Let $A|B$ a gap. Then we are in the position for define a continuous mapping f by

$$f(x) := \begin{cases} a & \text{if } x \in A \\ b & \text{otherwise} \end{cases}$$

with constant $a \in A$ and $b \in B$, that obviously **(IV)** dos not fulfil.

(**AS**) $\Longleftrightarrow$ (**MT**).

This is an immediate consequence of the two preceding equivalences, observe that the existence of a minimum results by duality.

(**AS**) $\Longleftrightarrow$ (**BW**).

($\Longrightarrow$) Let B be an infinite bounded subset of $[a, b]$. Then infinitely many elements of B are greater than a. Hence the set X of all elements x, satisfying

Infinitely many elements of B are greater than x

has a supremum.

Define $\Omega := Sup\,(X)$. Then Ω is a cluster point of B. For choose some neighbourhood (u, v) of Ω. Then right of v there are only finitely many, but right of u there are infinitely many elements of B. So infinitely many elements B belong to (u, v).

($\Longleftarrow$) Let $A|B$ be a gap of $\mathfrak{C}$. Then to any $a \in A$ there exists some a', a'' in A with $a < a' < a''$. Hence for any a we can choose an open interval $U(a) \ni a$ such that right of $U(a)$ there exists at least one further $u \in A$.

Consequently, by the counting indices we are in the position to choose successively a sequence $a_{i_1} < a_{i_2} < \ldots < a_{i_n} <$ ... of elements, such that any $a \in A$ would lie below some a_{i_n}. But this leads to a bounded subset without cluster point, a contradiction. $\square$

Let henceforth $\mathfrak{C}$ b a chain with a countable subset, dense in $\mathfrak{C}$. Then of course we may expect a bit more. We mention merely:

9. 2. 5 Proposition. *Let $\mathfrak{C}$ contain a countable subset B, dense in $\mathfrak{C}$. Then apart from 9.2.4 the following property is equivalent with LU:*

(MO) The Monotony Principle: *Any upper bounded strictly increasing (a_n) is convergent.*

PROOF.

(**AS**) $\Longleftrightarrow$ (**MO**).

($\Longrightarrow$) Obviously $\sup\{a_n\} = \lim a_n \ \ (n \in \mathbf{N})$.

($\Longleftarrow$) Let $A, B \subseteq C$ and suppose that B is countable and dense in $\mathfrak{C}$. Then we can choose successively elements $b_1, \ldots, b_n, \ldots \in B$ such that b_n is the first element of B below all upper bounds of A and greater than all b_i $(1 \leq i \leq n-1)$. Then (b_n) is an increasing sequence, satisfying $\lim(b_n) = \sup(A)$, whence A is upper limited. $\square$

9.3 Hölder and Clifford

This section is based on papers of Hölder [65], Clifford [47], and Fuchs [57], as presented in Fuchs [56], and written nearly independently w.r.t.

the previous chapters. Thus the reader will be in the position to study the case of real d-semigroups without particular knowledge. The expert however may turn to the author's alternative development at the end of this section.

In the class of all d-semigroups those models are of most natural origin, which arise – what way ever – from the additive group of the reals. These are – on the one hand – the substructures of $(\mathbf{R}, +, \min)$ and – on the other hand – certain homomorphic images of such substructures, the strong properties being *linearity* together with a very strict archimedean property.

9. 3. 1 Definition. We call a d-semigroup *strictly archimedean* if it satisfies:

$$a \neq 1 \neq b \Longrightarrow \exists\, n \in \mathbf{N} : \; a^n \geq b\,.$$

Strictly archimedean d-semigroups *are always* positive, since $ae = a = ea$ and $ab \not\geq a$ together imply $a(e \wedge b) < a$. Hence strictly archimedean d-semigroups in particular are archimedean, since $a^n \leq b$ $(\forall n \in \mathbf{N})$ implies $a^m = b$ $(\exists n \in \mathbf{N})$ and thereby finally $ab = a^m \cdot a = a^m = b = ba\,.$

9. 3. 2 Lemma. *Any strictly archimedean d-semigroup $\mathfrak{S}$ is linearly (totally, fully) ordered.*

PROOF. Let $R(a,b,a',b')$ with $a',b' \geq 1$ and w. l. o. g. $a'^{\,m} \geq b'$ be satisfied. Then it follows

$$b = (a \wedge b)(b' \wedge a'^{\,m}) \leq (a \wedge b)(a' \wedge b')^m = a \wedge b\,.$$

and thereby, of course, $b' = 1$. □

Next along the lines of Clifford [42] we prove:

9. 3. 3 Lemma. *Let $\mathfrak{S}$ be a non cancellative strictly archimedean d-monoid. Then it results:*

(1) *$\mathfrak{S}$ contains a maximal element u,*

(2) *For each $a \in S$ $(a \neq e)$ there exists a natural k with $a^k = u$,*

(3) *$ab = ac \neq u$ (or $ba = ca \neq u$) implies $b = c$.*

Hence, in particular $\mathfrak{S}$ is 0-cancellative.

PROOF. Let $a,b,c \in S$ satisfy $ab = ac$ & $b < c$ or $ba = ca$ & $b < c$. Because $c = bx$ $(\exists\, x : x \neq e)$ the element $u = ab$ satisfies $u = ux$. So, any $y > u$ with

$x^n \geq y$ would imply $u = ux^n \geq uy \geq y > u$, a contradiction. Thus (1) and (3) are verified.

Moreover $\mathfrak{S}$ is strictly archimedean. Hence – with a suitable $k \in \mathbf{N}$ – from $a \neq e$ it follows next $a^k \geq u$ and thereby $a^k = u$. $\square$

As shown above, archimedean d-monoids are commutative, and hence strictly archimedean d-monoids are commutative *a fortiori*. On the other hand the situation is much clearer in the strictly archimedean case. So we give a special proof for this special case.

9. 3. 4 Proposition. *Any strictly archimedean d-semigroup* $\mathfrak{S}$ *is commutative.*

PROOF. W. l. o. g. we consider a positive $\mathfrak{S}$ without identity and discuss the cases:

(i) $\mathfrak{S}$ contains a minimal properly positive element a.

(ii) $\mathfrak{S}$ does not contain a minimal properly positive element.

Ad (i). Start from $b \in S$ and $a \neq b$. Then there exists an element $k \geq 1$ satisfying $a^k < b \leq a^{k+1}$ and an element $c \leq a$ satisfying $b = a^k c$. But it holds $a^{k+1} = a^k a \geq a^k c = b \leq a^{k+1} \rightsquigarrow b = a^{k+1}$. Hence b is a power of a and S is the set of powers of a with positive exponents.

Ad (ii): In this case for any $x \in S$, there exists an element $z \in S$ with $z^2 \leq x$, since $y < x \;\&\; x = y \cdot w \;\; z = \min(y, w) \Longrightarrow \min(y, w)^2 \leq x$.

Suppose now $ab < ba < v$, say $abx = ba$ and $z^2 \leq x\,,\; z \leq a\,,\; z \leq b\,(\exists z)$.

Then it results $z^m \leq a \leq z^{m+1} \;\&\; z^n \leq b \leq z^{n+1}\,(\exists\, m, n \in \mathbf{N})$, recall 9.3.3. But this leads to $z^{m+n} \leq ab, ba \leq z^{m+n+2}$, a contradiction w. r. t. $z^2 \leq x$.

If however $ab < ba = u(= 0)$, then it holds $b = ax < u \vee a = by < u$ and thereby $ax = xa \vee by = yb$, leading to $ab = ba$. $\square$

Now we are in the position to prove:

9. 3. 5 A Theorem of Hölder and Clifford. *Let* $\mathfrak{S}$ *be a strictly archimedean d-semigroup. Then* $\mathfrak{S}$ *admits an* order preserving embedding

(i) *into the semigroup of all non negative reals w. r. t. the natural order, henceforth denoted by* $\mathfrak{P}$, OR (ii) *into the semigroup of all reals of the interval* $[0,1]$ *w. r. t. the usual order and* $ab := \min(a+b,1)$, *henceforth denoted by* $\mathfrak{P}_1$,

OR (iii) *into the semigroup of all reals of the interval* $[0,1]$, *extended by the symbol* ∞ *and considered under* $ab := a+b$, *if* $a+b \le 1$, *and* $ab := \infty$, *if* $a+b > 1$, *henceforth denoted by* ${\mathfrak{P}_1}^\infty$.

PROOF. Let $\mathfrak{S}$ be generated by a single element a. Then all elements of $\mathfrak{S}$ satisfy:

$$(e <)a < a^2 < \ldots < a^n < \ldots \text{ or } (e <)a < \ldots < a^n = a^{n+1},$$

and the function
$$a^k \to k \text{ or } a^k \to \frac{k}{n}$$
provides an o-isomorphic embedding of $\mathfrak{S}$ into $\mathfrak{P}$ or into $\mathfrak{P}_1$.

If, however, $\mathfrak{S}$ is not generated by a single element we drop the identity of $\mathfrak{S}$ if $\mathfrak{S}$ is a monoid. Then for any $x \in S$ there exists some $z \in S$ such that $z^2 \le x$ is valid. And this leads in case of $v < x$ and, say $vw = x$, to $z^2 := (v \wedge w)^2 < x$. Summarizing we get: For any $t \in \mathbf{N}$ there exists some $z \in S$ such that $z^t \le x$ is satisfied.

Suppose now that $\mathfrak{S}$ contains a maximal element u. Then we choose some $a < u$, Otherwise we choose an arbitrary $a \in S$ and define a function f on S as follows:

For each $b < u$ we form two classes of pairs of positive natural numbers:

$$\begin{array}{rcl} L_b &=& [\,(m,n)\,|\, x^m \le b \text{ and } a \le x^n \ \ (\exists\, x \in S)\,] \\ & \text{and} & \\ U_b &=& \big[\,(k\,,\,\ell)\,|\, b \le y^k \text{ and } \ y^\ell \le a \ \ (\exists\, y \in S\,)\big] \end{array}$$

According to the strict archimedean character of $\mathfrak{S}$ neither L_b nor U_b is empty. We show:

$$\frac{m}{n} \le \frac{k}{\ell} \text{ for all } (m,n) \in L_b \text{ and } (k,\ell) \in U_b. \tag{9.3}$$

To this end observe: For any (arbitrary large) $t \in \mathbf{N}^+$ we find some $z \in S$ with $z^t \le \min(x,y)$. Hence it holds $r \ge t$ and $s \ge t$ for all elements r, s defined by $z^r \le x < z^{r+1}, z^s \le y < z^{s+1}$. Consequently, we get

$$z^{rm} \le b < z^{(s+1)k} \quad \text{and} \quad z^{s\ell} \le a < z^{(r+1)n},$$

leading to $rm < (s+1)k$ and $s\ell < (r+1)n$, and we infer that

$$\frac{m}{n} < \left(1+\frac{1}{r}\right)\left(1+\frac{1}{s}\right)\frac{k}{\ell}$$

is satisfied for arbitrary elements r, s. Hence, it holds (9.3).

Start now from some $t > 0$. Then there exists some x with $x^t \leq \min(a, b)$. So we get elements $r, s \geq t$ with $x^r \leq a \leq x^{r+1}$ and $x^s \leq b \leq x^{s+1}$, that is with $(s, r+1) \in L_b$ and $(s+1, r) \in U_b$.

$$t \longrightarrow \infty \Longrightarrow \frac{s+1}{r} - \frac{s}{r+1} \longrightarrow 0$$

So, according to (9.3) there exists exactly one real number β for each chosen b, satisfying:

$$\frac{m}{n} \leq \beta \leq \frac{k}{\ell} \text{ for all } \quad (m,n) \in L_b \text{ and } \quad (k,\ell) \in U_b\,.$$

We put $f(b) := \beta$ for all b under consideration. In particular this means $f(a) = 1$, recall a is a b as well.

Next $b_1 \leq b_2$ implies $L_{b_1} \subseteq L_{b_2}$. So $f : S\backslash\{u\} \longrightarrow \mathbf{R}$ is isotone with $f(x) > 0$ for any $x \in S\backslash\{u\}$. Moreover it holds

$$f(bc) = f(b) + f(c)\,,$$

whenever $bc < u$ is satisfied – choose $z \in S$ small enough. Hence $f(x) = f(y)$ is satisfied if and only if $x = y$.

Now, we consider the different two cases (1) and (2) below:

(1) Let $\mathfrak{S}$ be cancellative. Then $\mathfrak{S}$ doesn't contain a maximal element. So, in this case f is an o-isomorphism (order preserving embedding) of $\mathfrak{S}$ in $\mathfrak{P}$.

(2) Suppose now that $\mathfrak{S}$ is not cancellative. Then according to 9.3.3 $\mathfrak{S}$ contains a maximum u. But the range of f over $S\backslash\{u\}$) is bounded, since in case of $a^k = u$ it results that k is an upper bound:

Hence there exists a minimum α with $f(x) \leq \alpha$ $(\forall x \in S\backslash\{u\})$.

Suppose now that there exists no $c \in S\backslash\{u\}$ with $f(c) = \alpha$. Then we put $f(u) = \alpha$. Otherwise we put $f(u) = \infty$.

Put now

$$g(x) = \frac{1}{\alpha} \cdot f(x)\,.$$

Then $g(x)$ is obviously an *order preserving isomorphism* (*o-isomorphism*) of $\mathfrak{S}$ into $\mathfrak{P}_1$ or $\mathfrak{P}_1^\infty$.

This completes the proof. □

It is easily shown that two o-isomorphisms of $\mathfrak{S}$ into $\mathfrak{P}$ differ – at most – by a positive factor, whereas those into $\mathfrak{P}_1$ or into $\mathfrak{P}_1{}^\infty$ are necessarily identic.

9. 3. 6 Corollary. *Any strictly archimedean positive cancellative semigroup $\mathfrak{S}$ satisfying $a < b \Longrightarrow a \,|\, b$ without an identity element but with a smallest element is order isomorphic with* $(\mathbf{N}, +)$.

PROOF. Let a be the smallest element of $\mathfrak{S}$. Then $a < a^2 < \ldots < a^n \ldots$

Suppose now $a^n < x \leq a^{n+1}$. Then for some $y \leq a$ it follows $x = ya^n$, leading to $x = a^{n+1}$. Hence S contains exactly the powers of a. □

The preceding results justify to call strictly archimedean d-semigroups also *real d-semigroups.*

By the propositions of this chapter we succeed in completing our results on subdirectly irreducible d-semigroups.

9. 3. 7 Definition. Let $\mathfrak{S}$ be an arbitrary d-semigroup. Then by $\mathfrak{S}^\bullet$ we mean the d-semigroup $\mathfrak{S}$, extended by a zero element 0.

9. 3. 8 Proposition. *Let $\mathfrak{S}$ be an archimedean subdirectly irreducible d-semigroup. Then $\mathfrak{S}$ admits an embedding into $\mathfrak{R}^\bullet$ or into $\mathfrak{P}_1^\infty$.*

PROOF. Let a, b be a critical pair and assume w.l.o.g. $a < b$. Recall that $\mathfrak{S}$ is linearly ordered and consider the positive and the non positive case.

If $\mathfrak{S}$ is positive, then $\mathfrak{S}$ is o-isomorphic to $\mathfrak{S}/\{x \,|\, x > a\}$.

If, however, in the opposite case it holds for instance $c < 1$, then $\mathfrak{S}$ contains a group $\mathfrak{G}$, and a must belong to G , since the elements x outside of G satisfy $xg = x$ for all $g \in G$, since $\mathfrak{S}$ is linearly ordered. Consequently in case of $a \notin G$ we succeed by shrinking the elements of G to a new identity element.

Thus in both cases the theorem of Hölder and Clifford contributes essentially to analyzing the situation. □

The results of this section could also have been developed by showing first that any strictly archimedean d-semigroup is commutative, in order to prove afterwards that any strictly archimedean d-semigroup is linearly ordered and then to apply the theorem that any cancellative (0-cancellative) positive strictly archimedean d-monoid $\mathfrak{S}$ can be embedded into the cancellative (0-cancellative) linearly ordered complete d-semigroup of its v-ideals.

Hereafter only the three cases, considered above, are possible: The case, in which $\mathfrak{S}$ contains no maximum, the case in which $\mathfrak{S}$ contains a maximum with hyperatom and the case in which $\mathfrak{S}$ contains a maximum without such an hyperatom.

The embedding of this chapter is then done by a short cut.

OBSERVE: Since in a complete linearly ordered d-monoid any $a > 0$ has a unique *square root* or additively spoken admits a *bisection,* any a admits a *binary representation.*

9.4 Archimedean Linear d-semigroups

Based on HÖLDER and CLIFFORD we are now in the position, to present a construction theorem for arbitrary linear archimedean d-semigroups.

To this end we observe first that the archimedean classes, considered in general in proposition 5.3.4, in totally ordered d-semigroups satisfy the implication $a_\approx \cap b_\approx = \emptyset \;\&\; a < b \Longrightarrow x \in a_\approx \;\&\; y \in b_\approx \Rightarrow x < y \;\&\; xy = y$. So we get:

9. 4. 1 Proposition. *The archimedean classes in totally ordered positive archimedean d-semigroups are of type $\mathfrak{P}$, $\mathfrak{P}_1$, $\mathfrak{P}_1^\infty$, or $(\{e\}, \cdot)$.*

9. 4. 2 Proposition. *Any linear archimedean d-semigroup is an ordinal sum of components of type $\mathfrak{P}, \mathfrak{P}_1, \mathfrak{P}_1^\infty$ or isomorphic to some chain w.r.t.* max.

PROOF. Since the classes are closed under multiplication, by the archimedean property all elements of lower classes are units of all elements of higher classes.

Consider now a totally ordered set $\mathfrak{I}$ and replace each of its elements i by some $\mathfrak{S}_i$ of the above types.

Then putting $a \circ b = \max(a, b)$ if a, b live in different components, and $a \circ b = c$ if a and b belong to the same component and their product in this component is equal to c, we get a totally ordered archimedean d-semigroup, called the ordinal sum[3)] $\sum \mathfrak{S}_i$. $\square$

So we arrive at:

9. 4. 3 Theorem. *Any positive linear archimedean d-semigroup* $\mathfrak{S}$ *with zero* 0 *can be embedded into a conditionally complete* $\bigvee$*-continuous d-monoid.*

PROOF. We consider a *gap*, recall, that is a Dedekind cut $(A \,|\, B)$ whose A has no last element and whose B has no first element, and assume that there exists no pair x, x^k with $x \in A, x^k \in B$. Then this gap can be filled canonically by some α by defining $a\alpha = \alpha$ if $a \in A$, $\alpha\alpha = \alpha$ and $\alpha b = b$ if $b \in B$. So, considering the set of all such elements α and defining $\alpha\beta = \max(\alpha, \beta)$ if α and β are separated by some $x_{\approx}$ we obtain an extension whose archimedean classes are separated by at least one idempotent.

Now in a second step, which could also have been done as the first step, we replace the equivalence classes by their complete extensions and extend the multiplication canonically.

Thus $\mathfrak{S}$ is embedded in a conditionally complete totally ordered d-semigroup $\sum$, and moreover by construction $\sum$ is even $\bigvee$-continuous.

This completes the proof. $\square$

HOWEVER (!)

9. 4. 4 Lemma. *Not any positive linear archimedean d-semigroup admits an embedding in a* $\bigwedge$*-continuous d-semigroup.*

Observe:

Any complete d-semigroup is archimedean. Hence any complete d-semigroup embedding of $\mathfrak{P}_1^\infty$ must satisfy $1 \circ \bigwedge x_{x\neq 0} = 1 \neq \infty = \bigwedge (1 \circ x)_{x \neq 0}$.

9.5 Interval Semigroups

Hereafter we are in the position to characterize classical sub-d-semigroups of the real unit interval by means of topology.

3) This construction was first presented by Fritz Klein-Barmen, compare [76].

9. 5. 1 Definition. By a continuum we mean a continuous chain $\mathbf{C}$.

As the most classical example we mention the real unit interval $\mathbf{E}$. But there exist also continua of higher cardinality than $\aleph$, as is easily seen. For instance: Replace the elements β of a well ordered set of what cardinality ever by the set $\{(\beta|r)\ \ (r \in \mathbf{R}^+)\}$, adjoin an element ∞ and extend the operation canonically.

Next a short cutout of Hofmann and Mislove, [64].

"A linearly ordered set I is called a *closed interval* if I contains a largest element 1 and a smallest element 0 and the order is complete and order dense. In this case I equipped with the order topology is compact and connected....

OBSERVE, $([-1,1],\cdot)$ is a compact connected topological semigroup, but, of course, it is not a totally ordered semigroup, consider $-1 < 0$, but $-1\cdot -1 = 1 > 0\cdot -1$....

9. 5. 2 Definition. A topological semigroup [4)] $\mathfrak{S}$ defined on a closed interval I equipped with the order topology is called an *I-semigroup*, if the 1 acts as an identity and the 0 as an *annihilator* [5)] of the semigroup $\mathfrak{S}$.

.... Three basic examples of I-semigroups [are] quickly surfaced.

1. The *real interval* $[0,1]$ under multiplication. Additively one can obtain this example by adjoining ∞ to the non negative reals $\mathbf{R}^+$ and letting ∞ act as an annihilator (the isomorphism being given by $t \longrightarrow -\log(t), 0 \longrightarrow \infty$).

2. The *nil interval* (pointed out by Calabi) can be defined on $[1/2,1]$ by defining $x\circ y := \max\{1/2, xy\}$. Note that all elements except 1 are nilpotent. It can alternately be obtained by shrinking the semigroup ideal $[0,1/2]$ of $[0,1]$ to a point and obtaining the Rees quotient semigroup $[0,1]/[0,1/2]$, or additively as the Rees quotient $\mathbf{R}^+[1] = \mathbf{R}^{\geq 0}/[1,\infty)$.

3. The *min interval,* is a commutative idempotent semigroup (i. e. a semilattice) and is defined on $[0,1]$ by $x\circ y := \min\{x,y\}$....

The systematic study of I-semigroups was initiated by W. M. Faucett in [53] and [54]. [He obtained]

9. 5. 3 Theorem. (Faucett 1955) *An I-semigroup is naturally totally ordered and commutative.*

[4)] that is, satisfying the rule of limits $(a_n) \longrightarrow a$ & $(b_n) \longrightarrow b \Longrightarrow (a_n\circ b_n) \longrightarrow a\circ b$,

[5)] that is as zero with the property $a \neq a^2 \Longrightarrow (a_n) \longrightarrow 0$.

9. 5. 4 Theorem. (FAUCETT 1955) *If $\mathfrak{S}$ is an I-semigroup with set of idempotents $E(S) = \{0, 1\}$ and $\mathfrak{S}$ contains no nilpotent elements, then $\mathfrak{S}$ is topologically isomorph to the real unit interval $[\,0, 1\,]$ under multiplication.*

The article of HOFMANN & LAWSON in[64] gives a good insight and survey, as well, w.r.t. the theory of measurement, totally ordered semigroups and one-parameter semigroups and may hence be considered as the best possible introduction to this field of mathematics, a field which was studied by highly recommended authors in highly recommended journals, including five papers of CLIFFORD on totally ordered semigroups, to cite only one cf. [42], and moreover papers of MOSTERT & SHIELDS on a compact manifold with boundary, cf. [80], [81], [82], and various other aspects, in addition.

Let henceforth $\mathbf{C}$ be a continuum endowed with an associative operation $\circ$, continuous w.r.t. the order topology. Then

$$x \longrightarrow s \circ x \ \ (s \in C)\,, \ y \longrightarrow y \circ s \ \ (s \in C) \text{ and } x \longrightarrow x \circ s \circ y \ \ (s \in C)$$

are *order-continuous* mappings.

9. 5. 5 Proposition. (FAUCETT 1955) *Any I-semigroup is a complete totally ordered d-semigroup, and is thereby in addition commutative.*

PROOF. Let $(I, 0, 1, \circ)$ be an interval semigroup with order $\succeq$. Then $a \circ I = [\,0, a\,] = I \circ a$.

SINCE: On the grounds of the intermediate value theorem, any value between $a \ (= a \circ 1)$ and $0 \ (= a \circ 0)$ is taken by $s \circ x$ and $y \circ s$, whence it holds $a \succeq b \Longrightarrow a \circ u = b = v \circ a \ \ (\exists\, u, v)$.

Hereby it follows next that idempotents satisfy $u \succeq a \Longrightarrow au \preceq a$, since $u \succeq a$ implies immediately $au = a$, and $a \circ u \succeq a$ implies $x \circ a \circ u = a \Longrightarrow a \circ u = a$.

Next we get nearly immediately $a^2 \neq a \succ b \Longrightarrow ab \preceq b$ since $ab \succeq b \Longrightarrow abx = b \Longrightarrow a^n b x^n = b \Longrightarrow a = a^2 \vee b = 0$. So, summarizing we get

$$a \succeq b \Longleftrightarrow \exists\, x, y : ax = b = ya\,.$$

Consequently $\mathfrak{S}$ is a d-semigroup w.r.t $x \leq y := x \succeq y$ with identity 1 and zero element 0.

Finally $\mathfrak{S}$ is archimedean, according to 7.2.6, and hence commutative. □

9. 5. 6 Proposition. (FAUCETT 1955) *An I-semigroup $\mathfrak{S}$ with exactly 2 idempotents is isomorphic to the real unit interval under multiplication or* *equivalently additively isomorphic to* $\mathfrak{P}$ *iff any nilpotent element is equal to the zero element* 0.

PROOF. By assumption $(S, \succeq)$ is complete and connected and $\mathfrak{S}$ is a strictly archimedean d-semigroup satisfying $a \neq 1 \Longrightarrow a^n \neq 0$. $\square$

9. 5. 7 Proposition. (CLIFFORD 1954) *An I-semigroup* $\mathfrak{S}$ *with exactly* 2 *idempotents is topologically isomorphic to the real unit interval under multiplication divided by the ideal* $[0, 1/2]$ *or – additively spoken – topologically isomorphic to* $\mathfrak{P}_1$ *iff there exists at least one not vanishing nilpotent element.*

PROOF. Clearly, if a is nilpotent, then all $x \preceq a$ are nilpotent, too. Moreover any x properly between 1 and 0 must be nilpotent since otherwise some element $\bigwedge x^n \succeq a$ would be idempotent but different from 0 and 1.

Hence $\mathfrak{S}$ is complete and strictly archimedean.

Moreover by assumption the chain $(S, \succeq)$ is connected. So $\mathfrak{S}$ cannot admit an embedding in $\mathfrak{P}_1^\infty$. Therefore it must be isomorphic to a sub-d-semigroup of $\mathfrak{P}_1$ and contain a countable subset, dense in $(S, \succeq)$.

Consequently by 9.1.10 the chain $(S, \succeq)$ is order isomorphic to the real unit interval $[\,0, 1\,]$. $\square$

ADDED in August 2013.

Recall: By Hausdorff any multiplication closed chain of a *cdl*-semingroup $\mathfrak{S}$ admits an extension to a maximal multiplication closed chain of $\mathfrak{S}$.

9. 5. 8 Proposition. *Let* $\mathfrak{S}$ *be a cdl-semigroup, recall definition 2.1.8, with a dense complete lattice satisfying* $s \cdot (\bigvee a_i) \cdot t = \bigvee (s a_i t)$. *Then any maximal multiplivation closed chain is naturally ordered.*

PROOF. Along the lines of the 9.5.5-proof, here left to the reader. $\square$

Chapter 10

Jakubuik Chains in lo-groupoids

A mathematical result may be ingenious or fundamental, may be merely beautiful, or even beautiful and fundamental, too. A result of the second type is Jakubík's Chain Theorem, at least to the author's mind. It says:

Jakubík's Chain Theorem. Any unbounded convex chain of an ℓ-group $\mathfrak{G}$ containing the identity element 1 is a direct factor of $\mathfrak{G}$.

Observe, any unbounded convex chain is a maximal chain, but there may exist maximal unbounded chains which are not convex. For instance consider in $(\mathbf{N}, |\,)$ the chain

$$1, 2\,,\, 2\cdot 3\,,\, 2\cdot 3\cdot 5\,,\, 2\cdot 3\cdot 5\cdot 7\,,\, ...$$

Jakubík's theorem is exhibited in [72], and the topic is taken up again in [**?**]. There a corresponding theorem is given for MV-Algebras. But in fact, that paper provides more, as will be pointed out in the present paper.

10. 0. 9 Definition. By a left divisibility-groupoid, for short LD-groupoid, we mean an inf-closed $p.o.$-groupoid $\mathfrak{G} = (G, \wedge, \cdot, 1)$ with identity element 1, that is $a \cdot 1 = a = 1 \cdot a$, satisfying

(LD) $$a \leq b \;\Rightarrow\; \exists\, x : a \cdot x = b$$

(DSM) $$\begin{aligned} a \cdot (b \wedge c) &= ab \wedge ac \\ (a \wedge b) \cdot c &= ac \wedge bc\,. \end{aligned}$$

If in addition $\mathfrak{G}$ is a right divisibilty- groupoid that is if $\mathfrak{G}$ satisfies moreover

(RD) $$a \leq b \;\Rightarrow\; \exists\, y : y \cdot a = b$$

we call $\mathfrak{G}$ a divisibility groupoid, briefly a D-groupoid.

Finally if $\mathfrak{G}$ is an LD-groupoid satisfying

$$\text{(RN)} \qquad \forall\, a, b \,\exists\; a^\circ \perp b^\circ : (a \wedge b)a^\circ = a \;\&\; (a \wedge b)b^\circ = b$$

we call $\mathfrak{G}$ a right normal LD-groupoid, briefly an RN-LD-groupoid, and consequently, if $\mathfrak{G}$ is even a right normal D-groupoid we call $\mathfrak{G}$ an RN-D-groupoid.

Clearly (LD) results from (RN), so we could omit axiom (LD) from the logical point of view. Observe

So far no joins were required !

Classical examples are ℓ-loops and normal complementary semigroups, nowadays called hoops, that is complementary semigroups satisfying (N) $x \leq a * b, b * a \Longrightarrow x = 1$, compare [15], [25]. Therefore also partially ordered sets are included inasmuch brouwerian semilattices satisfying (N) are subdirectly decomposable into totally ordered brouwerian lattices, that is chains, considered w.r.t. $a * b = 1$ if $a \geq b$ and $a * b = b$ if $a \not\geq b$.

To begin with let $\mathfrak{G}$ be a positive RN-LD-groupoid, that is let $\mathfrak{G}$ satisfy $1 \leq g \ \ (\forall g \in G)$.

Henceforth, whenever a RN-LD-groupoid is considered, let a°, b° tacitly be a pair of elements satisfying the conditions of axiom (RN) w.r.t a, b. Clearly, under this assumption x°, y° are incomparable whenever x, y are incomparable.

10. 0. 10 Lemma. *Let $\mathfrak{G}$ be a positive RN-LD-groupoid and let $[1, a]$ and $[1, b]$ be chains with incomparable elements a, b. Then $a \perp b$.*

PROOF. Since a, b are incomparable, a° and b° are incomparable, too. But $a \wedge b$ and a° belong to $[1, a]$ and $a \wedge b$ and b° belong to $[1, b]$. Therefore it must hold $a \wedge b \leq a^\circ, b^\circ$, that is $a \wedge b \leq a^\circ \wedge b^\circ = 1$. $\square$

Next we prove:

10. 0. 11 A splitting Lemma.

$$\text{(SP)} \quad y \leq ab \;\&\; (a \wedge y)y^\circ = y \Longrightarrow y = (y \wedge a)y^\circ \wedge yb \wedge ab = (y \wedge a)(y^\circ \wedge b)\,.$$

10. 0. 12 Lemma. *Let $\mathfrak{S}$ be a positive RN-LD-groupoid and let $[1, a]$ be a chain. Then $[1, a^2]$ is a chain, too.*

PROOF. Suppose that $x, y \in [\,1, a^2\,]$ are incomparable. Then x° and y° are incomparable, too, that is $x^\circ \neq 1 \neq y^\circ$. But it is $(a \wedge x^\circ) \wedge (a \wedge y^\circ) = 1$ which means $a \wedge x^\circ = 1 \vee a \wedge y^\circ = 1$, say $a \wedge x^\circ = 1$, and thereby $x^\circ \leq (x^\circ)^2 \wedge x^\circ a \wedge a x^\circ \wedge a^2 = (x^\circ \wedge a)(x^\circ \wedge a) = 1 \rightsquigarrow x^\circ = 1$, a contradiction. $\square$

By lemma 10.0.12 it follows immediately

10. 0. 13 Lemma. *In a positive RN-LD-groupoid any convex maximal chain is multiplication closed.*

Now we are ready to prove:

10. 0. 14 A first Factor Theorem. *Let $\mathfrak{S}$ be a positive RN-LD-groupoid and let C be an unbounded convex chain in $\mathfrak{S}$. Then $S = C \cdot C^\perp$ and $S = C \cdot C^\perp$ is a direct decomposition of $(C, \wedge)$.*

PROOF. Since C is unbounded, for any $a \in S$ there exists some x in C with $x \not\leq a$, that is with $a \wedge x < x$. Let now $(a \wedge x) \cdot x^\circ = x$ and $(a \wedge x) \cdot a^\circ = a$ be satisfied.

Then $a \wedge x < x$ implies $x^\circ \neq 1$, whence $x \wedge x^\circ \wedge a^\circ = 1 \rightsquigarrow a^\circ \wedge x = 1$.

Next consider some $c \in C$ above x. Then $a^\circ \wedge c$ belongs to C and must satisfy $a^\circ \wedge c \leq x$ that is $a^\circ \wedge c = 1$.

Hence a° is orthogonal to all elements of C, that is a° belongs to $C^\perp$. This implies $a = (a \wedge x) \cdot a^\circ \in C \cdot C^\perp$ for all $a \in S$, that is $S = C \cdot C^\perp$.

It remains to show that $a = u.v = x.y \in C \cdot C^\perp$ implies $u = x$ and $v = y$.

Here we succeed by the splitting-lemma, observe

$$x = (x \wedge u)(x^\circ \wedge v) = x \wedge u \rightsquigarrow x \leq u$$

and hence by duality $x = u$ – and $y = (y \wedge u)(y \wedge v) = y \wedge v \rightsquigarrow y \leq v$, that is even $y = v$.

FINALLY in case of $a \perp b, d\ rc \perp a, d$ we get:

$$\begin{aligned} ab \wedge cd &= a(b \wedge cd) \wedge cd \\ &= (a \wedge cd)(b \wedge d) \wedge cd \\ &= (a \wedge c)(b \wedge d) \wedge cd \\ &= (a \wedge c)(b \wedge d)\,, \end{aligned}$$

that is $\wedge$ respects the decomposition property. This completes the proof. $\square$

Sofar all results hold in any positive RN-LD-groupoid, and it has been shown that the set S may be considered as cartesian product $S = C \cdot C^{\perp}$.
As a main tool for the next proof we remark

$$a \wedge bc = a \wedge ac \wedge bc = a \wedge (a \wedge b)c \tag{10.6}$$
$$a \wedge bc = a \wedge ba \wedge bc = a \wedge b(a \wedge c)\,. \tag{10.7}$$

Now we are ready to verify

10. 0. 15 A second Factor Theorem. *Let $\mathfrak{S}$ be a positive LD-groupoid satisfying*

$$\text{(DSJ)} \qquad \begin{aligned} a \cdot (b \vee c) &= ab \vee ac \\ (a \vee b) \cdot c &= ac \vee bc\,, \end{aligned}$$

for instance let $\mathfrak{S}$ a an ℓ-loop cone, and suppose $S = C \times C^{\perp}$. Then $\cdot$ respects $\times$.

PROOF. In any LD-groupoid it holds

$$u \perp v \;\&\; u, v \leq w \;\&\; w = ux \Longrightarrow v = (u \wedge v) \cdot (v \wedge x) = v \wedge x \Longrightarrow uv \leq w\,, \tag{10.9}$$

that is

$$u \perp v \Longrightarrow uv = u \vee v = vu\,. \tag{10.10}$$

So, in case of $a, c \in C$ & $b, d \in C^{\perp}$ by $u \wedge vw \leq (u \wedge v)(u \wedge w)$ we get first $ac \in C$ & $cd \in C^{\perp}$, and thereby next

$$\begin{aligned} ab \cdot cd = (a \vee b) \cdot (c \vee d) &= ac \vee ad \vee bc \vee bd \\ &= ac \vee (a \vee d) \vee (b \vee c) \vee bd = ac \vee bd = ac \cdot bd \end{aligned} \tag{10.11}$$

This tells: multiplication respects the decomposition. $\square$

Finally we remark

10. 0. 16 A third Factor Theorem. *Let $\mathfrak{S}$ be an arbitrary RN-LD-<u>semigroup</u> and and suppose $S = C \times C^{\perp}$. Then multiplication respects $\times$.*

PROOF. If $\mathfrak{S}$ is positive we get $a \perp b \Longrightarrow ab = a \vee b$ as above. So in this case the presumption $a, c \in C$ & $b, d \in C^{\perp}$ leads to associativity by

$$ab \cdot cd = a(bc)d = a(cb)d = (ac)(bd)\,.$$

Let now $\mathfrak{S}$ be an arbitrary RN-DL-monoid and suppose

$$a(1 \wedge a)^{-1} = u \cdot v, (1 \wedge a)^{-1} = x \cdot y \;\; (x, u \in C, y, v \in C^{\perp})a\,.$$

Then

$$a = a(1{\wedge}a)^{-1}{\cdot}(1{\wedge}a) = uv{\cdot}x^{-1}y^{-1} = ux^{-1}{\cdot}vy^{-1} = \;\; (u, x^{-1} \in C, v, y^{-1} \in C^{\perp})\,.$$

Assume next

$$u_1x_1^{-1} \cdot v_1y_1^{-1} = u_2x_2^{-1} \cdot v_2y_2^{-1}$$

Then

$$u_1v_1 \cdot (y_1x_1)^{-1} = u_2v_2 \cdot (y_2x_2)^{-1}$$

with

$$u_1v_1 \perp y_2x_2 \text{ and } u_2v_2 \perp y_1x_1$$

which leads to $y_1x_1 = y_2x_2$ and hence by cancellation also to $u_1v_1 = u_2v_2$.

Hence

$$S = (C \cup C^{-1}) \times (C^{\perp} \cup (C^{\perp})^{-1})$$

It remains to verify that $(C \cup C^{-1})$ with $C^{-1} := \{c^{-1} \,|\, c \text{ invertible } \;\&\; c \in C\}$ forms a multiplication closed chain.

Clearly, $(C \cup C^{-1})$ forms a chain. In order to verify that $(C \cup C^{-1})$ is multiplication closed we show:

CASE 1. If $1 \leq a \leq b$ and a^{-1} exists we get $1 \leq a^{-1}b, ba^{-1} \leq b$ whence the products ab^{-1} and ba^{-1} belong to C.

CASE 2. If $1 \leq b \leq a$ and a^{-1} exists then also b^{-1} exists and $b^{-1}a$ and ab^{-1} belong to C. But this means that $a^{-1}b$ and ba^{-1} belong to C^{-1}. $\square$

Chapter 11

Special archimedean d-semigroups

11.1 Hyper-archimedean d-Semigroups

In this chapter we will study a type of d-semigroups stronger than archimedean d-semigroups in general but weaker than strictly archimedean d-semigroups.

In particular we will investigate *hyper-archimedean* and *super-archimedean* d-semigroups, and we shall see that *super-archimedean* d-semigroups are hyper-archimedean and hyper-archimedean ℓ-groups are super-archimedean.

11. 1. 1 Definition. A d-semigroup is called *hyper-archimedean*, if it satisfies:

(HY) $\qquad \forall a, t \in S^+ \ \exists\, n \in \mathbf{N} : \qquad t \cdot a \cdot t \leq a \vee t^n\,.$

Obviously the homomorphic images of a hyper-archimedean d-semigroup are again hyper-archimedean, and moreover any hyper-archimedean d-semigroup is *a fortiori* also archimedean. This provides – according to 9.3.8 –

11. 1. 2 Proposition. *The subdirect irreducible images of a hyper-archimedean d-semigroup are exactly the sub-d-semigroups of* $\mathfrak{P}$ *and* $\mathfrak{P}_1$ *, that is:*

Any hyper-archimedean d-semigroup is a subdirect product of real d-semigroups.

By 7.2.4 the canonical 1-extension of a hyper-archimedean d-semigroup is always archimedean. But moreover we even get:

11. 1. 3 Proposition. *Let* $\mathfrak{S}$ *be a hyper-archimedean d-semigroup, then* $\mathfrak{S}^1$ *is again hyper-archimedean.*

PROOF. Choose some $\alpha, \beta \in \Sigma^+$. Then, if $\alpha \vee \beta \in S^+$ and if e is a unit of $\alpha \vee \beta$, it follows by assumption:

$$\begin{aligned} \alpha \cdot \beta &\leq e\alpha \cdot e\beta \\ &\leq e\alpha \vee (e\beta)^n \\ &= e(\alpha \vee \beta^n) \\ &= \alpha \vee \beta^n \ \ (\exists\, n \in \mathbf{N})\,. \end{aligned}$$

Otherwise we may suppose $\beta \in \Sigma^+ \backslash S^+$ and $\beta = (1 \wedge a)(1 \wedge b)^{-1} \geq 1$. Then β is *coprime* to $f := 1 \vee b \in S^+$, because $(1 \wedge a)(1 \wedge b)^{-1} \leq (1 \wedge b)^{-1}$ and $(1 \wedge b)^{-1} \perp (1 \vee b)$. Consequently by the first part of the proof we get:

$$\alpha \cdot \beta \leq f\alpha \cdot \beta \ \leq \ f\alpha \vee \beta^m \ \ (\exists\, m \in \mathbf{N})\,.$$

Suppose now $1 \leq g \leq f$ with $g \in S^+$. Then it holds $g \perp \beta$, and it follows by analogy:

$$\alpha \cdot \beta \leq g\alpha \cdot \beta \ \leq \ g\alpha \vee \beta^n \ \ (\exists\, n \in \mathbf{N})\,.$$

We define $k := \min(m, n)$. Then it results

$$\begin{aligned} \alpha \cdot \beta &\leq (f\alpha \wedge g\alpha) \vee (f\alpha \wedge \beta^n) \vee (g\alpha \wedge \beta^m) \vee \beta^k \\ &= g\alpha \vee (\alpha \wedge \beta^n) \vee (\alpha \wedge \beta^m) \vee \beta^k \\ & \ (\text{observe } f, g \perp \beta) \\ &= g\alpha \vee \beta^k \\ &\leq g\alpha \vee \beta^m\,, \end{aligned}$$

that is $\alpha \cdot \beta \leq g\alpha \vee \beta^m$ for all elements g between 1 and f. But this means – in case of $x = xe \in S^+$ with some e between 1 and g:

$$x \cdot \alpha\beta \ \leq \ x \cdot (\alpha \vee \beta^n)\,,$$

which by varying the element x according to 3.1.10 [1] provides

$$\alpha \cdot \beta \ \leq \ \alpha \vee \beta^n\,.$$

Thus the proof is complete. □

Now we are in the position to prove

11. 1. 4 Proposition. *Let $\mathfrak{S}$ be a d-semigroup. Then the following are pairwise equivalent:*

[1] Recall: $1 \wedge c$ stands for $I \wedge F_c = \overline{F}_c$, an automorphism of $\mathfrak{S}$. So it holds $1 \wedge a = 1 \wedge b$ iff $x(1 \wedge a) = x(1 \wedge b)$ $(\forall x \in S)$.

(*i*) $\mathfrak{S}$ *is hyper-archimedean.*

(*ii*) $\mathfrak{S}$ *satisfies* $\forall a, t \in S\ \exists n \in \mathbf{N} : t \cdot a \cdot t \leq a \vee t^n$.

(*iii*) *Any homomorphic image of* $\mathfrak{S}$ *is archimedean.*

(*iv*) *Any irreducible ideal of* $\mathfrak{S}$ *is archimedean.*

(*v*) *Any irreducible filter of* $\mathfrak{S}$ *is primary.*

(*vi*) *The semigroup of (lattice) ideals of* $\mathfrak{S}$ *is archimedean.*

(*vii*) *Any irreducible ideal* P *of* $\mathfrak{S}$ *satisfies* $P = \ker(P) \cup \mathrm{rad}\,(P)$.

PROOF. (*i*) $\Longrightarrow$ (*ii*). Let (*i*) be satisfied. Then $\mathfrak{S}$ is archimedean and thereby commutative. Let moreover $a \geq 1$ and $t = xy^{-1}$ be satisfied in $\mathfrak{S}^1$ with $x \perp y$, that is with $x \cdot y^m = x \vee y^m$. Then for some suitable $n \in \mathbf{N}$ it results

$$\begin{aligned} ax \leq a \vee x^n \ &\Longrightarrow\ ax \vee ay^{n-1} \leq ay^n \vee x^n \\ &\Longrightarrow\ \quad axy^{n-1} = ax \vee ay^{n-1} \\ &\qquad\qquad\qquad\ \leq ay^n \vee x^n \\ &\Longrightarrow\ \quad axy^{-1} \leq a \vee (xy^{-1})^n \,. \end{aligned}$$

This leads to the general case – recall $a = (1 \wedge a)(1 \vee a)$ – by

$$\begin{array}{rcl} (1 \vee a)xy^{-1} & \leq & (1 \vee a) \vee (xy^{-1})^n \\ & \Longrightarrow & \\ (1 \wedge a)(1 \vee a)xy^{-1} & \leq & (1 \wedge a)(1 \vee a) \vee xy^{-1} \,. \end{array}$$

(*ii*) $\Longrightarrow$ (*iii*). If (*ii*) holds in $\mathfrak{S}$, then (*ii*) holds as well in any homomorphic image. Consequently any homomorphic image of $\mathfrak{S}$ is archimedean.

(*iii*) $\Longrightarrow$ (*iv*). Let P be an irreducible ideal with $t^n \in P$ $(\forall n \in \mathbf{N})$ and $a \in P$. Then in the linear homomorphic image $\mathfrak{S}/P$ it holds either $\overline{a} \leq \overline{t}^m$ for some $m \in \mathbf{N}$, or it holds $\overline{a}\,\overline{t} \leq \overline{a}$. But this means that $a \in P$ & $at \notin P$ is impossible.

(*iv*) $\Longrightarrow$ (*v*) results by definition.

(*v*) $\Longrightarrow$ (*vi*). Observe (*v*) $\Longleftrightarrow$ (*iv*) and (*iv*) $\Longrightarrow$ (*vi*) for irreducible ideals. Now, recall that any ideal B is equal to some intersection $\bigcap P_i$ $(i \in I)$ of irreducible ideals P_i . Hence in the case of $A^n \subseteq B$ $(\forall n \in \mathbf{N})$ it results:

$$\begin{aligned} A \subseteq B \ &\Longrightarrow\ A \subseteq P_i \ (\forall i \in I) \\ &\Longrightarrow\ AB \subseteq \bigcap AP_i \ (i \in I) = \bigcap P_i = B \,. \end{aligned}$$

$(vi) \Longrightarrow (vii)$. Let P be an irreducible and hence according to (vi) also an archimedean ideal and let t belong to P.

Now, if $t \notin \mathrm{Rad}\, P$ we get Then

$$\forall n \in \mathbf{N} : t^n \in P \rightsquigarrow Pt \subseteq P\,.$$

Thus, in any case, t belongs to $\mathrm{rad}\,(P) \cup \ker(P)$.

$(vii) \Longrightarrow (iii)$. By (vii) $\mathfrak{S}$ is archimedean and hence commutative, which results as follows:

Suppose w. l. o. g. that $t^n \leq a$ $(\forall n \in \mathbf{N})$ and $a < at$ $(t \in S^+)$. Then there exists an irreducible ideal P with $a, t^n \in P$ $(\forall n \in \mathbf{N})$ but $at \notin P$ in spite of $t \in \ker(P)$. Hence $a \cdot e_a \in P \Longrightarrow at \leq a \cdot t \cdot e_a \in P$.

Now we consider a subdirectly irreducible image $\overline{\mathfrak{S}}$ of $\mathfrak{S}$ with critical pair $a < b$. According to 5.4.9. $\overline{\mathfrak{S}}$ is a totally ordered 0-cancellative d-monoid. Hence the irreducible ideal $P := \{x \,|\, \overline{x} \leq \overline{a}\}$ satisfies $t^n \in P$ $(\forall n \in \mathbf{N}) \Longrightarrow ta \in P$, that is $\overline{t} \cdot \overline{a} = \overline{a}$, a contradiction w. r. t. the 0-cancellation property. Consequently, by (vii), for each $t \in P$ with $\overline{1} < \overline{t}$ there exists some $n \in \mathbf{N}$, satisfying $t^n \in S \backslash P$, that is $\overline{t}^n \geq \overline{a}$.

This means in particular that each $\overline{c}^{\,-1} < \overline{1}$ satisfies $\overline{c}^{\,n} \geq \overline{a}$ for some suitable $n \in \mathbf{N}$. Hence $\overline{\mathfrak{S}}$ is either positive and thereby isomorphic with $\overline{\mathfrak{S}}/\{\overline{y} \,|\, \overline{y} > \overline{a}\}$ or it is $\overline{\mathfrak{S}}$ equal to its cancellative kernel or $\overline{\mathfrak{S}}$ is equal to its cancellative kernel extended by a zero element 0.

$(iii) \Longrightarrow (i)$. Start from (iii) and suppose that $at \not\leq a \vee t^n$ $(\forall n \in \mathbf{N})$. Then there exists an irreducible ideal P with $a, t^n \in P$ $(\forall n \in \mathbf{N})$ but $at \notin P$. This provides in the linearly ordered and on the grounds of (iii) archimedean $\overline{\mathfrak{S}} := \mathfrak{S}/P$,

$$\forall n \in \mathbf{N} : \overline{t}^n < \overline{a} \;\&\; \overline{a} < \overline{a} \cdot \overline{t}\,,$$

since $\overline{a} \leq \overline{t}^m$, would lead to $\overline{a} \cdot \overline{t} \leq \overline{t}^m \cdot \overline{t}$ and thereby to $at \in P$, a contradiction. Consequently (iii) implies (i), that is $\mathfrak{S}$ must be hyper-archimedean. □

11.2 Super-archimedean d-semigroups

11. 2. 1 Definition. A d-semigroup $\mathfrak{S}$ is called *super-archimedean*, if it satisfies:

(SU) $$\forall a, t \in S^+ \;\exists\, n \in \mathbf{N} : a \wedge t^n = a \wedge t^{n+1}\,.$$

Obviously in particular any *locally finite* d-semigroup $\mathfrak{S}$ is super-archimedean.

In a super-archimedean $\mathfrak{S}$ by definition any $a \in S$, contains an idempotent (private) unit. Furthermore, by evidence any homomorphic image of a super-archimedean $\mathfrak{S}$ is super-archimedean and any subdirectly irreducible super-archimedean d-semigroup is strictly archimedean. So super-archimedean implies archimedean.

As a first hint to the relation between hyper- and super- we get:

11. 2. 2 Lemma. *Any super-archimedean d-semigroup $\mathfrak{S}$ is hyper-archimedean.*

Any hyper-archimedean ℓ-group is super-archimedean.

PROOF. Let $\mathfrak{S}$ be a d-semigroup with $t \in S^+$, $a \wedge t^n = a \wedge t^{n+1}$ and $(a \wedge t^n)a' = a$. Then $a \vee t^n = a \vee t^{n+1}$ and thereby furthermore

$$a \leq a \vee t^n \rightsquigarrow at \leq (a \vee t^n)t = t^n a' t = t^{n+1} a' = a \vee t^n \,.$$

Let next $\mathfrak{G}$ be an ℓ-group and $at \leq a \vee t^n$. Then it results

$$a \cdot t^{n+1} \leq (a^2 \vee at^{n+1}) \wedge (a \cdot t^n \vee t^{2n}) \leq (a \wedge t^n)(a \vee t^{n+1}) \leq a \cdot t^{n+1} \,,$$

that is

$$(a \wedge t^{n+1})(a \vee t^{n+1}) = (a \wedge t^n)(a \vee t^{n+1}) \rightsquigarrow a \wedge t^n = a \wedge t^{n+1} \,. \qquad \square$$

Now we can show:

11. 2. 3 Proposition. *If the d-semigroup $\mathfrak{S}$ is super-archimedean, then $\mathfrak{S}^1$ is super-archimedean as well.*

PROOF. Suppose $\alpha, \beta \in S$. Then there is nothing to show.

Otherwise, assume $\alpha \notin S^+$ but $\beta =: t \in S^+$. Then $\alpha = (1 \wedge a)(1 \wedge b)^{-1}$ with $a = 1 \ \vee \ a \in S$ and $b \in S$, and it holds $(1 \wedge a)(1 \wedge b)^{-1} \leq (1 \wedge b)^{-1}$, and thereby

$$(1 \wedge b)^{-1} \wedge t^n = (1 \wedge b)^{-1} \wedge t^{n+1} \Longrightarrow \alpha \wedge t^n = \alpha \wedge t^{n+1} \,.$$

Consequently it suffices to consider $\beta = (1 \wedge b)^{-1}$. To this end let us suppose $e \in E(t) \cap S^+$ and $1 \leq f \leq e$. Then because $e(1 \wedge b)^{-1} \in S^+$ it results for some $n \in \mathbf{N}$

$$e(1 \wedge b)^{-1} \wedge t^n \ = \ e(1 \wedge b)^{-1} \wedge t^{n+1} \,.$$

But for any x , f with $fx = x = xf$ and $1 \leq f \leq e$ this leads to

$$x((1 \wedge b)^{-1} \wedge t^n) \ = \ x((1 \wedge b)^{-1} \wedge t^{n+1}) .$$

Consequently, by varying x we get

$$(1 \wedge b)^{-1} \wedge t^n \ = \ (1 \wedge b)^{-1} \wedge t^{n+1} .$$

Suppose next $\alpha =: a \in S^+$ and $\beta = (1 \wedge a)(1 \wedge b)^{-1} \in \Sigma^+ \backslash S^+$. Then we can choose a unit u of a , which is coprime to β, for instance $(1 \vee b) \wedge e$ with positive unit e of a, and since $\mathfrak{S}$ is super-archimedean, we may assume in addition that u is idempotent. So we get $a \wedge (u\beta)^n = a \wedge (u\beta)^{n+1}$ $(\exists n \in \mathbf{N})$, and thereby:

$$\begin{array}{rrcl} & a \wedge (u\beta)^n & = & a \wedge (u\beta)^{n+1} \\ \rightsquigarrow & a \wedge (u \vee \beta^n) & = & a \wedge (u \vee \beta^{n+1}) \\ \rightsquigarrow & (a \wedge u) \vee (a \wedge \beta^n) & = & (a \wedge u) \vee (a \wedge \beta^{n+1}) \ . \end{array}$$

Because $u \perp \beta$ and $a = \alpha$ by intersecting with $a \wedge \beta^{n+1}$ this leads to:

$$\alpha \wedge \beta^n \ = \ \alpha \wedge \beta^{n+1} .$$

It remains to settle the case $\alpha \notin S$ & $\beta \notin S$. But in this case we are acting in the cancellative kernel and may infer:

Since $\mathfrak{S}$ is super-archimedean, according to 11.2.2 $\mathfrak{S}$ is hyper-archimedean as well. This proves the assertion. $\square$

Before presenting a representation theorem for super-archimedean d-semigroups recall the notion of a *real* d-semigroup, given in the preceding chapter on Hölder and Clifford.

11. 2. 4 Proposition. *Let $\mathfrak{S}$ be a d-semigroup. Then the following are pairwise equivalent:*

(*i*) *$\mathfrak{S}$ is super-archimedean.*

(*ii*) *All totally ordered images of $\mathfrak{S}$ are super-archimedean.*

(*iii*) *$\mathfrak{S}$ admits a subdirect decomposition into real factors such that the representing functions satisfy:*

$$\forall f, g \geq id \ \exists n \in \mathbf{N} : \ \ f(x)^n \geq g(x) \ \ (\forall x : f(x) > 0) .$$

(*iv*) *$\mathfrak{S}^+/F^+$ is locally finite for all filters $F^+ \subseteq \mathfrak{S}^+$.*

(v) $\mathfrak{S}$ *admits a subdirect decomposition into* $\mathfrak{C}(t)$ *and* $\mathfrak{S}/C(t)$.

PROOF. $(i) \Longrightarrow (ii)$ is evident, since together with $\mathfrak{S}$ even all homomorphic images are super-archimedean.

$(ii) \Longrightarrow (i)$. Let $\mathfrak{S}$ be represented as a subdirect product of real factors. Then, according to 9.3.8 there are positive and group factors, determining a positive homomorphic image $\mathfrak{S}_p$ and a homomorphic group image $\mathfrak{S}_g$, respectively, of $\mathfrak{S}$. So it suffices to show that (i) is satisfied in each of these images.

First we consider a product $\mathfrak{S}_p$ of strictly archimedean factors. Provided, for instance, it would hold $a \wedge t^n \neq a \wedge t^{n+1}$ $(\forall n \in \mathbf{N})$, then we could turn to $\mathfrak{S}_p/[a)$. This would be an image $\overline{\mathfrak{S}}$ with $\overline{t}^n \neq \overline{t}^{n+1}$ $(\forall n \in \mathbf{N})$ & $\overline{a} = \overline{0}$. Hence we may start from an image $\mathfrak{S}_1$ with $t^n \neq t^{n+1} < 0$ $(\forall n \in \mathbf{N})$. But then according to 6.2.2 there exists a maximal $E(t)$ containing c-ideal M, which is in addition irreducible. We form $\overline{\mathfrak{S}} := \mathfrak{S}/M$. Because

$$R(x,y,x',y') \Longrightarrow (t \wedge x)(t' \wedge x') = t \wedge x \Longrightarrow t' \in M \vee x' \in M$$

in this model all $\overline{x}$ are comparable with $\overline{t}$. Hence $\overline{x}$ is comparable also with all $\overline{t}^n$, consider t^n w.r.t. M. So, $\overline{F} := \{\overline{y} \mid \overline{y} > \overline{t}^n \ (\forall n \in \mathbf{N})\}$ is not empty because $\overline{0} \in \overline{F}$ and in addition it is a filter since $\overline{t}^n$ is comparable with all $\overline{x}$. But then $\overline{\overline{\mathfrak{S}}} := \overline{\mathfrak{S}}/\overline{F}$ is a totally ordered image which is not strictly archimedean, a contradiction!

Now we turn to the group case. Here hyper- and super- are equivalent.

So, if $\mathfrak{S}_g^+$ is not super-archimedean there exists a pair $t \neq 1, a$ in S^+ with $at \not\leq a \vee t^n$ $(\forall n \in \mathbf{N})$. Consequently, there must exist an irreducible ideal P with $a, t^n \in P$ $(n \in \mathbf{N})$ & $at \notin P$. But in $\mathfrak{S}_g/P =: \overline{\mathfrak{S}}$ this leads to

$$\overline{1} < \overline{t} \ \& \ \overline{t}^n \leq \overline{a} \ (\forall n \in \mathbf{N}) \ \& \ \overline{a} < \overline{a} \cdot \overline{t}\,,$$

since in case of $\overline{t}^m \geq \overline{a}$ it would result $at \in P$. But this contradicts the assumption of $a \cdot 1 \in P$ & $a \cdot t \notin P$.

$(i) \Longleftrightarrow (iii)$ is evident.

$(i) \Longleftrightarrow (iv)$ is nearly evident. For, suppose that some $\mathfrak{S}^+/F^+$ is not locally finite. Then there exist elements $a \in F^+, t \in S^+ \setminus F^+$ such that $a \wedge t^n \neq a \wedge t^{n+1}$ $(\forall n \in \mathbf{N})$ is satisfied. On the other hand if any $\mathfrak{S}^+/F^+$ is locally finite, then in particular any $\mathfrak{S}^+/[a)$ is locally finite, which implies condition (ii).

Hence we are through, once $(i) \Longleftrightarrow (v)$ is verified. To begin with we suppose that (v) is satisfied and show

$(v) \Longrightarrow (i)$. Obviously any two elements of $C(t)$ are congruent *modulo* $C(t)$. Hence the canonical mapping $\phi : \mathfrak{S} \longrightarrow \mathfrak{C}(t)$ generates a residue class image $\mathfrak{S}$, isomorphic with $\mathfrak{C}(t)$. But, here $\phi(a)$ lies below some $(\phi(t))^n$, whence we get:

$$\begin{aligned} \phi(a \wedge t^n) &= \phi(a) \wedge (\phi(t))^n \\ &= \phi(a) \wedge (\phi(t))^{n+1} \\ &= \phi(a) \wedge \phi(t^{n+1}) \\ &= \phi(a \wedge t^{n+1})\,. \end{aligned}$$

Therefor it must hold $a \wedge t^n = a \wedge t^{n+1}$.

It remains to show

$(i) \Longrightarrow (v)$. We consider first a super-archimedean positive $\mathfrak{S}$. Here any $a \in S$ produces a uniquely determined element $a \wedge t^n = a \wedge t^{n+1}$, since together with $a \wedge t^n = a \wedge t^{n+1}$ also $a \wedge t^{n+1} = a \wedge (a \wedge t^n)t = a \wedge (a \wedge t^{n+1})t = a \wedge t^{n+2}$ is satisfied. Thus we get a homomorphism ϕ. Observe, that

$$a \wedge t^{n+1} = a \wedge t^n \;=\; b \wedge t^n = b \wedge t^{n+1}\,,$$

leads to

$$\begin{aligned} \phi(a) &= \phi(b) \\ &\Longrightarrow \\ sa \wedge t^n &= s(a \wedge t^n) \wedge t^n \\ &= s(b \wedge t^n) \wedge t^n \\ &= sb \wedge t^n \\ &\Longrightarrow \\ \phi(sa) &= \phi(sb)\,, \end{aligned}$$

and that *a fortiori*

$$\begin{aligned} \phi(a) &= \phi(b) \\ &\Longrightarrow \\ \phi(s \wedge a) &= \phi(s \wedge b)\,. \end{aligned}$$

We consider:

$$x\,\rho\,y \;:\Longleftrightarrow\; \phi(x) = \phi(y)$$

$$\text{and} \quad x\,\sigma\,y \;:\Longleftrightarrow\; x \equiv y\;(C(t))\,.$$

Then
$$\begin{array}{rcl} x\,\rho\,y & \& & x\,\sigma\,y\,, \\ x \wedge t^k = y \wedge t^k & = & y \wedge t^{k+1} = x \wedge t^{k+1} \\ \text{and} \qquad x \leq yt^p & \& & y \leq xt^p \qquad (\exists k, p), \\ \text{that is} \qquad x \leq y \vee t^p & \& & y \leq x \vee t^p\,, \end{array}$$

and thereby for a suitable $\ell \in \mathbf{N}$

$$\begin{array}{rcl} x \wedge t^\ell & = & y \wedge t^\ell \\ \text{and} \qquad x \vee t^\ell & = & y \vee t^\ell\,. \end{array}$$

Hence it holds $x = y$. So, ρ and σ produce a subdirect decomposition of $\mathfrak{S} = \mathfrak{S}^+$.

Since together with $\mathfrak{S}^+$ also $\mathfrak{S}^{1+}$ is super-archimedean, the construction shows that the subdirect decomposition extends to $\mathfrak{S}^{1+}$, respectively that the congruence ρ is the reduction of $\rho_{\mathfrak{S}^{1+}}$ to $\mathfrak{S}$.

Consequently this proof is complete, once we have shown that the quotient hull $Q(\mathfrak{S}^{1+}) =: Q$ decomposes subdirectly even in the sense of the theorem. To this end suppose $\equiv\ \in \{\rho, \sigma\}$ on $\mathfrak{S}^{1+}$.

We consider the extensions of ρ, σ from $\mathfrak{S}^{1+}$ to $\mathfrak{S}^1$, according to 5.1.5. They provide a subdirect decomposition of $\mathfrak{S}^1$, and it is nearly immediately clear, that σ_Q doesn't make any problem. So it remains to verify that the extension of ρ works, too.

This is clear for positive elements, since we obtain:

$$\begin{array}{rcl} a^+\,\rho_Q\,b^+ & \Longleftrightarrow & a^+\,\rho\,b^+ \\ & \Longleftrightarrow & \phi\,(a^+) = \phi\,(b^+)\,. \end{array}$$

Let now a be an arbitrary element of $\mathfrak{Q}$. Then, inspired by the formula $a = a^+ \cdot a^- = a^+ \cdot (a^*)^{-1}$ with cancellable $\phi\,(a^*)$ we define

$$\phi\,(a) \ := \ \phi\,(a^+) \cdot (\phi\,(a^*))^{-1}\,,$$

which, according to the rules of arithmetic and to $\phi\,(a^+) \perp \phi\,(a^*)$ implies:

$$\begin{array}{rrcl} \phi\,(x) = \phi\,(y) \ \Longleftrightarrow & \phi\,(x^+) \cdot \phi\,(y^*) & = & \phi\,(y^+) \cdot \phi\,(x^*) \\ \Longleftrightarrow & \phi\,(x^+y^*) & = & \phi\,(y^+x^*) \\ \Longleftrightarrow & x^+y^* & \rho & y^+x^* \\ \Longleftrightarrow & x^+(x^*)^{-1} & \rho_Q & y^+(y^*)^{-1} \\ \Longleftrightarrow & x & \rho_Q & y\,. \end{array}$$

This completes the proof. $\square$

11.3 Discrete Archimedean d-Semigroups

By $\mathfrak{S}_n$ henceforth we will mean the d-semigroup, built by the set $\{0, 1, \ldots, n\}$ under – see above – $a \circ b = \min(a + b, 1)$ and $a \wedge b := \min(a, b)$. Obviously any $\mathfrak{S}_n$ is a sub-d-semigroup of $\mathfrak{P}_1$ and also of $\mathfrak{P}_1{}^\circ$.

11. 3. 1 Definition. A d-semigroup $\mathfrak{S}$ is called *discrete archimedean* if any subdirectly irreducible image $\overline{\mathfrak{S}}$ is of type $\mathfrak{Z}$ or $\mathfrak{Z}^\bullet$ or $\mathfrak{S}_n$.

11. 3. 2 Proposition. *For a d-semigroup* $\mathfrak{S}$ *the following are equivalent:*

(i) $\mathfrak{S}$ *is discrete archimedean.*

(ii) *If* P *is prime then* $A \subseteq P \Longrightarrow A \,|\, P$.

PROOF. (i) $\Longrightarrow$ (ii). Suppose $A \subseteq P \neq S$. $\mathfrak{S}/P$ is totally ordered and archimedean of type $\mathfrak{S}_n$, $\mathfrak{Z}$ or $\mathfrak{Z}^\bullet$. Furthermore no $x \in P$ is mapped to the eventual maximum of some homomorphic image – observe the implication:

$$y \notin P \;\&\; x \in P \;\Longrightarrow\; \exists e : xe = x \in P \;\&\; ye = y \notin P\,.$$

Consequently $\overline{P}$ is a principal ideal $(\,\overline{p}\,] \neq \overline{0}$, and it results $\overline{A} = (\,\overline{a}\,]\ (\exists\, a)$.
Choose now some $q \in P$. Then for suitable elements s it follows

$$q \;=\; (q \wedge a) \cdot s\,,$$

and each $a' \in A$ satisfies

$$\overline{a}\,' \cdot \overline{s} \;\leq\; \overline{a} \cdot \overline{s} = \overline{a} \vee \overline{q} \in \overline{P}\,.$$

But it holds $P = \{x \,|\, \overline{x} \leq \overline{p}\}$. Consequently we get $a's \in P$ and thereby $A \,|\, P$.

(ii) $\Longrightarrow$ (i). First we show that $\mathfrak{S}$ is hyper-archimedean. To this end let $t^n \leq a$ ($\forall n \in \mathbf{N}$) but $at \neq a$. Then there exists some maximal a containing but a, at separating ideal P, which by $T := \{x \,|\, x \leq\ t^n\ (\exists\, n \in \mathbf{N})\}$ leads to the contradiction

$$at \notin P \;\&\; P = XT\ \ (\exists X) = XTT = PT \ni at\,.$$

Hence $\mathfrak{S}$ is at least archimedean.

Let now $\overline{\mathfrak{S}}$ be a subdirectly irreducible homomorphic image of $\mathfrak{S}$. Then $\overline{\mathfrak{S}}$ is totally ordered, since $\mathfrak{S}$ is commutative, and we get:

$$\overline{t}^n \;\leq\; \overline{a} \;\; (\forall n \in \mathbf{N}) \Longrightarrow \overline{t} \cdot \overline{a} = \overline{a}\,.$$

For, putting

$$\begin{aligned} T \;&:=\; \{x \,|\, x \leq t^n \;\; (\exists\, n \in \mathbf{N})\} = TT \\ \text{and} \qquad P \;&:=\; \{x \,|\, \overline{x} \leq \overline{a}\}\,, \end{aligned}$$

it results $T \subseteq P$, that is, $P = TX$ and thereby $TP = P$. But this leads to $\overline{T}\,\overline{P} = \overline{P}$ and thereby to $\overline{t} \cdot \overline{a} = \overline{a}$. Consequently any subdirectly irreducible image of $\mathfrak{S}$ is archimedean, that is $\mathfrak{S}$ itself is even hyper-archimedean.

Now we infer:

If $\overline{\mathfrak{S}}$ is a subdirectly irreducible image w. r. t. $a < b$ and if in addition $\overline{c}^{\,-1} < \overline{1}$ $(\overline{c} \in C(\overline{\mathfrak{S}}) =: \overline{C})$, then $\overline{\mathfrak{C}}$ is isomorphic with $\mathfrak{Z}$. For, $\overline{\mathfrak{C}}$ admits an embedding into $\mathfrak{R}$, and if there would exists no minimal strictly positive element, we could form

$$\begin{aligned} A \;&:=\; \{a \,|\, \overline{a} < \overline{c}\} \\ P \;&:=\; \{p \,|\, \overline{p} \leq \overline{c}\} \end{aligned}$$

resulting in $A \subseteq P$ and thereby in $A \,|\, P$ and $\overline{A} \,|\, \overline{P}$, respectively, a contradiction!

Consequently $\overline{\mathfrak{S}}$ must be of type $\mathfrak{Z}$ or of type $\mathfrak{Z}^{\bullet}$. This is clear if $\overline{a} \in \overline{C}$.

And in case of $\overline{a} \notin \overline{C}$ it holds for all $\overline{c} \in \overline{C}$ the equation $\overline{a}\,\overline{c} = \overline{a}$, that is $\overline{C} \subseteq E(\overline{a})$, whence $E(\overline{a})$ must be equal to $\{\overline{1}\}$. So $\overline{\mathfrak{S}}$ couldn't contain a negative element.

But then it results – as above – that $\overline{\mathfrak{S}} \setminus \{\overline{1}\}$ contains a minimum. So in this case it must hold $\overline{\mathfrak{S}} \cong \mathfrak{S}_n$ $(\exists n \in \mathbf{N})$. □

The question arises whether in the preceding proposition even

$$A \subseteq B \;\;\Longrightarrow\;\; A \,|\, B$$

may be required. That such an request is too strong is verified by the product $\prod \mathfrak{S}_{i+1}$ $(i \in \mathbf{N})$. Consider the ideals

$$A := (\{f \,|\, f(j) = 0 \text{ for } j < i \;\; ; \;\; f(j) = i \text{ for } j \geq i\})$$

and
$$B \;:=\; (\{f \mid f(i) \leq i\})\ .$$

Then it holds
$$A \subseteq B \quad \& \quad A \nmid B\ .$$

11.4 Factorial d-Semigroups

As a special class of discrete archimedean d-semigroups will turn out the class of *factorial* d-semigroups.

11. 4. 1 Definition. A d-semigroup $\mathfrak{S}$ is called *factorial*, if any positive $a \in S$ is a product of primes.

Recall that *prime, semiprime and completely prime* are equivalent properties, as was shown in Chapter 1. Recall furthermore, that factorial is a cone property.

As a first consequence of prime we get, that prime elements commute. Observe: from $p \not\leq q \not\leq p$ it results $pq = qx = qpy$, that is $pq \leq qp \leq pq$. Hence, factorial implies commutative. Furthermore we get:

11. 4. 2 Proposition. *If $\mathfrak{S}$ is factorial and $\prod p_i^{e_i} = a = \prod q_j^{e_j}$ are irredundant products with pairwise incomparable factors p_i and pairwise incomparable factors q_j, then these products coincide up to permutation.*

PROOF. Recall that primes are completely prime. □

Now we are in the position to show:

11. 4. 3 Proposition. *Let $\mathfrak{S}$ be a positive d-monoid. Then the following are pairwise equivalent:*

- (i) *$\mathfrak{S}$ is factorial.*
- (ii) *The ideal semigroup of $\mathfrak{S}$ satisfies $A \cdot \bigcap B_i = \bigcap AB_i$ $(i \in I)$.*
- (iii) *The ideal semigroup of $\mathfrak{S}$ is complementary.*

PROOF. We symbolize ideals, generated by a or A, respectively, by (a) or (A), respectively.

$(i) \Longrightarrow (ii)$. First of all $\mathfrak{S}$ is complementary. To realize this, recall that $ax \geq b \iff (a \wedge b)x \geq b$ means that all $a * b$ with $a \leq b$ exist, since the irredundant prime factor products of the elements $a \in S$ are unique, whence the irredundant prime factor products of the complements in b are subproducts of their irredundant prime decomposition of b.

In particular, there are only finitely many complements in x.

Let now x belong to $\bigcap AB_i \ \ (i \in I)$. Then for any $a_i \in A$ we find some $b_i \in B_i$ with $a_i \cdot b_i = x$, and in addition we may assume $b_i = a_i * x$ and $a_i = x : (a_i * x)$. But there are only finitely many complements $a_i * x$. Consequently, according to 2.2.2 we get $x = \bigvee(x : (b_i * x)) \cdot \bigwedge(b_i * x)$ with $\bigvee(x : (b_i * x)) \in A$ and $\bigwedge(b_i * x) \in \bigcap B_i \ \ (i \in I)$. But this implies:

$$A \cdot \bigcap B_i \subseteq \bigcap AB_i \ \ (i \in I)$$

and thereby condition (ii).

$(ii) \Longrightarrow (iii)$. Again we show first that $\mathfrak{S}$ is complementary, if the condition – here (ii) – is satisfied. Let to this end $\{x_i \,|\, i \in I\}$ be the set of all x with $ax \geq b$. Then it holds $(a) \cdot \bigcap(x_i) = \bigcap(a \cdot x_i) = (b)$, whence some $y \in \bigcap(x_i)$ exists with $ay = b$ and $y \leq x_i \ \ (i \in I)$, that is an element y satisfying $y = a*b$, and dually we get some z with $z = b : a$.

Now we prove:

$$A \subseteq B \Longrightarrow B = A \cdot X = Y \cdot A \ \ (\exists\ X, Y)$$

for the set of ideals of $\mathfrak{S}$.

To this end we start from $A \subseteq (b)$. Then any $a_i \in A$ satisfies $(a_i)(c_i) = (b) \ \ (\exists c_i)$ and thereby $A \cdot \bigcap(c_i) \ \ (i \in I) = (b)$. This means by duality:

$$A \subseteq (b) \Longrightarrow (b) = A \cdot X = Y \cdot A \ \ (\exists\ X, Y).$$

Assume now $A \subseteq B$. Then for any $b \in B$ there exists some ideal X_b satisfying $(A \cap (b)) \cdot X_b = (b)$. This implies next $AX_b \subseteq B$ because

$$x \in X_b \Longrightarrow ax = (a : b)((a : b) * a)x \leq (a : b)b = a \vee b \in B\,.$$

Hence it results $A \cdot \bigvee X_b \ (b \in B) = \bigvee(A \cdot X_b) = B$ and its dual.

In particular $\mathfrak{S}$ is commutative as was shown in the preceding proof, and by distributivity we get:

$$A \cdot \bigcap X_i \ (A \cdot X_i \supseteq B) = A \cdot B$$

and thereby (iii).

$(iii) \Longrightarrow (ii)$. First we show that together with its ideal semigroup $\mathfrak{S}$ also $\mathfrak{S}$ itself is complementary:

To this end suppose $(a)*(b) = K$. Then K must be principal because $b \leq ak$ with $k \in K$ and $(k) \subseteq K$. Consequently $\mathfrak{S}$ is $*$-closed and $:$-closed .

Suppose now $K = A * \bigcap AB_i \;\; (i \in I)$. Then it holds $K \subseteq B_i \;\; (\forall\, i \in I)$ and thereby $K \subseteq \bigcap B_i$ which leads to $A \cdot K = \bigcap AB_i \subseteq A \cdot \bigcap B_i \;\; (i \in I)$. Thus we arrive at (ii) .

Finally we show:

$(ii) \Longrightarrow (i)$. As seen above, under condition (ii) $\mathfrak{S}$ is complementary . But this means $A \cdot \bigcap B_i = \bigcap AB_i \;\; (i \in I)$.

Let now $a_1 < a_2 < a_3 < \ldots$ be an ascending chain of *divisors* of a with $a_i = b_i * a$, that is also with $a_i = (a_i * a) * a \;\; (i \in I)$. Then we get $a = a_i(a_i * a) \;\; (\forall\, i \in I) \leadsto (a) = (a_1\,, a_2, \ldots) \cdot \bigcap (a_i * a) \;\; (i \in I)$. But it holds $(a_i * a) * a = a_i$, whence there must exist a final a_n , since otherwise $(a) \neq (a_1, a_2, \ldots) \cdot \bigcap (a_i * a) \;\; (i \in I)$ would follow, a contradiction. Hence the set $\{b_i * a\}$ must satisfy ACC.

But this provides DDC w. r. t. $\succeq$ where $a \succ b :\Longleftrightarrow \exists\, c : b = c * a$. Observe: because $d * (c * a) = dc * a \succ$ is transitive, and the reader easily checks that for any descending chain $a \succ a_1 \succ a_2 \ldots$ there exists a properly ascending chain of complements. Consequently $\mathfrak{S}$ is complementary with DCC for $\succ$. But this means that $\mathfrak{S}$ is factorial, since $a * b = 1 \vee a * b = b$ means *"b is prime"*. □

Finally we study some variations:

11. 4. 4 Corollary. *Let $\mathfrak{G}$ be an ℓ-group. Then the following are pairwise equivalent:*

- (i) *$\mathfrak{G}$ is factorial.*
- (ii) *Any bounded ideal of $\mathfrak{G}^+$ is principal.*
- (iii) *Any bounded filter of $\mathfrak{G}^+$ is principal.*
- (iv) *If A, B are ideals of $\mathfrak{G}^+$, then it holds:*
  $$A \subseteq B \implies B = A \cdot X = Y \cdot A \;\; (\exists\, X, Y)\,.$$
- (v) *If A, B are filters of $\mathfrak{G}^+$, then it holds:*
  $$A \supseteq B \implies B = A \cdot X = Y \cdot A \;\; (\exists\, X, Y)\,.$$

PROOF. $\mathfrak{G}^+$ is factorial iff it satisfies DCC or equivalently the ACC for bounded sets. This provides immediately $(i) \Longrightarrow (ii)$ & (iii) & (iv) & (v) .

Next it holds $(ii) \Longrightarrow (i)$. Consider a chain $a > a_1 > a_2 > \ldots$ and the ideal, generated by the elements $a_i * a$.

By analogy we get $(iii) \Longrightarrow (i)$.

So, it remains to verify that (iv) implies (ii) and that (v) implies (iii), which is now demonstrated by $(iv) \Longrightarrow (ii)$:

$A \subseteq (b)$ leads to some X satisfying $A \cdot X = (b)$, and thereby to a pair a, x satisfying $a \in A, x \in X$ and $ax = b$. This means further $sax = b$ for all $sa \in A$, whence by cancellation it results $s = 1$ and thereby $A = (a)$. $\square$

11. 4. 5 Corollary. *Let $\mathfrak{L}$ be a distributive lattice. Then the following are pairwise equivalent:*

- (i) *$\mathfrak{L}$ is factorial.*
- (ii) *The ideal lattice of $\mathfrak{L}$ is $\bigcap$-distributive.*
- (iii) *The ideal lattice of $\mathfrak{L}$ is complementary.*

Chapter 12

Ideal Extensions

Throughout this chapter $\mathfrak{S}$ is assumed to be positive

12.1 Cut Criteria

In this section we settle the problem, under which conditions a d-semigroup $\mathfrak{S}$ admits some $\bigwedge$-*complete extension*, recall that is some *complete extension* satisfying $x \cdot (\bigwedge a_i) \cdot y = \bigwedge (xa_iy) \ \ (i \in I)$, and dually, under which conditions some d-semigroup $\mathfrak{S}$ admits some $\bigvee$-*complete extension*. In this context the archimedean property proves to be necessary, of course, since any $\wedge$- and any $\bigvee$-complete d-semigroup, as well, is archimedean. But opposite to the classical case, the archimedean property is not strong enough in general, as is shown by $\mathfrak{P}_1^\circ$. Hence we have to look for properties, providing – together with the archimedean property – extensions of the required type. To this end – according to 2.4.2 – we may start from some positive d-monoid with zero element 0. This doesn't really weaken the results, but is more convenient.

In this context, the pair *pair* v-ideal, u-ideal will prove to be most fruitful, since these ideals respect the cancellation law, and clearly the v-ideal structure is an $\wedge$-complete extension iff $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \,|\, \mathfrak{b}$, and the u-ideal structure is a $\bigvee$-complete extension iff it satisfies $\mathcal{A} \subseteq \mathcal{B} \Longrightarrow \mathcal{A} \,|\, \mathcal{B}$. Here $|$ means $|_\ell$ & $|_r$. But, in fact, throughout most parts of this section we will be concerned with archimedean d-semigroups, and thereby with commutative ones.

It will turn out to be of some advantage, to notice the v-ideal, generated by A by $\underline{A}$ and the u-ideal, generated by A by $\overline{A}$. Furthermore – again – whenever A and $\mathfrak{a}$ or $\mathcal{A}$, respectively, are under consideration we tacitly suppose that A be a basis of $\mathfrak{a}$ or $\mathcal{A}$, respectively. Furthermore:

Let $\sum$ be a sup-d-semigroup of $\mathfrak{S}$ and suppose $\Lambda \subseteq \Sigma$. We define:

$$[\Lambda] := \{x \mid x \in S \ \&\ x \leq \Lambda\} \quad \text{and} \quad (\Lambda) := \{x \mid x \in S \ \&\ \Lambda \leq x\}\ .$$

Here $[\Lambda]$ may be empty, since $\mathfrak{S}$ has a zero element 0, and dually (Λ) may be empty since $\mathfrak{S}$ has an identity element 1.

12. 1. 1 Definition. Let $\sum$ be an extension of $\mathfrak{G}$. We call $\sum$ an extension of DEDEKIND type if any α satisfies

$$\alpha = \bigwedge(\alpha) = \bigvee[\alpha]. \tag{12.1}$$

12. 1. 2 Proposition. *A d-semigroup $\mathfrak{S}$ admits an $\wedge$-complete extension of* DEDEKIND *type iff $\mathfrak{V}$ satisfies:*

$$\textbf{(SS)} \qquad \mathfrak{a}^n \supseteq \mathfrak{b}\ \ (\forall : n \in \mathbf{N}) \implies \mathfrak{a} \circ \mathfrak{b} = \mathfrak{b} = \mathfrak{b} \circ \mathfrak{a}$$
$$\textbf{and} \qquad \mathfrak{a} \ = \ \bigcap(t)\ \ ((t) \supseteq \mathfrak{a})$$

PROOF. **(a)** Let $\sum$ be an $\bigwedge$-complete extension of DEDEKIND type w. r. t. $\mathfrak{S}$. Then $\sum$ is archimedean and commutative, and it results first for any v-ideal of $\mathfrak{S}$:

$$\underline{A} \ = \ (\bigwedge A)\ .$$

FOR, since $\sum$ is a cut extension w. r. t. $\mathfrak{S}$, it holds $\bigwedge A = \bigvee[A]$, whence it results:

$$\begin{aligned} c \in \underline{A} &\implies c \in ([A]) \\ &\implies c \in \left(\bigvee[A]\right) \\ &\implies c \in \left(\bigwedge A\right)\ , \end{aligned}$$

that is

$$\underline{A} \ \subseteq \ (\bigwedge A)\,,$$

and moreover $s, t \in S$ implies:

$$\begin{aligned} s \mid At &\implies s \mid \bigwedge(At) \\ &\implies s \mid (\bigwedge A) \cdot t\ , \end{aligned}$$

that is

$$\underline{A} \ \supseteq \ (\bigwedge A)\,,$$

whence we get altogether

$$\underline{A} \ = \ (\bigwedge A)\ .$$

Consequently, exactly the sets (α) of $\sum$ are v-ideals in $\mathfrak{S}$. We define ϕ : $\alpha \longmapsto (\alpha)$. Then it results:

$$\begin{aligned} s\,|\,(\alpha)(\beta) &\Longrightarrow s\,|\,\bigwedge(\alpha)(\beta) \\ &\Longrightarrow s\,|\,\bigwedge(\alpha)\bigwedge(\beta) \\ &\Longrightarrow s\,|\,\alpha\beta \\ &\Longrightarrow s\,|\,(\alpha\beta)\,. \end{aligned}$$

Hence $\sum$ is isomorphic with $\mathfrak{V}$, and hereby it follows condition **(SS)**.

(b) Let now inversely **(SS)** be satisfied. Then $\mathfrak{V}$ is commutative and b.a. it suffices to verify

$$(\mathbf{M}_v) \qquad \mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a}\,\Big|\,\mathfrak{b}$$

To this end suppose next $\mathfrak{b} = \underline{b} =: \mathsf{b}$ and $\mathfrak{a} = \underline{A}$ with $a \le b \ (\forall\, a \in A)$, and $\mathfrak{x} := \mathfrak{a} * \mathsf{b} = \underline{X}$ with $x \le b \ (\forall\, x \in X)$, and moreover $c \le AX$ and $d = b \vee c$. Then for all $a \in A$, $x \in X$ it results

$$\begin{array}{rcl} ax & \geq & d \ge b \\ & \rightsquigarrow & \\ x \in \mathsf{a} * \mathsf{d} & \& & a \in \mathsf{x} * \mathsf{d} \\ & \rightsquigarrow & \\ x \in \mathsf{b} * \mathsf{d} & \& & a \in \mathsf{b} * \mathsf{d}\,. \\ & \rightsquigarrow & \\ \mathsf{b} * \mathsf{d} & \supseteq & \mathsf{a}, \mathsf{x}. \end{array}$$

This implies furthermore for any $\mathsf{t} \supseteq \mathsf{b} * d \supseteq \mathsf{a}, \mathsf{x}$

$$\begin{array}{rcl} ax & \geq & b \\ & \Longrightarrow & \\ \mathsf{t} \circ (\mathsf{t} * \mathsf{a}) \circ \mathsf{t} \circ (\mathsf{t} * \mathsf{x}) & \subseteq & \mathsf{t} \circ (\mathsf{t} * \mathsf{d}) = \mathsf{d} \\ & \Longrightarrow & \end{array}$$

$$\mathsf{t} * \mathsf{d} \ = \ (\mathsf{t} * \mathsf{b}) \circ (\mathsf{b} * \mathsf{d})\,, \tag{12.4}$$

But, it holds:

$$\mathsf{t} * \mathsf{d} \ = \ (\mathsf{t} * \mathsf{b}) \circ (\mathsf{b} * \mathsf{d})\,, \tag{12.5}$$

which results as follows: By evidence we get

$$\mathsf{t} * \mathsf{d} \ \supseteq \ (\mathsf{t} * \mathsf{b}) \circ (\mathsf{b} * \mathsf{d})\,, \tag{12.6}$$

and *vice versa* $t \le b \le d$ implies $\mathsf{t} * \mathsf{d} \subseteq (\mathsf{t} * \mathsf{b}) \circ (\mathsf{b} * \mathsf{d})$, observe

$$tu = b \ \& \ bv = d \ \& \ y \in \mathsf{t} * \mathsf{d}$$

for any y' with $(y \wedge u)y' = y$ implies first of all $tuy' = t(u \vee y)$ and thereby furthermore

$$t(y \wedge u) = b \quad \& \quad b(y' \wedge v) = d\,.$$

So we get $y \in \mathsf{t} * \mathsf{d} \Longrightarrow y = y_1 \cdot y_2 \ (y_1 \in \mathsf{t} * \mathsf{b},\ y_2 \in \mathsf{b} * d)$, and thereby equation (12.6).

Now, by (12.4) and $\mathsf{t} \supseteq \mathsf{b} * \mathsf{d}$ we are in the position to show next:

$$\begin{array}{rcl} \mathsf{a} \circ (\mathsf{t} * \mathsf{x}) & \subseteq & (\mathsf{t} * \mathsf{b}) \circ (\mathsf{b} * \mathsf{d}) \\ & \subseteq & \mathsf{t} \circ (\mathsf{t} * \mathsf{b}) \\ & = & \mathsf{b}\,. \end{array}$$

Thus, each $x \in X$ satisfies $\mathsf{t} * \mathsf{x} \subseteq \mathfrak{x}$ which entails – recall $\mathsf{t} \supseteq \mathsf{b} * \mathsf{d} \supseteq \underline{X}$:

$$\begin{array}{rcl} \mathsf{t} \circ \mathfrak{x} & \supseteq & \underline{\mathsf{t} \circ (\mathsf{t} * \mathsf{x})} \ (x \in X) \\ & = & \mathfrak{x} \\ & \supseteq & \mathsf{t} \circ \mathfrak{x}\,, \\ & \rightsquigarrow & \\ \mathfrak{x} & = & \mathsf{t} \circ \mathfrak{x} \end{array}$$

But this implies $\mathsf{t}^n \circ \mathfrak{x} = \mathfrak{x} \rightsquigarrow t^n \leq b \ (\forall\, n \in \mathbf{N})$, meaning $b \cdot t = b$. Let now g divide $\mathsf{b} = \mathsf{b} \circ (\mathsf{b} * \mathsf{d}) = \mathsf{d}$. Then $g = (b \wedge g) \cdot g'$ with $g' \leq b * d$, recall (2.19). So, by (**SS**) we get first $\mathsf{b} = \mathsf{b} \circ (\mathsf{b} * \mathsf{d}) = \mathsf{d}$ and thereby furthermore $b \geq c$, which leads to $\mathsf{b} = \mathfrak{a} \circ \mathfrak{x}$.

Let's consider now the general case. Then for each $b \in \mathfrak{b}$ we get an $\mathfrak{x}_b$ satisfying $\mathfrak{a} \cdot \mathfrak{x}_b = \mathsf{b}$ which entails $\mathfrak{a} \cdot \sum\limits_{b \in \mathfrak{b}} \mathfrak{x}_b = \mathfrak{b}$. □

Dually w. r. t. 12.1.2 we get:

12. 1. 3 Proposition. *A d-semigroup $\mathfrak{S}$ admits a $\bigvee$-complete cut extension iff $\mathfrak{S}$ is archimedean and satisfies in addition:*

(**SV**) $$\overline{A} = [\,(A)\,]$$

and in this case any $\bigvee$-complete cut extension is isomorphic with the semigroup of u-ideals.

PROOF. First of all: The isomorphism, claimed above, results by the mapping $\phi : \alpha \longmapsto [\,\alpha\,]$ along the lines below 12.1.2.

Now we turn to

(a) Condition **(SV)** is necessary, consult the development below (a) in the proof of 12.1.2.

(b) Condition **(SV)** is sufficient:

By **(SV)** any u-ideal $\overline{A}$ satisfies $\overline{A} = [\,(A)\,]$. Next, for any pair of u-ideals $\mathcal{A}, \mathcal{B}$ it holds

$$(\mathbf{M}_u) \qquad \mathcal{A} \subseteq \mathcal{B} \Longrightarrow \mathcal{A} \,|\, \mathcal{B}\,.$$

In the special case $A \leq \mathsf{b}$ with $X := \{x \,|\, Ax \leq \mathsf{b}\}$ it holds $c \geq Ax \Longleftrightarrow c \wedge b = d \geq Ax$. So $ds = b$ implies:

$$\begin{aligned} AX \subseteq \mathsf{b} \;&\Longrightarrow\; AX \subseteq \mathsf{d} \\ &\Longrightarrow\; AX \cdot s \subseteq \mathsf{d}\,, \end{aligned}$$

whence it results $Xs^n \subseteq \mathsf{d}$ implying $s^n \leq d \;\; (\forall\, n \in \mathbf{N})$. This leads further to $d = ds = b$ and thus to $\mathsf{b} = [\,(b)\,] = [\,(AX)\,] = \overline{AX}$, whence in case of $A = \overline{A}$ we get $\overline{A} \cdot \overline{X} = \overline{b}$.

Suppose now $\mathcal{A} \subseteq \mathcal{B}$, $b \in \mathcal{B}$ and $\mathcal{A}_b = \{b \wedge a \,|\, a \in \mathcal{A}\}$. Then, for some suitable $\mathcal{X}_b$, we get the relations $\mathsf{b} = \mathcal{A}_b \circ \mathcal{X}_b \subseteq \mathcal{A} \circ \mathcal{X}_b$ and $\mathcal{A} \circ \mathcal{X}_b \subseteq \mathcal{B}$, the first by the development above, the latter because of the implication $x \in \mathcal{X}_b \Longrightarrow ax = a''(a \wedge b)x \leq a''b = a \vee b$. So we get $\mathcal{B} = \mathcal{A} \circ \mathcal{X}$ with $\mathcal{X} = \sum\limits_{b \in \mathcal{B}} \overline{\mathcal{X}}_b$. □

Proposition 12.1.2 and proposition 12.1.3 provide each a base for characterizing d-semigroups with $\bigwedge$- and $\bigvee$-complete cut extension. This is done w. r. t. 12.1.2.

12. 1. 4 Proposition. *$\mathfrak{S}$ admits an $\bigwedge$-&$\bigvee$-complete cut extension iff $\mathfrak{S}$ satisfies axiom* **(SS)** *and in addition $\mathfrak{V}$ satisfies:*

$$\mathsf{a} \circ \bigcap \mathsf{b}_i \;=\; \bigcap (\mathsf{a} \circ \mathsf{b}_i) \quad (i \in I)\,.$$

PROOF. It is to verify:

$$\mathfrak{a} \circ \bigcap \mathfrak{b}_i \;=\; \bigcap (\mathfrak{a} \circ \mathfrak{b}_i) \quad (b_i \in I)\,.$$

This is valid for principal ideals by assumption. Consider now $\mathfrak{a} = \underline{A}$. Then for each $a \in A$ there exists some $\mathfrak{x}_a$ with $\mathsf{a} = \mathfrak{a} \circ \mathfrak{x}_a$, and this implies:

$$\begin{array}{rrcl} & \mathfrak{a} \circ \bigcap \mathsf{b}_i & \supseteq & \mathfrak{x}_a \circ \mathfrak{a} \circ \bigcap \mathsf{b}_i \\ & & = & \mathsf{a} \circ \bigcap \mathsf{b}_i \\ & & = & \bigcap(\mathsf{a} \circ \mathsf{b}_i) \\ & & = & \bigcap(\mathfrak{x}_a \circ \mathfrak{a} \circ \mathsf{b}_i) \\ & & \supseteq & \mathfrak{x}_a \circ \bigcap(\mathfrak{a} \circ \mathsf{b}_i) \\ \rightsquigarrow & \mathfrak{a} \circ \bigcap \mathsf{b}_i & \supseteq & \sum\limits_{a \in \mathfrak{a}} \left(\mathfrak{x}_a \circ \bigcap \mathfrak{a} \circ \mathsf{b}_i\right) \\ & & = & (\sum\limits_{a \in \mathfrak{a}} \mathfrak{x}_a) \circ \bigcap(\mathfrak{a} \circ \mathsf{b}_i) \\ & & = & \bigcap(\mathfrak{a} \circ \mathsf{b}_i)\,, \end{array}$$

the final line according to $(\sum\limits_{a \in \mathfrak{a}} \mathfrak{x}_a) \circ \mathfrak{a} = \mathfrak{a}$ and $\mathfrak{a} \supseteq \bigcap(\mathfrak{a} \circ \mathsf{b}_i)$.

Consequently, the required condition is valid for the special case where every $\mathfrak{b}_i$ is principal.

Start now from arbitrary v-ideals $\mathfrak{b}_i$. Then – according to 12.1.2 – any $\mathfrak{b}_i$ is the intersection of principal ideals b_{ik} $(i \in I, k \in K)$, and this implies, see above,

$$\begin{array}{rcl} \mathfrak{a} \circ \bigcap \mathfrak{b}_i & = & \mathfrak{a} \circ \bigcap(\bigcap \mathsf{b}_{ik}) \\ & = & \mathfrak{a} \circ \bigcap \mathsf{b}_{ik} \\ & = & \bigcap(\mathfrak{a} \circ \mathsf{b}_{ik}) \\ & \supseteq & \bigcap(\mathfrak{a} \circ \mathfrak{b}_i)\,. \end{array}$$

□

The question arises, when the semigroup of principal ideals of some arbitrary monoid admits a normal complete d-semigroup extension. This is equivalent to the question, when the semigroup of v-ideals satisfies

(M) $$\mathfrak{a} \supseteq \mathfrak{b} \implies \mathfrak{a} \,\big|\, \mathfrak{b}\,.$$

By considering some *zero-monoid* $(ab = 0)$ we see immediately that the archimedean property for v-ideals in general is not sufficient for the existence of an $\wedge$-complete extension. However in the later chapter on real d-semigroups we shall see that in the positive case the condition

(CE) $$A^n \supseteq \mathsf{b} \;\; (\forall n \in \mathbf{N}) \Longrightarrow \mathfrak{a} \cdot \mathsf{b} = \mathsf{b} = \mathsf{b} \cdot \mathfrak{a}$$

where A is assumed to be a filter and $\mathfrak{a}$ is assumed to be the A-generated v-ideal, guarantees a cube-extension. However we can show:

12. 1. 5 Proposition. *A positive d-monoid $\mathfrak{S}$ admits an $\wedge$-normal extension $\sum$ that is an $\wedge$-complete extension, in which any α is* infimum *of some $A \supseteq S$, iff the semigroup $\mathfrak{V}$ of v-ideals satisfies:*

$$\textbf{(A)} \qquad \mathfrak{a}^n \supseteq \mathfrak{b} \ \ (\forall\, n \in \mathbf{N}) \implies \mathfrak{a} \circ \mathfrak{b} = \mathfrak{b} = \mathfrak{b} \circ \mathfrak{a}$$

$$\textbf{(C)} \qquad \mathfrak{a} \supseteq \mathfrak{b} \supseteq \mathfrak{a} * \mathsf{b} \ \ (\forall b \in \mathfrak{b}) \implies \mathfrak{a}^n \supseteq \mathfrak{b} \ \ (\forall\, n \in \mathbf{N})\,.$$

PROOF. **(a)** Let $\sum$ be an $\wedge$-normal extension w. r. t. $\mathfrak{S}$. Then the mapping $h : \bigwedge A \longmapsto \underline{A}$ is a function from $\sum$ onto $\mathfrak{V}$, since $\bigwedge A = \bigwedge B$ implies $s \,|\, uAv \iff s \,|\, uBv$, that is $\underline{A} = \underline{B}$. Furthermore h is even a homomorphism. Hence v-ideals satisfy $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \,|\, \mathfrak{b}$, whence $\mathfrak{V}$ is $\wedge$-complete. This proves necessity by the implication:

$$\begin{aligned} \mathfrak{a} \supseteq \mathfrak{b} \supseteq \mathfrak{a} * \mathsf{b} \ \ (\forall b \in \mathfrak{b}) &\implies \mathfrak{a} \circ \mathfrak{b} \supseteq \mathfrak{a} \circ \textstyle\sum(\mathfrak{a} * \mathsf{b}) = \mathfrak{b} \\ &\implies \mathfrak{a} \circ \mathfrak{b} = \mathfrak{b} \\ &\implies \mathfrak{a}^n \supseteq \mathfrak{b} \ \ (\forall n \in \mathbf{N}). \end{aligned}$$

(b) First of all, condition **(A)** implies commutativity.

Suppose now $\mathfrak{a} = \underline{A} \ni b$, $\forall a \in A : a \leq b$, $\mathsf{b} = \underline{b}$, $\mathfrak{x} = \underline{X} = \mathfrak{a} * \mathsf{b}$ and choose some $a \in A$, $x \in X$. Then it results

$$au = b \ \ (\exists u \in S) \ \ \& \ \ ax \geq b \ \ \& \ \ x = us \ \ (\exists s \in S)$$

and thereby $$au(a \wedge s) \in \mathfrak{a} \circ (\mathfrak{a} * \mathsf{b}) =: \mathfrak{c}\,,$$

that is in particular $\underline{a \wedge s} \subseteq \mathsf{b} * \mathfrak{c}$. We next put $(\underline{a \wedge s}) * (\underline{a \wedge s})\,\mathsf{u} =: \mathfrak{d}$. This entails

$$\mathsf{a}\mathfrak{d} = \mathsf{b} \quad \text{ and } \quad \mathfrak{d} = (\underline{a \wedge s}) * (\underline{a \wedge s})\,\mathsf{u} \supseteq (\underline{a \wedge s}) * \mathsf{x} \supseteq (\mathsf{b} * \mathfrak{c}) * \mathsf{x}\,,$$

whence it follows

$$\mathfrak{a} \circ ((\mathsf{b} * \mathfrak{c}) * \mathsf{x}) \subseteq \mathsf{b} \rightsquigarrow \mathsf{b} * \mathfrak{c} \supseteq \mathfrak{a} * \mathfrak{c} = \mathfrak{a} * \mathsf{b} = \mathfrak{x} \supseteq (\mathsf{b} * \mathfrak{c}) * \mathsf{x} \quad (\forall\, x \in \mathfrak{x})\,,$$

that is

$$(\mathsf{b} * \mathfrak{c}) \supseteq \mathfrak{x} \supseteq (\mathsf{b} * \mathfrak{c}) * \mathsf{x} \quad (\forall\, x \in \mathfrak{x}) \Longrightarrow (\mathsf{b} * \mathfrak{c})^n \supseteq \mathfrak{x} \Longrightarrow (\mathsf{b} * \mathfrak{c})^n \supseteq \mathsf{b}$$

hence $$\mathfrak{a} \circ (\mathfrak{a} * \mathsf{b}) =: \mathfrak{c} = \mathsf{b} \circ (\mathsf{b} * \mathfrak{c}) = \mathsf{b}.$$

Thus the proof is complete, recall $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cdot \sum \mathsf{b}$ $(b \in \mathfrak{b})$. □

As another characterization of $\wedge$-*normal* monoids, we present:

12. 1. 6 Proposition. *A positive d-monoid* $\mathfrak{S}$ *admits an* $\wedge$*-normal extension* $\sum$ *iff the semigroup* $\mathfrak{V}$ *of v-ideals satisfies:*

$$\textbf{(A)} \qquad \mathfrak{a}^n \supseteq \mathfrak{b} \ \ (\forall\, n \in \mathbf{N}) \implies \mathfrak{a} \circ \mathfrak{b} = \mathfrak{b} = \mathfrak{b} \circ \mathfrak{a}$$

$$\textbf{(F)} \qquad \mathsf{a} * \mathsf{b} \supseteq \mathfrak{c} \implies \mathsf{a} * \mathsf{b} \,\Big|\, \mathfrak{c}\,.$$

PROOF. All we have to show is $\mathfrak{a} \supseteq \mathsf{b} \Longrightarrow \mathfrak{a} \,|\, \mathsf{b}$. So, assume $\mathfrak{a}\mathfrak{x} \subseteq \mathfrak{b} = \mathsf{b}$ with $\mathfrak{x} = \mathfrak{a} * \mathsf{b}$, and $s \,|\, \mathfrak{a}\mathfrak{x}$. Then it holds:

$$(\star) \qquad \mathfrak{y} := \mathsf{b} * \mathsf{s} \supseteq \mathfrak{x} * \mathsf{s} \supseteq \mathfrak{x} * \mathfrak{a}\mathfrak{x} \supseteq \mathfrak{a}\,,$$

that is $\quad \mathrm{E}\,(1): \quad \mathfrak{y}^1 \,|\, \mathfrak{a}$ and $\mathfrak{y}^1 \,|\, \mathsf{b}$.

Suppose now $\quad \mathrm{E}\,(n): \quad \mathfrak{y}^n \,|\, \mathfrak{a}$ and $\mathfrak{y}^n \,|\, \mathsf{b}$.

Then $\quad \mathfrak{a}_1 := \mathfrak{y}^n * \mathfrak{a}$ and $\mathfrak{b}_1 := \mathfrak{y}^n * \mathsf{b}$

leads to

$$\begin{aligned} \mathfrak{a}_1 * \mathfrak{b}_1 &= (\mathfrak{y}^n * \mathfrak{a}) * (\mathfrak{y}^n * \mathsf{b}) \\ &= \mathfrak{a} * \mathsf{b} = \mathfrak{x}\,. \end{aligned}$$

Hence we get

$$\mathfrak{b}_1 \supseteq \mathfrak{a}_1 \circ \mathfrak{x}\,.$$

So, defining

$$\mathfrak{s}_1 := \mathfrak{y}^n * \mathsf{s}\,,$$

it results

$$\begin{aligned} \mathfrak{s}_1 &\supseteq \mathfrak{y}^n * \mathfrak{a} \circ \mathfrak{x} \\ &\supseteq (\mathfrak{y}^n * \mathfrak{a}) \circ \mathfrak{x} \\ &= \mathfrak{a}_1 \circ \mathfrak{x} \end{aligned}$$

and it holds

$$\begin{aligned} \mathfrak{b}_1 * \mathfrak{s}_1 &= (\mathfrak{y}^n * \mathsf{b}) * (\mathfrak{y}^n * \mathsf{s}) \\ &= \mathsf{b} * \mathsf{s} = \mathfrak{y}\,. \end{aligned}$$

Thus, by $(\star)$, we get: $\quad \mathfrak{y} \,|\, \mathfrak{y}^n * \mathfrak{a} \rightsquigarrow \mathfrak{y} \,|\, \mathfrak{y}^n * \mathsf{b}$

implying $\quad \mathrm{E}\,(n+1): \quad \mathfrak{y}^{n+1} | \mathfrak{a}$ & $\mathfrak{y}^{n+1} \,|\, \mathsf{b}$.

Summarizing: **(A)** implies $\mathsf{b} \circ \mathfrak{y} = \mathsf{b}$, and thereby $\mathsf{b} \circ \mathfrak{y} = \mathsf{b} \cap \mathsf{s} = \mathsf{b}$, which means $\mathsf{s} \supseteq \mathsf{b}$.

It remains to show $\mathfrak{a} \circ \mathfrak{x} \supseteq \mathsf{b}$. To this end let $s \,|\, \mathfrak{a}\mathfrak{x}\, t$ be satisfied. Then it holds $\mathsf{t} * \mathsf{s} \supseteq \mathfrak{a} \circ \mathfrak{x}$ and along the lines above we get – because $\mathsf{b} * (\mathsf{t} * \mathsf{s}) = \mathsf{bt} * \mathsf{s}$ – that $\mathsf{t} * \mathsf{s} \supseteq \mathsf{b}$ and thereby $\mathsf{s} \supseteq \mathsf{t}(\mathsf{t} * \mathsf{s}) \supseteq \mathsf{b} \circ \mathsf{t}$ is satisfied, i. e. $s \,|\, \mathsf{b}t$. Thus it results $\mathfrak{a} \circ \mathfrak{x} = \mathsf{b}$.

Hence: **(A)** & **(F)** is also sufficient. □

12. 1. 7 Corollary. *If each* $\mathsf{a} * \mathsf{b}$ *is principal, that is if the underlying monoid is complementary, then condition (M) is equivalent to the archimedean property for principal ideals.*

Furthermore it should be given the hint, that the first part of the preceding proof "works" in any case where $b * s$ is replaced with some divisor $\mathfrak{d}$, satisfying $\mathsf{b} * (\mathsf{b} \circ \mathfrak{d}) = \mathfrak{d}$.

12.2 Sufficient Conditions

Apart from the characteristic conditions in the remainder we will present some sufficient conditions, necessary (in addition) in various classical structures, like boolean lattices and ℓ-group cones.

12. 2. 1 Proposition. *Let* $\mathfrak{S}$ *satisfy the equation* $[\,A\,][\,B\,] = [\,AB\,]$*, then* $\mathfrak{S}$ *admits an* $\bigwedge$*-complete cut extension .*

PROOF. Suppose $A \neq \emptyset$ and $X = \{x \,|\, Ax \geq b\}$. Then it follows:

$$b \in [\,A\,][\,X\,] \implies b = b_A b_X \ \ (\exists\, b_A \leq A\,,\, b_X \leq X)\,,$$

whence among all x with $Ax \geq b$ there exists a (uniquely determined) minimum $A * b$ and dually, among all y with $yA \geq b$ a there exists a (uniquely determined) minimum $b : A$. Hence $[\,A\,] = [\,B\,] \implies \underline{A} = \underline{B}$, since by $[\,A\,] = [\,B\,]$ it results:

$$\begin{aligned} s \,|\, uAv \iff (s:v) \,|\, uA \ &\iff \ u * (s:v) \,|\, A \\ &\iff \ (u * s) : v \,|\, B \iff s \,|\, uBv\,. \end{aligned}$$

Consequently the v-ideal structure $\mathfrak{V}$ is a cut extension w. r. t. $\mathfrak{S}$.

Let now $\mathfrak{a} \supseteq \mathsf{b}$, $\mathfrak{a} * \mathsf{b} = \mathsf{u}$ and $b \leq d \leq \mathfrak{a}\mathsf{u}$ be given. Then it follows $d : u \leq A$ and thereby $d : u \leq b$, that is $b = (d : u)y$ with some suitable y. But this implies $Ay \geq b$, that is $y \geq u$ and thereby $b = (d : u)y \geq (d : u)u = d$. Hence the divisors of $\mathfrak{a}\mathsf{u}$ also divide b. So we get $\mathfrak{a}\mathsf{u} = \mathsf{b}$.

The rest follows by v-ideal arithmetic. □

Dually w.r.t. 12.2.1 we get:

12. 2. 2 Proposition. *Let $\mathfrak{S}$ satisfy $(A)(B) = (AB)$. Then $\mathfrak{S}$ admits a $\bigvee$-complete cut extension .*

PROOF. Let $\mathcal{A} \subseteq \mathsf{b}$ and $\mathcal{X} = \mathcal{A} * \mathsf{b}$ be given. Then it holds $b \geq \mathcal{A}\mathcal{X}$, that is $b = b_{\mathcal{A}} b_{\mathcal{X}}$ with $b_{\mathcal{A}} \geq \mathcal{A}$ and $b_{\mathcal{X}} \geq \mathcal{X}$. Hence $b_{\mathcal{X}}$ is maximum of $\mathcal{X}$. This implies first

$$\begin{array}{rlrcl} c \geq \mathcal{A}\mathcal{X} & \Longrightarrow & d & = & b \wedge c \geq \mathcal{A}\mathcal{X} \\ & \Longrightarrow & d & = & d_{\mathcal{A}} \cdot d_{\mathcal{X}} \\ & \text{where} & & & d_{\mathcal{A}} \geq \mathcal{A} \ \& \ d_{\mathcal{X}} \geq \mathcal{X} \ , \end{array}$$

and thereby next

$$\begin{array}{rlrcl} b = d_{\mathcal{A}} d_{\mathcal{X}} s & \Longrightarrow & d_{\mathcal{X}} s & \in & \mathcal{X} \\ & \Longrightarrow & d_{\mathcal{X}} s & \leq & d_{\mathcal{X}} \\ & \Longrightarrow & d & = & d_{\mathcal{A}} d_{\mathcal{X}} = d_{\mathcal{A}} d_{\mathcal{X}} s = b \, . \end{array}$$

So it is proven $(\mathcal{A}\mathcal{X}) = (\mathsf{b})$, and we are in the position to verify $\overline{A} = [\,(A)\,]$, in order to prove 12.2.1.

Thus we may continue along the proof lines of 12.1.3 – recall, in the final part of that proof commutativity was not applied. □

Proposition 12.2.1 implies $[\,A\,][\,B\,] = [\,AB\,]$, on the one hand, and, of course, on the other hand also $[\,a\,][\,B\,] = [\,aB\,]$. But the latter condition is equivalent with existing complements $a * b$, which has been proven implicitly below proposition 12.2.1.

In analogy $(a)(B) = (aB)$ holds iff any pair $a \leq b$ defines a maximum x w.r.t. $ax \leq b$.

So, d-semigroups with $[\,a\,][\,B\,] = [\,aB\,]$, according to 2.8.2 are complementary – or v-complementary.

Dually d-semigroups with $(a)(B) = (aB)$ are u-complementary.

12. 2. 3 Proposition. *Let $\mathfrak{S}$ be archimedean and v-complementary. Then $\mathfrak{S}$ admits an $\bigwedge$-complete cut extension.*

PROOF. We get $\underline{A} = ([\,A\,])$ along the lines below 12.2.1, and furthermore in the proof of 12.1.3 the element t may be thought of as $b * d$. □

12. 2. 4 Proposition. *Let $\mathfrak{S}$ be archimedean and u-complementary. Then $\mathfrak{S}$ admits a $\bigvee$-complete cut extension.*

PROOF. Along the proof lines of 12.2.2 we get $\overline{A} = [\,(A)\,]$, and, because of the archimedean property we may apply $\mathcal{A} \subseteq \mathsf{b} \implies \mathcal{A} \,|\, \mathsf{b}$ of the proof below proposition 12.1.3. □

Proposition 12.2.3 is not new, of course, since this result has already been presented in chapter on archimedean d-semigroups.

The proof of 12.2.4 verifies – by applying 12.1.3 – that archimedean d-semigroups always satisfy $\mathsf{b} \supseteq \mathcal{A} \implies \mathsf{b} = \mathcal{A} \circ (\mathcal{A} * \mathsf{b})$. This implies – as a strengthening of proposition 12.2.4.

12. 2. 5 Proposition. *Let $\mathfrak{S}$ be archimedean and let $\mathfrak{S}$ satisfy moreover the implication $s = \sup(a_i) \implies s \cdot t = \sup(a_i) \cdot t$. Then $\mathfrak{S}$ admits a $\bigvee$-complete extension.*

From this it results further, in addition to the results on the 1-extension $\mathfrak{S}^1$ of $\bigvee$-complete d-semigroups:

12. 2. 6 Corollary. *Let $\mathfrak{S}$ be $\bigvee$-complete. Then also the semigroup of all u-ideals of $\mathfrak{S}^1$ is $\bigvee$-complete.*

PROOF. Obviously our distributivity requirement is valid for all cancellable elements t, and if t fails to be cancellable then for any unit e of t we calculate $\sup(a_i t) = \sup((a_i e)t) = t \geq t \sup(a_i)$. □

Chapter 13

Polars

13.1 Prime c-ideals

Throughout this chapter let $\mathfrak{S}$ be a right normal d-monoid, although many propositions do not really depend on right normality, recall, that according to 5.4.6 any d-semigroup is embedded in a normal d-semigroup. In order to emphasize, that not only $R(a, b, a', b')$, but also $a' \perp b'$ is satisfied, we denote this situation by $R(a, b, a^\circ, b^\circ)$.

The classical (right-)normal d-monoid is the ideal semigroup of *arithmetical* commutative rings with identity 1, that is the ideal semigroup of commutative rings with:

$$\langle a_1, \ldots, a_n \rangle \supseteq \langle b \rangle \Longrightarrow \langle a_1, \ldots, a_n \rangle \Big| \langle b \rangle \,,$$

and thereby in particular any ideal semigroup of some *residue class ring* $\mathbf{Z}_n$, observe, that here any ideal is even *principal.*

Further abstract examples are the boolean algebra, and the ℓ-group, and thereby of course the ℓ-group cone, in particular the d-semigroup of $\mathbf{N}$, considered under multiplication and GCD. This latter example, above all, provides a most helpful background. The reader should check the propositions of this chapter and the next one in any case with $\mathbf{N}$ as background.

In this chapter we investigate the special role of c-ideals. Since these ideals are operationally closed, we may consider them also as *submonoids* in the sense of sub-d-monoids. So we are faced on the one hand with c-ideals A, that is special subsets, and on the other hand with c-monoids $\mathfrak{A}$ of $\mathfrak{S}$, with c-ideal A as carrier.

13. 1. 1 Definition. Let C be a c-ideal and $A \subseteq S$. Then by the *polar* of A in C we mean $A^{\perp C} := \{x \,\big|\, |\,a\,| \wedge |\,x\,| \in C \ (\forall a \in A)\}$, briefly called the *$C$-polar,* of A.

In particular, if $C = \{1\}$ we call $A^{\perp\{1\}}$ briefly the *polar* of A, symbolized by $A^{\perp}$. In order to simplify the notation we denote $(A^{\perp})^{\perp}$ by $A^{\perp\perp}$ and call $A^{\perp\perp}$ a *bipolar*.

13. 1. 2 Proposition. *Let $\mathfrak{S}$ be a right normal d-monoid and P a c-ideal of $\mathfrak{S}$. Then the following are pairwise equivalent:*

(i) *P is prime .*

(ii) $|\,a\,| \wedge |\,b\,| \in P \Longrightarrow |\,a\,| \in P \vee |\,b\,| \in P$.

(iii) $a^+ \wedge b^+ \in P \Longrightarrow a^+ \in P \vee b^+ \in P$.

(iv) $a \wedge b = 1 \Longrightarrow a \in P \vee b \in P$.

(v) *$\mathfrak{S}/P$ is linearly ordered w. r. t. $\supseteq$.*

(vi) $\{A \,|\, P \subseteq A \in C(\mathfrak{S})\}$ *is linearly ordered .*

PROOF. $(i) \Longrightarrow (ii)$, because

$$\begin{aligned} |\,a\,| \wedge |\,b\,| \in P &\Longrightarrow |\,a\,|^{\perp P} \cap |\,b\,|^{\perp P} \subseteq P \\ &\Longrightarrow |\,a\,|^{\perp P} \subseteq P \vee |\,b\,|^{\perp P} \subseteq P \\ &\Longrightarrow |\,a\,| \in P \vee |\,b\,| \in P\,. \end{aligned}$$

$(ii) \Longrightarrow (iii) \Longrightarrow (iv) \Longrightarrow (v)$ results nearly by evidence.

$(v) \Longrightarrow (vi)$. Let A and B be c-ideals, and let $a \in A$, $b \in B$ be arbitrarily chosen. Then it follows $a \wedge b \in A \cap B$ and $R(a, b, a^\circ, b^\circ)$ $(a^\circ \in A \ \&\ b^\circ \in B)$.

Let now A, B be incomparable with $a^\circ \in A \backslash B$ and $b^\circ \in B \backslash A$. Then we get $a^\circ \leq b^\circ e$ for some $e \in P$ or $b^\circ \leq a^\circ f$ for some $f \in P$, a contradiction!

$(vi) \Longrightarrow (i)$ finally, follows nearly immediately. □

Next we will characterize prime c-ideals as special intersections of regular ideals. First of all

13. 1. 3 Proposition. *Let $\mathfrak{S}$ be a right normal d-monoid and P a prime c-ideal of $\mathfrak{S}$. Then the set of all sup-c-ideals of P forms a $\supseteq$-chain.*

PROOF. Let A and B be c-ideals with $A, B \supseteq P$. Then (w. l. o. g.) $A \not\subseteq B$ would imply the existence of some $a \in A \backslash B$. We consider the set of all

$a \wedge b \ \ (b \in B)$. Then, by $a \notin B$, in case of $R(a, b, a^\circ, b^\circ)$ it results first $b^\circ \in P$ and thereby next $(a \wedge b)b^\circ \in A \cap B$. So it must hold $B \subseteq A$. □

13. 1. 4 Corollary. *A c-ideal of a right normal d-monoid is prime if it is the intersection of a linearly ordered set of regular c-ideals.*

13. 1. 5 Definition. Let R be a regular c-ideal and let c be an element in the sense of 4.2.11. Then R is called a *value* of c, and the set of all values is denoted by $\mathrm{val}\,(c)$.

Since c-ideals C satisfy $a \in C \iff |a| \in C$ it holds $\mathrm{val}\,(c) = \mathrm{val}\,(|\,c\,|)$, and we get furthermore:

$$\mathrm{val}\,(a^+) \cup \mathrm{val}\,(a^-) = \mathrm{val}\,(|\,a\,|) \text{ and } \mathrm{val}\,(c^+) \cap \mathrm{val}\,(c^-) = \emptyset\,. \tag{13.1}$$

PROOF. By evidence, the left side of the first equation is contained in the right side.

Furthermore it holds $\mathrm{val}\,(a^-) = \mathrm{val}\,(a^*)$ and $a^+ \perp a^*$. Hence any value of $|\,a\,|$ contains one of the elements a^+, a^* and is thereby a value of the other one. So, also the right side of the first equation is contained in the left one.

Moreover, no M can be value of both, c^+ and c^*, since $c^+ \wedge c^* = 1$ leads to $c^+ \in M$ or $c^* \in M$. □

In addition it turned out that any value is value even of a positive element.

13. 1. 6 The projection Theorem. *Let $\mathfrak{S}$ be a d-monoid and let C be a c-ideal. If then M is a value of $c \in C$ in $\mathfrak{S}$, then $M \cap C$ is a value of c in C and any value of $c \in C$ arises this way. Thus $R \longmapsto R \cap C$ provides a surjective function sending the regular c-ideals of $\mathfrak{S}$ to the regular c-ideals of $\mathfrak{C}$. Moreover, the restriction of this function to regular c-ideals of $\mathfrak{S}$, not containing C, is even a bijection.*

PROOF. Let M be a value of $c \in C^+$ and let d belong to $C^+ \backslash M$. Then it follows:

$$\begin{aligned} & c \leq dm_1 \cdot dm_2 \cdot \ \ldots \ \cdot dm_n \ \ (m_i \in M^+) \\ \rightsquigarrow \ \ & c \leq (c \wedge d)(c \wedge m_1) \cdot (c \wedge d)(c \wedge m_2) \cdot \ldots \cdot (c \wedge d)(c \wedge m_n) \end{aligned}$$

and thereby $c \in ((C \cap M), d)^c$. So $M \cap C$ is a value in C of d.

Let now D be a value of $c \in C$ in C. Then D admits an extension to some value M of c in $\mathfrak{S}$, and this value must satisfy $D = M \cap C$.

Hence, the defined mapping is surjective.

Finally, let A, B be two different regular c-ideals of $\mathfrak{S}$, not containing C. Then $A \cap C$ and $B \cap C$ must be different. For, assume $A \cap C = B \cap C$, and suppose that A is a value of a, B a value of b and that d belongs to $C \backslash (C \cap A \cap B)$. Then $A \cap C = B \cap C$ would be a value of $c = a \wedge b \wedge d$ in $\mathfrak{C}$, leading to the contradiction:

$$c \notin C \cap A \cap B \ \& \ c \in C \cap (A \vee B) = (C \cap A) \vee (C \cap B) = C \cap A \cap B. \qquad \square$$

13.2 Polars

First of all, recall: $a, b \in S$ are called orthogonal if $|\,a\,| \wedge |\,b\,| = 1$. So a and b are orthogonal iff $|\,a\,|$ and b or a and $|\,b\,|$ or $|\,a\,|$ and $|\,b\,|$ are orthogonal.

13. 2. 1 Proposition. *Two elements $a \neq 1 \neq b$ are orthogonal iff their values are incomparable.*

PROOF. M is a value of a iff M is a value of $|\,a\,|$.

Suppose now that $|\,a\,| \not\perp |\,b\,|$. Then each value of $|\,a\,| \wedge |\,b\,|$ admits an extension to a value A of $|\,a\,|$ and to a value B of $|\,b\,|$. But these are comparable, according to 13.1.3.

Conversely, in case of $|\,a\,| \perp |\,b\,|$ there cannot exist a pair A, B of comparable elements of $\mathrm{val}\,(a)$ and $\mathrm{val}\,(b)$, respectively, since from $A \subseteq B$, for instance, would follow $|\,a\,| \notin A \ \& \ |\,b\,| \notin A$, in spite of $|\,a\,| \wedge |\,b\,| = 1$. $\square$

Now we turn to polars. By evidence we get:

$$A \supseteq B \implies B^{\perp} \supseteq A^{\perp}. \tag{13.2}$$

Moreover, by definition, any homomorphism h of $(S, \wedge)$ satisfies the inclusion $h(A^{\perp}) \subseteq h(A)^{\perp}$.

$$A \subseteq A^{\perp\perp} \ \text{ and } \ A^{\perp} = A^{\perp\perp\perp}. \tag{13.3}$$

PROOF. $A \subseteq A^{\perp\perp}$ implies $A^{\perp} \subseteq A^{\perp\perp\perp}$, while $A^{\perp} \supseteq A^{\perp\perp\perp}$ results from (13.2). $\square$

13. 2. 2 Corollary. *A is a polar iff $A = A^{\perp\perp}$.*

Orthogonality of elements of S is closely connected with orthogonality of c-ideals of $\mathfrak{S}$. First by polar arithmetic we get:

13. 2. 3 Proposition. *Any polar A is a c-ideal.*

This leads to

$$x \perp A \iff x^c \cap A^c = \{1\}. \tag{13.4}$$

PROOF. $x \perp A \Longrightarrow x^c \subseteq A^{\perp} \Longrightarrow A \subseteq x^{c\perp} \Longrightarrow A^c \subseteq x^{c\perp} \Longrightarrow x^c \cap A^c = \{1\}$ and $x^c \cap A^c = \{1\} \Longrightarrow |\,y\,| \wedge |\,z\,| = 1$ $(\forall\, y \in x^c, z \in A^c)$. $\square$

In addition it turned out:

$$A^{\perp} \;=\; (A^c)^{\perp}. \tag{13.5}$$

Henceforth we denote the set of polars of $\mathfrak{S}$ by $P(\mathfrak{S})$. Obviously $P(\mathfrak{S})$ is partially ordered, but, in fact, it holds much more. However, before continuing we emphasize, that we will have to distinguish between the *c-(ideal-)hull* of two polars and their *P-(olar-)hull.* Therefore we will indicate by indices c and p, respectively, which hull is just under consideration. Furthermore we repeat that $\bigvee$ without index stands for the c-ideal-hull.

$$(\bigvee A_i)^{\perp} \;=\; \bigcap(A_i{}^{\perp}) \;\; (i \in I). \tag{13.6}$$

PROOF. By (13.2) the left side is contained in the right side. On the other hand, if x belongs to the right side, x is orthogonal to all A_i, and the positive cone of $\bigvee A_i$ contains exactly the (finite) products of positive elements of the components A_i, whence also the right side is contained in the left side. $\square$

In particular, by (13.6) the intersection of polars is again a polar. Furthermore, as immediate consequences, we get:

13. 2. 4 Corollary. *$P(\mathfrak{S})$ is a* MOORE *family.*

13. 2. 5 Corollary. *The set of polars forms a complete lattice $\mathfrak{P}(\mathfrak{S})$ under*

$$\bigwedge A_i := \bigcap A_i \;\text{ and }\; \bigvee_p A_i := (\bigcap A_i{}^{\perp})^{\perp} \quad (i \in I). \tag{13.7}$$

PROOF. According to (13.6) along with any family also its intersection is a polar, and the second assertion results from

$$\begin{aligned} P \supseteq \bigvee A_i \iff & P^\perp \subseteq \bigcap {A_i}^\perp \\ \iff & P \supseteq (\bigcap {A_i}^\perp)^\perp \quad (i \in I)\,. \end{aligned} \qquad \square$$

Next we will show, that the polars do not only form a complete lattice, but even a complete boolean algebra. To this end we observe first:

13. 2. 6 Proposition. *The mapping $A \longmapsto A^{\perp\perp}$ respects boundaries and is a homomorphism of the lattice of c-ideals of $\mathfrak{G}$ onto the lattice $\mathfrak{P}(\mathfrak{G})$ of polars. In particular this implies that the lattice of polars is distributive.*

PROOF. Let A, B be c-ideals. Then it results

$$(A \vee_c B)^{\perp\perp} \supseteq A^{\perp\perp} \vee_p B^{\perp\perp} \supseteq A, B \tag{13.8}$$

and thereby, recall that $A^{\perp\perp}$ is a polar,

$$(A \vee_c B)^{\perp\perp} = A^{\perp\perp} \vee_p B^{\perp\perp}\,. \tag{13.9}$$

Next we obtain

$$(A \cap B)^{\perp\perp} = A^{\perp\perp} \cap B^{\perp\perp}\,. \tag{13.10}$$

FOR: Let's start from $x \in A^{\perp\perp} \cap B^{\perp\perp}$ and $y \in (A \cap B)^\perp$. Then all $a \in A$, $b \in B$ satisfy $|\,a\,| \wedge |\,b\,| \in A \cap B$ and

$$|a| \wedge |b| \wedge |x| \wedge |y| = 1 \;\rightsquigarrow\; |b| \wedge |x| \wedge |y| \in A^\perp \cap A^{\perp\perp} = \{1\}\,.$$

And this implies

$$|\,x\,| \wedge |\,y\,| \;\in\; B^{\perp\perp} \cap B^\perp = \{1\}\,,$$

that is $x \in (A \cap B)^{\perp\perp}$ – recall that y was taken as an arbitrary element of $(A \cap B)^\perp$. $\square$

The preceding proposition provides nearly immediately:

$$a^{\perp\perp} \cap b^{\perp\perp} = (|\,a\,| \wedge |\,b\,|)^{\perp\perp}\,, \tag{13.11}$$

SINCE $\quad a^{\perp\perp} \cap b^{\perp\perp} = a^{c\perp\perp} \cap b^{c\perp\perp} = (a^c \cap b^c)^{\perp\perp} = (|\,a\,|^c \cap |\,b\,|^c)^{\perp\perp}\,.$ $\square$

Moreover, according to 13.2.5 any polar A satisfies

$$A \cap A^{\perp} = \{1\} \quad \text{and} \quad A \vee_p A^{\perp} = S\,. \tag{13.12}$$

Thus we are led to the main theorem of this section:

13. 2. 7 Proposition. *$P(\mathfrak{S})$ forms a complete boolean lattice. This means in particular, that $P(\mathfrak{S})$ satisfies:*

$$A \vee_p \bigwedge B_i \;=\; \bigwedge (A \vee_p B_i)\,. \tag{13.13}$$

$$A \cap \bigvee_p B_i \;=\; \bigvee_p (A \cap B_i)\,. \tag{13.14}$$

PROOF. These laws are valid in any complete boolean algebra – recall the formula $u \vee v = u \vee (\overline{u} \wedge v)$ implying $u \vee v \leq u \vee w \iff \overline{u} \wedge v \leq \overline{u} \wedge w$ and thereby

$$\begin{aligned} \bigwedge (a \vee b_i) = a \vee (\overline{a} \wedge x) &\implies \overline{a} \wedge x \leq \overline{a} \wedge b_i \qquad (i \in I) \\ &\implies \bigwedge (a \vee b_i) \leq a \vee \bigwedge b_i \quad (i \in I) \end{aligned}$$

and the dual calculation. □

13.3 Filets and z-ideals

13. 3. 1 Definition. Let a belong to S. Then the bipolar $a^{\perp\perp}$ is also called the *principal polar*, generated by a, and the set of all principal polars in $\mathfrak{S}$ is symbolized by $PP(\mathfrak{S})$.

Immediately we get from 13.2.6:

13. 3. 2 Proposition. *The set of principal polars of $\mathfrak{S}$ forms a sublattice $\mathfrak{PP}(S)$ of the lattice of all polars.*

Let $f : V \longmapsto V'$ be some lattice homomorphism and let V' have a minimum z'. Then we call *kernel* of f the set $\{x \mid f(x) = z'\} =: \ker(f)$.

13. 3. 3 Proposition. *$a^+ \longmapsto a^{+\perp\perp}$ defines a homomorphism of $(S^+, \wedge, \vee)$ onto $\mathfrak{PP}(S)$, and the associated lattice congruence $\sim_f$ is the coarsest lattice congruence of $\mathfrak{S}^+$ with kernel $\{1\}$.*

PROOF. By evidence, ϕ is a lattice homomorphism with kernel $\{1\}$. Let now ρ be another congruence with kernel $\{1\}$. Then from $x\,\rho\,y$ it follows $x \wedge a = 1 \Longrightarrow (y \wedge a)\,\rho\,1 \Longrightarrow y \wedge a = 1$, that is $x^{\perp\perp} = y^{\perp\perp}$. □

13. 3. 4 Definition. Let $\mathfrak{S}$ be a right normal d-monoid. Then $\sim_f$ is called the *filet-congruence* on $\mathfrak{S}^+$, and its classes $F(a)$ are called the filets of $\mathfrak{S}^+$.

So, keep in mind, $a^+ \sim_f b^+$ is equivalent to $a^{+\perp\perp} = b^{+\perp\perp}$.

13. 3. 5 Proposition. *The filets of a right normal d-monoid are convex and closed under multiplication, $\wedge$, and $\vee$.*

PROOF. (13.1) implies $a^{+\perp\perp} = b^{+\perp\perp} \Longrightarrow a^{+\perp} = b^{+\perp} \Longrightarrow (a^+b^+)^{\perp\perp} = (a^+a^+)^{\perp\perp} = a^{+\perp\perp}$. The rest follows from (13.8) and (13.9). □

13. 3. 6 Proposition. *If F is the filet of a^+, then F^c is equal to $a^{\perp\perp}$.*

PROOF. First $x^+ \in F \Longrightarrow x^{+\perp\perp} = a^{+\perp\perp} \Longrightarrow x^+ \in a^{+\perp\perp} \subseteq |\,a\,|^{+\perp\perp} = a^{\perp\perp}$, that is $F \subseteq a^{\perp\perp}$, and thereby $F^c \subseteq a^{\perp\perp}$.

Suppose now $x \in a^{\perp\perp}$. Then it results, recall $u^{\perp\perp} = |u|^{\perp\perp}$, $x^+ \vee a^+ \in a^{\perp\perp} \subseteq a^{+\perp\perp}$, implying $(x^+ \vee a^+)^{\perp\perp} = x^{+\perp\perp} \vee a^{+\perp\perp} = a^{+\perp\perp}$, that is $x^+ \vee a^+ \in F$, and hence $x \in F^c$ since $x \leq x^+ \vee a^+ \subseteq F \subseteq F^c$, meaning $a^{\perp\perp} \subseteq F^c$. □

13. 3. 7 Definition. A *z-ideal* is a c-ideal, closed w. r. t. to $\sim_f$.

By 13.3.6 any z-ideal A satisfies $a \in A \Longrightarrow a^{\perp\perp} = |\,a\,|^{\perp\perp} \subseteq A$.

13. 3. 8 Proposition. *Let $\mathfrak{S}$ be a d-monoid. Then the following are pairwise equivalent:*

(*i*) *A is a z-ideal.*

(*ii*) *A is union of an up-directed set of bipolars.*

(*iii*) *A is union of all elements of some sublattice of $\mathfrak{P}\mathfrak{P}(S)$.*

(*iv*) *A is union of all elements of some sublattice of $\mathfrak{P}(\mathfrak{S})$.*

(*v*) *A is union of an up-directed set of polars.*

PROOF. (*i*) $\Longrightarrow$ (*ii*). First, by assumption of (*i*) we are led to the implication: $x \in A^+ \Longrightarrow F(x) \subseteq A \Longrightarrow C(F(x)) \subseteq A \Longrightarrow x^{\perp\perp} \subseteq A$, i. e. $A = \bigcup x^{\perp\perp}$ $(x \in A^+)$. Furthermore we get $x, y \in A^+ \Longrightarrow x \vee y \in x^{\perp\perp} \vee y^{\perp\perp} = (x \vee y)^{\perp\perp} \subseteq A$.

$(ii) \Longrightarrow (iii)$. Let $A = \bigcup {x_i}^{\perp\perp}$ $(i \in I)$ for some up-directed system ${x_i}^{\perp\perp}$. Then the system of all $x^{\perp\perp} \subseteq {x_j}^{\perp\perp}$ $(\exists\, j \in I)$ satisfies obviously the assertion.

$(iii) \Longrightarrow (iv) \Longrightarrow (v)$ holds *a fortiori.*

$(v) \Longrightarrow (i)$. Consider $A = \bigcup {A_i}^{\perp}$ $(i \in I)$ with some up-directed system of polars ${A_i}^{\perp}$. Here we get $y^+ \sim_f x^+ \in {A_j}^{\perp}$ $(\exists\, j \in I) \Longrightarrow y \in y^{\perp\perp} \subseteq {A_j}^{\perp\perp} \subseteq A$. $\square$

Next we present a characterization of *filet respecting congruences.*

13. 3. 9 Proposition. *Let h be a homomorphism from some d-monoid $\mathfrak{S}$ onto some d-monoid $\mathfrak{T}$. Then the following are equivalent:*

(i) $a^\perp = b^\perp \Longrightarrow h(a)^\perp = h(b)^\perp$

(ii) $H := \ker(h)$ *forms a z-ideal.*

PROOF. $(i) \Longrightarrow (ii)$. Let (i) be satisfied and suppose $h(a) = e$. Then

$$\begin{aligned} b^\perp = a^\perp \ \&\ a \in H &\Longrightarrow h(b)^{\perp\perp} = h(a)^{\perp\perp} = \{e\} \\ &\Longrightarrow h(b) = e \\ &\Longrightarrow b \in H\,. \end{aligned}$$

$(ii) \Longrightarrow (i)$. First we show $h(a)^\perp \supseteq h(a^{\perp\perp})^\perp$ and thereby

$$(\star) \qquad h(a)^\perp = h(a^{\perp\perp})^\perp\,.$$

OBSERVE:

$$\begin{aligned} h(x) \in h(a)^\perp &\Longrightarrow h(|x|) \wedge h(|a|) = h(1) \\ &\Longrightarrow h(|x| \wedge |a|) = h(1) \\ &\Longrightarrow |x| \wedge |a| \in ker(h)) \\ &\Longrightarrow (|x| \wedge |a|)^{\perp\perp} \subseteq ker(h) \\ &\Longrightarrow x^{\perp\perp} \cap a^{\perp\perp} \subseteq ker(h) \\ &\Longrightarrow x \wedge y \in ker(h) \ \ (\forall y \in a^{\perp\perp}) \\ &\Longrightarrow h(x) \wedge h(y) = h(1) \ \ (\forall y \in a^{\perp\perp}) \\ &\Longrightarrow h(x) \in h(a^{\perp\perp})^\perp\,. \end{aligned}$$

Now by $(\star)$ we get

$$\begin{array}{rcl} a^\perp & = & b^\perp \\ & \Longrightarrow & \\ h(a)^\perp = h(a^{\perp\perp})^\perp & = & h(b^{\perp\perp})^\perp = h(b)^\perp\,, \end{array}$$

which had to be proven. □

Finally we show:

13. 3. 10 Proposition. *Let $\mathfrak{S}$ be a right normal d-monoid. Then the following are pairwise equivalent:*

- (i) *Any c-ideal C is a z-ideal.*
- (ii) *Each a of $\mathfrak{S}$ satisfies $a^c = a^{\perp\perp}$.*
- (iii) $a^{\perp\perp} = b^{\perp\perp}$ *is equivalent to* $a^c = b^c$.

PROOF. $(i) \Longrightarrow (ii)$. $a^c \subseteq a^{\perp\perp}$ is always satisfied, and condition (i) implies that any z-ideal of type a^c satisfies $a^{\perp\perp} \subseteq a^c$, by definition.

$(ii) \Longrightarrow (iii)$ is obvious.

$(iii) \Longrightarrow (i)$. Condition (iii) entails

$$b \sim_f a \in C \Longrightarrow a^{\perp\perp} = b^{\perp\perp} \Longrightarrow b^c = a^c \subseteq C \Longrightarrow b \in C\,. \qquad \square$$

13.4 Minimal prime c-Ideals

Minimal prime c-ideals on the one hand and *polars* on the other hand are closely connected. It turns out that any prime c-ideal is a z-ideal, that is a union of polars whereas any polar is the intersection of minimal prime c-ideals. We start by verifying the second assertion.

13. 4. 1 Proposition. *Any $A^\perp \neq S$ of a d-monoid $\mathfrak{S}$ is the intersection of all minimal prime c-ideals, not containing A.*

PROOF. We show, that $A^\perp$ is the intersection of all values of elements of A and then that all minimal prime c-ideals, not containing C, contribute to this intersection.

Since $A^\perp$ is a c-ideal, $A^\perp$ can be extended w. r. t. any $a \in A$ to some value of a. We consider the intersection D of all values of this type. Then it follows $D = A^\perp$, since otherwise, there would exist some $x^+ \in D\backslash A^\perp$ and some $a^+ \in A$, with $x^+ \wedge a^+ \in D\backslash A^\perp$, a contradiction!

Finally any minimal prime c-ideal $P \not\supseteq A$, contributes to the intersection, since $a \notin P \Longrightarrow P \supseteq a^{\perp} \Longrightarrow P \supseteq A^{\perp}$. □

As shown above, the mapping $M \longrightarrow S^{+}\backslash M$ provides a bijection between the set of all minimal prime c-ideals and the set of all ultrafilters of $\mathfrak{S}^{+}$ and this mapping provides, in a canonical manner, a bijection between the set of all minimal prime c-ideals of $\mathfrak{S}$ and the set of all ultrafilters of the lattice $\mathfrak{P}\mathfrak{P}(S)$, since the mapping $a^{+} \longmapsto a^{\perp\perp}$ provides a surjective lattice homomorphism of $(S^{+}, \wedge, \vee)$ onto $\mathfrak{P}\mathfrak{P}(S)$ with $1 \neq a^{+} \longmapsto a^{\perp\perp} \neq \{1\}$.

13. 4. 2 Proposition. *Let P be a* proper prime c-ideal *of $\mathfrak{S}$. Then the following are pairwise equivalent:*

(*i*) *P is a minimal prime c-ideal.*

(*ii*) $P = \bigcup x^{\perp}\ \ (x \notin P)$.

(*iii*) $y \in P \Longrightarrow y^{\perp} \not\subseteq P$.

PROOF. $(i) \Longrightarrow (ii)$. Let P be prime. Then we get $x \notin P \Longrightarrow x^{\perp} \subseteq P$. Let now P be even minimal prime. Then $S^{+}\backslash P$ forms an ultrafilter, whence for each $x^{+} \in P$ there exists some $y^{+} \in S^{+}\backslash P$ with $x^{+} \perp y^{+}$. Consequently the cone of P and thereby the whole of P is exhausted by $\bigcup x^{\perp}\ \ (x \notin P)$.

$(ii) \Longrightarrow (iii)$. In case of (ii) any $y \in P$ is orthogonal to at least one $x \notin P$.

$(iii) \Longrightarrow (i)$. In case of (iii) the set $S^{+}\backslash P$ is an ultrafilter. □

The previous result implies the stronger proposition

13. 4. 3 Proposition. *Let C be a c-ideal of $\mathfrak{S}$ and let U be an ultrafilter of C^{+}. Then the set $\bigcup x^{\perp}\ \ (x \in U)$ forms a minimal prime c-ideal P in $\mathfrak{S}$, and any minimal prime $M \not\supseteq C$ arises this way.*

PROOF. Let U be an ultrafilter in $\mathfrak{C}$. We show first, that the subset $V := \{x \mid \exists\, u \in U : x \geq u\}$ is an ultrafilter in $\mathfrak{S}^{+}$. This will prove the first part. To this end let $x \in S^{+}\backslash V$ and u be arbitrary chosen in U, and thereby elements also of V. Then it holds $x \wedge u \in C\backslash U$, since otherwise x must belong to V. Consequently there exists some $y \in U$ with $x \wedge u \wedge y = 1$ and thereby some $u \wedge y \in V$ with $x \wedge (u \wedge y) = 1$.

Let now M be an arbitrary minimal prime c-ideal of $\mathfrak{S}$, not containing C. We define $V := S^{+}\backslash M$ and $U = V \cap C$. Thus we get U as an ultrafilter in

C^+, and the elements $x \geq u \in U$ form an ultrafilter in $\mathfrak{S}^+$, containing the ultrafilter V, because $v \geq u \wedge v \in U$. Hence, according to the first part, this ultrafilter must be equal to V. But, because $1 \leq u \leq v \Longrightarrow v^\perp \subseteq u^\perp$ this leads to $M = \bigcup v^\perp \ (v \in V) = \bigcup u^\perp \ (u \in U)$. □

Finally we mention, as a certain application of 13.4.1 and as a generalization of proposition 13.4.2.

13. 4. 4 Corollary. *Let P a prime c-ideal of $\mathfrak{S}$. Then the intersection D of all minimal prime c-ideals, contained in P, equals $N := \bigcup x^\perp \, (x \notin P)$.*

PROOF. By evidence, it holds $N \subseteq D$.

Start now from $a \in D \backslash N$. Then it follows $|\,a\,| \wedge |\,x\,| \neq 1 \ (\forall x \notin P)$. Hence, in this case, the set of all x with $|\,a\,| \wedge |\,x\,| \neq 1 \ (|\,x\,| \in S^+ \backslash P)$ is a filter F , containing $S^+ \backslash P$ and embedded in an ultrafilter U, containing a. So $S^+ \backslash U$ would be a minimal c-ideal, contained in P, but not containing a , a contradiction! □

13.5 Direct Factors

Let $\mathfrak{S}$ and $\mathfrak{T}$ be two d-semigroups. Then also their *direct product* is a d-semigroup. But there need not be substructures of this direct product, isomorphic with the starting d-semigroups $\mathfrak{S}$, $\mathfrak{T}$ unless $\mathfrak{S}$ and $\mathfrak{T}$ are not both monoids, that is, like other algebraic structures, also in the case of d-semigroups to be a direct product does not imply to admit an inner decomposition. Hence, admitting an inner decomposition is stronger then arising from direct (outer) factors. In spite of this we will speak of *direct factors* instead of *inner direct factors.*

Henceforth, in this section, we will consider c-ideals as *substructures.* Therefore c-ideals will be called c-monoids of $\mathfrak{S}$, here. Again, recall the distributivity of the lattice of all c-monoids of a d-monoid.

13. 5. 1 Lemma. *Let $\mathfrak{S}$ be a d-monoid. Then any inner direct decomposition $\mathfrak{S}^+$ induces an inner direct decomposition of $\mathfrak{S}$.*

PROOF. Let $a \in S$ and suppose $\mathfrak{S}^+ = \mathfrak{S}_1^+ \times \mathfrak{S}_2^+$. Then it follows Δ:

$$a = (a^+)(a^-) = (a_1^+ \cdot a_2^+) \cdot (a_2^* \cdot a_1^*)^{-1} = (a_1^+ \cdot a_1^{*-1}) \cdot (a_2^+ \cdot a_2^{*-1}).$$

Hence it holds $S = S_1 \cdot S_2$. But it follows as well $S_1 \cap S_2 = \{1\}$, because $a \in S_1 \cap S_2 \Longrightarrow |\,a\,| \in S_1 \cap S_2 \Longrightarrow a = 1$. It remains to verify uniqueness. To this end, let $a = uv = xy$ with $u, x \in S_1$ and $v, y \in S_2$. Then it results

$$\begin{array}{rrcl} & u \cdot v & = & x \cdot y \\ \Longrightarrow & (u^+v^+) \cdot (v^*u^*)^{-1} & = & (x^+y^+) \cdot (y^*x^*)^{-1} \\ \Longrightarrow & (u^+v^+) \cdot (y^*x^*) & = & (x^+y^+) \cdot (v^*u^*) \\ \Longrightarrow & u^+ = x^+ \ \&\ u^* = x^* & \& & v^+ = y^+ \ \&\ v^* = y^* \\ \Longrightarrow & u = x & \& & v = y. \end{array}$$

Thus we are through. □

13. 5. 2 Proposition. *Let $\mathfrak{S}$ be a d-monoid and let $\mathfrak{A}$, $\mathfrak{B}$ be c-monoids in $\mathfrak{S}$. Then it holds $\mathfrak{S} = \mathfrak{A} \otimes \mathfrak{B}$ iff $S = A \cdot B$, $A = B^\perp$ and $B = A^\perp$.*

PROOF. $|\,a\,| \wedge |\,b\,| \neq 1$ would mean that $|\,a\,| \wedge |\,b\,|$ has different decompositions. Hence the condition is necessary. But, by the rules of arithmetic it is also sufficient, since the positive elements are uniquely decomposed. □

Next we get

13. 5. 3 Proposition. *A c-monoid $\mathfrak{A}$ is a direct factor of $\mathfrak{S}$ if it satisfies $A \cdot A^\perp = S$, and in this case it satisfies moreover $A = A^{\perp\perp}$.*

PROOF. $A \cdot A^\perp = S$ implies $A^{\perp\perp} \cdot A^\perp = S$ with $A = A^{\perp\perp}$, the rest is clear. □

13. 5. 4 Corollary. *Let $\mathfrak{C}$ be a c-monoid in $\mathfrak{S}$. Then $\mathfrak{A}^\perp$ is a direct factor of $\mathfrak{C}$, iff $A^\perp \subseteq C \subseteq A^\perp A^{\perp\perp}$.*

Now we are in the position to prove:

13. 5. 5 Proposition. *Let $\mathfrak{A}$, $\mathfrak{B}$ be direct factors of $\mathfrak{S}$. Then it holds*

$$(\mathfrak{A} \cap \mathfrak{B})^\perp = \mathfrak{A}^\perp \vee \mathfrak{B}^\perp = \mathfrak{A}^\perp \cdot \mathfrak{B}^\perp .$$

PROOF. If $\mathfrak{A}$, $\mathfrak{B}$ are direct factors, we get first

$$AA^\perp = S = BB^\perp \Longrightarrow (A \cap B)(A^\perp \vee B^\perp) = S$$

with $(A \cap B) \cap (A^\perp \vee B^\perp) = \{1\}$. So, $(A \cap B)^\perp = A^\perp \vee_p B^\perp$, whereby we get

$$A^\perp \vee_p B^\perp \;=\; A^\perp \cdot B^\perp\,,$$

by the equations $(A \cap B) \cdot (A^\perp B^\perp) = S$ and $A^\perp B^\perp \subseteq A^\perp \vee_p B^\perp$, and the uniqueness of complements in distributive lattices. □

13. 5. 6 Corollary. *The direct factors of any d-monoid form a boolean sublattice of the lattice of polars.*

By a *directly indecomposable* d-monoid one means a d-monoid, not containing any non trivial direct factor, like for instance linearly ordered d-monoids or the ℓ-groups with 0.

As a less trivial example we present the additive ℓ-group of continuous functions $f : \mathbf{R} \longrightarrow \mathbf{R}$. Here, for instance, the function $f : x \longmapsto 1$ has no decomposition into orthogonal components, which results from continuity.

Now we turn to infinite direct products.

13. 5. 7 Definition. Let $\mathfrak{A}_i$ $(i \in I)$ be a family of c-monoids of $\mathfrak{S}$ and let $\mathfrak{B}_j$ for each $j \in I$ be the c-monoid, generated in $\mathfrak{S}$ by the union of all A_i $(i \neq j)$. If then for each $i \in I$ $\mathfrak{S}$ is the direct product of $\mathfrak{A}_i$ and $\mathfrak{B}_i$, then we call $\mathfrak{S}$ an inner direct product of the factors $\mathfrak{A}_i$ and we write $\mathfrak{P} = \bigotimes \mathfrak{A}_i$ $(i \in I)$.

As an immediate consequence of 13.5.6 this definition leads to

13. 5. 8 Proposition. *Let $\mathfrak{A}_i$ $(i \in I)$ be a family of c-monoids of $\mathfrak{S}$. Then $\mathfrak{S}$ is equal to $\bigotimes \mathfrak{A}_i$ $(i \in I)$ iff $\mathfrak{S}$ is generated by $\{A_i\}$ and if in addition each $i \neq j$ satisfies $A_i \subseteq {A_j}^\perp$.*

Furthermore, as an immediate consequence of 13.1.6 we get

13. 5. 9 Proposition. *$\mathfrak{S} = \bigotimes \mathfrak{A}_i$ $(i \in I)$ implies that any c-monoid $\mathfrak{C}$ of $\mathfrak{S}$ satisfies $\bigotimes(\mathfrak{A}_i \cap \mathfrak{C})$ $(i \in I)$.*

Thus we get next

13. 5. 10 Proposition. *Suppose that $\mathfrak{S} = \bigotimes \mathfrak{A}_i$ $(i \in I)$ and $\mathfrak{S} = \bigotimes \mathfrak{B}_j$ $(j \in J)$ are inner direct decompositions of $\mathfrak{S}$. Then $\bigotimes(\mathfrak{A}_i \cap \mathfrak{B}_j)$ $(i, j \in I \times J)$ is an inner direct decomposition of $\mathfrak{S}$, too.*

In particular this implies

13. 5. 11 Corollary. *Whenever $\mathfrak{S}$ admits a direct decomposition into directly indecomposable components, then this decomposition is uniquely determined.*

Chapter 14

Orthogonality and Linearity

14.1 Lexicographical Extensions

AN EXAMPLE: Let $\mathfrak{A}$ be a linearly ordered group and $\mathfrak{B}$ some ℓ-group. We put $(a_1, b_1) < (a_2, b_2)$ iff $a_1 < a_2$ or $a_1 = a_2$ and $b_1 < b_2$ are satisfied. Then a new ℓ-group $\mathfrak{A} \circ \mathfrak{B}$ is defined, called the *lexicographic product* of $\mathfrak{B}$ over $\mathfrak{A}$. Obviously, then $\mathfrak{A}$ forms a *prime c-monoid*, which is *majorized* by any positive element of $S \backslash A$. This motivates the definition:

14. 1. 1 Definition. Let $\mathfrak{C}$ be a prime c-monoid of $\mathfrak{S}$. Then $\mathfrak{S}$ is called a *lexicographic extension*, also a *lex-extension* of $\mathfrak{C}$, if each $s \in S^+ \backslash C$ majorizes each $c \in C$.

Lex-extensions play a most important role in ℓ-group structure theory. But we shall see that the results, presented in BIGARD-KEIMEL-WOLFENSTEIN, [11], up to minimal exceptions remain valid in right normal d-monoids. As a first result we present:

14. 1. 2 Proposition. *Let C be a c-ideal of $\mathfrak{S}$. Then the following are pairwise equivalent:*

(*i*) *$\mathfrak{S}$ is a lex-extension of $\mathfrak{C}$.*

(*ii*) *C is prime and comparable with all c-ideals L of $\mathfrak{S}$.*

(*iii*) *C contains all polars, different from S .*

(*iv*) *C contains all minimal prime c-ideals of $\mathfrak{S}$.*

(*v*) *Any $a \in S$ outside of C has exactly one value .*

(*vi*) *Any $a \in S$ outside of C satisfies $a^\perp = \{1\}$.*

PROOF. $(i) \Longrightarrow (ii)$. (i) implies by definition that C is prime. Let now L be a further c-ideal, satisfying $L \not\subseteq C$. Then the positive elements of $L\backslash C$ majorize the set C^+. Hence we get $C \subseteq L$.

$(ii) \Longrightarrow (iii)$. In case of (ii) the c-ideal C is prime and comparable with all polars. Hence from $A^\perp \not\subseteq C$ it follows first $A^{\perp\perp} \subseteq C$, that is $A^{\perp\perp} \subseteq A^\perp$, and thereby next $A \subseteq A^{\perp\perp} = \{1\}$, which means $A^\perp = S$.

$(iii) \Longrightarrow (iv)$. Recall, any minimal prime c-ideal is a union of polars.

$(iv) \Longrightarrow (v)$. Consider $a \notin C$ and let V and W be values of a. Then V and W contain minimal prime c-ideals, which themselves are contained in C. Hence C is comparable with V and with W, and thereby contained in V and in W. This means that V and W contain a common prime c-ideal. Hence V and W are comparable.

$(v) \Longrightarrow (vi)$. Suppose $1 \neq a \perp b \neq 1$ with positive elements a, b and $a \notin C$. Then a is associated with some value $W(b)$ and b is associated with some value $W(a)$. But $W(a)$ and $W(b)$ both admit an extension to the uniquely determined $W(a \vee b)$. So we get $W(a) = W(a \vee b) = W(b)$, a contradiction!

$(vi) \Longrightarrow (i)$. By (vi) the c-ideal C is prime, according to 13.1.2 (vi), and if $x \in S^+\backslash C$, $y \in C^+$, then there exist elements x°, y° with $x^\circ \notin C$ such that $(x \wedge y)x^\circ = x$ and $(x \wedge y)y^\circ = y$ are satisfied. And this implies $y^\circ = 1$ by assumption, and thereby $y \leq x$, whence $\mathfrak{C}$ is a lex-extension of $\mathfrak{C}$. □

Nearly immediately we get

14. 1. 3 Lemma. *Let $C \subseteq H \subseteq S$ $(C, H \in C(\mathfrak{S}))$. Then $\mathfrak{S}$ is a lex-extension of $\mathfrak{C}$ iff $\mathfrak{S}$ is a lex-extension of $\mathfrak{H}$ and $\mathfrak{H}$ is a lex-extension of $\mathfrak{C}$.*

PROOF. Recall 14.1.2 □

In other words: $\mathfrak{S}$ is a lex-extension of $\mathfrak{C}$ iff $\mathfrak{S}$ is lex-extension of all c-monoids between $\mathfrak{C}$ and $\mathfrak{S}$.

14. 1. 4 Definition. By the *lex-kernel* of a d-monoid $\mathfrak{S}$, symbolized by Lex$(\mathfrak{S})$, we mean the hull of all proper polars P of $\mathfrak{S}$ in $C(\mathfrak{S})$, that is – compare 14.1.2 – the hull of all minimal prime c-ideals.

If even Lex$(\mathfrak{S}) = \mathfrak{S}$, $\mathfrak{S}$ is called *lex-simple.*

Otherwise, that is if Lex$(\mathfrak{S}) \neq \mathfrak{S}$ is satisfied, then we call $\mathfrak{S}$ a *lex-monoid.*

Nearly, by definition, we get

14. 1. 5 Lemma. $\mathfrak{A} \supseteq \mathfrak{B} \Longrightarrow \mathrm{Lex}\,(\mathfrak{A}) \supseteq \mathrm{Lex}\,(\mathfrak{B})$.

14. 1. 6 Lemma. $\mathfrak{S}$ *is a lex-extension of* $\mathfrak{C}$ *iff* $\mathrm{Lex}\,(\mathfrak{S})$ *is contained in* $\mathfrak{C}$.

14. 1. 7 Lemma. *Any linearly ordered convex submonoid of* $\mathfrak{S}$ *of cardinality* ≥ 2 *is a lex-monoid.*

Moreover $\mathfrak{S}$ is obviously linearly ordered iff $\mathrm{Lex}\,(\mathfrak{S}) = \{1\}$.

14. 1. 8 Proposition. $\mathrm{Lex}\,(\mathfrak{S})$ *is the biggest lex-simple c-monoid of* $\mathfrak{S}$.

PROOF. If $\mathrm{Lex}\,(\mathfrak{S})$ is a lex-extension of $\mathfrak{C}$, then according to the preceding remarks $\mathfrak{S}$ is a lex-extension of $\mathfrak{C}$, too, implying $C = \mathrm{Lex}\,(\mathfrak{S})$.

Let now $\mathfrak{L}$ with $L \in C(\mathfrak{S})$ be lex-simple. Then according to 14.1.2 (ii) it holds $\mathrm{Lex}\,(\mathfrak{S}) \supseteq L$ or $\mathrm{Lex}\,(\mathfrak{S}) \subseteq L$. But it cannot hold $\mathrm{Lex}\,(\mathfrak{S}) \subset L$ since L is lex-simple. $\square$

Furthermore we get

14. 1. 9 Proposition. *Let* $\mathfrak{a}^c$ *be the c-monoid, generated by* a. *Then* $\mathfrak{a}^c$ *is a lex-monoid iff* a *has exactly one value.*

PROOF. Let $\mathfrak{a}^c$ be a lex-monoid. Then a belongs to $\mathfrak{a}^c \backslash \mathrm{Lex}\,(\mathfrak{a}^c)$ and has accordingly exactly one value in $\mathfrak{a}^c$. Hence, in this case, a has only one value also in $\mathfrak{S}$ recall 13.1.6.

On the other hand suppose that a has only one value in $\mathfrak{S}$. Then a has only one value W in $\mathfrak{a}^c$, too. But then W is a value also of all other elements of $a^c \backslash W$. Consequently in $\mathfrak{a}^c$ any $V \in \mathrm{val}\,(k)$ $(k \notin W)$ admits an extension to W. Consequently any $k \notin W$ has exactly one value, whence $\mathfrak{a}^c$ is a lex-monoid by 14.1.2 (v). $\square$

14. 1. 10 Proposition. *Any pair of lex-monoids* $\mathfrak{A}\,, \mathfrak{B}$ *of* $\mathfrak{S}$ *is orthogonal or comparable.*

PROOF. Suppose that $\mathfrak{A}$ and $\mathfrak{B}$ are neither orthogonal nor comparable. Then there exist two elements $a \in A \backslash B$ and $b \in B \backslash A$ with $a \wedge b > 1$. We show that this implies either $\mathfrak{a}^c \subseteq \mathfrak{b}^c$ or $\mathfrak{b}^c \subseteq \mathfrak{a}^c$.

By 14.1.9 both, $\mathfrak{a}^c$ and $\mathfrak{b}^c$, are lex-monoids. So both, a and b, in $\mathfrak{S}$ would have values C and D, respectively, with

$$b \in B \subseteq C \in \mathrm{val}\,(a) \ \&\ a \in A \subseteq D \in \mathrm{val}\,(b),$$

respectively, and in addition these values would contain a common minimal prime c-ideal M, for instance a value of $a \wedge b$. So it would result $C \subseteq D \vee D \subseteq C$, in spite of $C \not\supseteq \{a, b\} \not\subseteq D$. $\square$

Observe, by 14.1.10 one may conclude from the local structure of some $\mathfrak{s}^c$ to the global structure of $\mathfrak{S}$ and conversely from the global structure of $\mathfrak{S}$ to the local structure of this $\mathfrak{s}^c$.

14. 1. 11 Proposition. *Let $\mathfrak{A}$ be a lex-monoid of $\mathfrak{S}$ and let $s \geq 1$. Then it holds*

$$s \notin A \times A^{\perp} \implies s > a \ (\forall\, a \in A)\,.$$

PROOF. Let L be the lex-kernel of A, $s \notin A \times A^{\perp}$, and $t \in A^{+} \backslash L$, and suppose $R(s, t, s^{\circ}, t^{\circ})$. Then by $t = (s \wedge t)t^{\circ} \notin L$ the assumption $s \wedge t \in L$ we would lead first to $t^{\circ} \in A^{+} \backslash L$ and thereby next:

$$\begin{array}{rrcl} & t^{\circ} \wedge (s^{\circ} \wedge a) & = & 1 \ (\forall\, a \in A^{+}) \\ \implies & s^{\circ} \wedge a & = & 1 \ (\forall\, a \in A^{+}) \\ \implies & s^{\circ} & \in & A^{\perp} \\ \implies & s & \in & A \times A^{\perp}, \end{array}$$

a contradiction. Hence it holds $s \geq s \wedge t > L$, that is $s > L$ for all $s \notin A \times A^{\perp}$. It remains to show $s \geq t \in A^{+} \backslash L$. To this end we consider s°. Since t and thereby also $s \wedge t$ belong to A^{+}, recall $s \notin A \times A^{\perp}$, also the element s° cannot belong to $A \times A^{\perp}$. Therefore t° must belong to L, since otherwise $t^{\circ} \wedge s^{\circ} \neq 1$ would follow. Thus we get $s^{\circ} \geq t^{\circ} \rightsquigarrow t^{\circ} = 1$, that is $s \geq t$ and thereby $s > A$. $\square$

14. 1. 12 Corollary. *Any lex-monoid $\mathfrak{A}$ not upper bounded by some $s \notin A$ is a direct factor of $\mathfrak{S}$.*

14. 1. 13 Proposition. *Let A and B be two c-ideals of $\mathfrak{S}$ and let A be properly contained in B. Then the following are pairwise equivalent:*

- (i) *$\mathfrak{B}$ is a lex-extension of $\mathfrak{A}$.*
- (ii) *$\mathfrak{B}^{\perp\perp}$ is a lex-extension of $\mathfrak{A}$.*
- (iii) *For all b of $B \backslash A$ it holds $\mathfrak{b}^{c\perp} = b^{\perp} = B^{\perp}$.*

PROOF. $(i) \implies (ii)$. In case of $B^{\perp\perp} = B$, there is nothing to show. Otherwise, let $1 < x \in B^{\perp\perp} \backslash B$ be satisfied. Then x cannot belong to $B \times B^{\perp}$, observe $B \times B^{\perp} = B \vee B^{\perp}$ and

$$(B \vee B^{\perp}) \cap B^{\perp\perp} = (B \cap B^{\perp\perp}) \vee (B^{\perp} \cap B^{\perp\perp}) = B \cap B^{\perp\perp}.$$

Consequently, it holds $x > B$, that is $\mathfrak{B}^{\perp\perp}$ is a lex-extension of $\mathfrak{B}$ and thereby also of $\mathfrak{A}$.

$(ii) \Longrightarrow (iii)$. Let $\mathfrak{B}^{\perp\perp}$ be a lex-extension of $\mathfrak{A}$. Then also $\mathfrak{B}$ is a lex-extension of $\mathfrak{A}$. Let now hold $1 < x \in B\backslash A$ and $x \in b^{\perp}$. Then any $y \in B$ satisfies the implication $b \perp x \Longrightarrow |\,b\,| \perp |\,y\,| \wedge |\,x\,| \Longrightarrow |\,y\,| \wedge |\,x\,| = 1$ and thereby $x \in B^{\perp}$. Hence, recall 14.1.2 (vi), $\mathfrak{B}$ is a lex-extension of $\mathfrak{A}$.

$(iii) \Longrightarrow (i)$. Suppose $b \in B\backslash A$, $x \in B$, and $|\,b\,| \wedge |\,x\,| = 1$. Then by (iii) we get $|\,x\,| \in B \cap b^{\perp} = B \cap B^{\perp} = \{1\}$. So it holds (i) by 14.1.2 (vi). □

14. 1. 14 Corollary. *If* $\mathfrak{B}$ *be a lex-extension of* $\mathfrak{A}$ *in* $\mathfrak{G}$ *then* $\overline{\overline{\mathfrak{B}}}$ *is a maximal lex-extension of* $\mathfrak{A}$ *in* $\mathfrak{G}$.

PROOF. According to 14.1.10 the lex-extensions $\mathfrak{C}$ of $\mathfrak{A}$ with $\mathfrak{B} \subseteq \mathfrak{C}$ form a chain. Hence there exists at most one maximal lex-extension of the formulated type. Let now $B^{\perp\perp} \subseteq C$ be satisfied, and let $\mathfrak{C}$ be a lex-extension of $\mathfrak{A}$. Then according to 14.1.13 (iii) it holds $B^{\perp} = C^{\perp}$, that is $B^{\perp\perp} \subseteq C \subseteq C^{\perp\perp} = B^{\perp\perp}$. □

14. 1. 15 Proposition. *Let* $\mathfrak{B}$ *be a lex-extension of* $\mathfrak{A} \neq \{1\}$ *in* $\mathfrak{G}$. *Then it follows* $A^{\perp} = B^{\perp}$.

PROOF. $B^{\perp} \subseteq A^{\perp}$ holds *a fortiori*.

Let now $x \in A^{\perp}$ & $b \in B$. Then we get $|\,b\,| \wedge |\,x\,| \in B$ and $|\,a\,| \wedge |\,x\,| \wedge |\,b\,| = 1$ for all $|\,a\,|$ of A, that is also $|\,b\,| \wedge |\,x\,| \in A^{\perp} \cap B$. But $|\,b\,| \wedge |\,x\,|$ belongs to A, since $|\,b\,| \wedge |\,x\,| \in B\backslash A$ would imply $|\,b\,| \wedge |\,x\,| \geq |\,a\,| \in A^{+}$ implying $A = \{1\}$, a contradiction!

Hence we get $|\,b\,| \wedge |\,x\,| \in A$ and thereby $|\,b\,| \wedge |\,x\,| \in A \cap A^{\perp}$, i.e. $|\,b\,| \wedge |\,x\,| = 1$, meaning $|\,x\,| \in B^{\perp}$, thus leading all at all to $A^{\perp} \subseteq B^{\perp}$. □

Again we emphasize:

14. 1. 16 Corollary. *In case of* $\{1\} \neq A \in C(\mathfrak{G})$ *the lex-extensions of* $\mathfrak{A}$ *form a chain with maximum* $\mathfrak{A}^{\perp\perp}$.

Henceforth we study the relations between the linearly ordered c-ideals of $\mathfrak{G}$ on the one hand, and the polars and minimal prime c-ideals of $\mathfrak{G}$ on the other hand. First of all we get:

14. 1. 17 Proposition. *Let P be a proper polar of $\mathfrak{G}$. Then the following are pairwise equivalent:*

(i) *P is linearly ordered.*

(ii) *P is maximal in the set of all linearly ordered c-ideals.*

(iii) *$P^\perp$ is prime.*

(iv) *$P^\perp$ is minimal prime.*

(v) *$P^\perp$ is a maximal polar.*

(vi) *P is a minimal polar.*

PROOF. (i) $\Longrightarrow$ (ii). Let (i) be satisfied and let C be a linearly ordered sup-c-ideal of P. Then according to 14.1.7 $\mathfrak{C}$ is a lex-extension of $\mathfrak{P}$ with $\overline{\overline{\mathfrak{C}}} \supseteq \overline{\overline{\mathfrak{P}}}$, and, according to 14.1.13, along with $\mathfrak{C}$ also $\overline{\overline{\mathfrak{C}}}$ is a lex-extension of $\mathfrak{P}$ and according to 14.1.16 $\overline{\overline{\mathfrak{P}}}$ is a maximal lex-extension of $\mathfrak{P}$ in $\mathfrak{G}$. This provides $C^{\perp\perp} \supseteq P^{\perp\perp} = P \rightsquigarrow C = P$.

(ii) $\Longrightarrow$ (iii). Suppose $R(x, y, x^\circ, y^\circ)$ and $x \wedge y \in P^\perp$, but x°, $y^\circ \notin P^\perp$. Then for some a^+, $b^+ \in P$ we get $1 \neq x^\circ \wedge a^+ \in P$ & $1 \neq y^\circ \wedge b^+ \in P$. Since P is linearly ordered, from this follows $x^\circ \wedge y^\circ > 1$, a contradiction! Consequently $P^\perp$ is prime.

(iii) $\Longrightarrow$ (iv), since – according to 13.4.1 – any polar is an intersection of minimal prime c-ideals.

(iv) $\Longrightarrow$ (v). Let $P^\perp$ be minimal prime and $P^\perp \subseteq Q^\perp \subseteq M$ with some minimal prime c-ideal M. Then it results $P^\perp = Q^\perp$.

(v) $\Longrightarrow$ (vi). Observe the antitonicity of $A \longmapsto A^\perp$ in the boolean algebra of the polars.

(vi) $\Longrightarrow$ (i). Let x, $y \in P$ be satisfied and assume $R(x, y, x^\circ, y^\circ)$. Then $x^\circ \neq 1$ implies first $P = x^{\circ\perp\perp}$, since P is minimal. This leads further to $y^\circ \in x^{\circ\perp} \cap x^{\circ\perp\perp}$, that is to $y^\circ = 1$ and thereby to $y \leq x$. □

Next we get:

14. 1. 18 Proposition. *Let C be a convex set of $\mathfrak{G}$ with $1 \in C$. Then the following are pairwise equivalent:*

(i) *C is linearly ordered.*

(ii) *$C^{\perp\perp}$ is linearly ordered.*

(iii) *C^c is linearly ordered.*

PROOF. $(i) \Longrightarrow (ii)$. In case of $C^{\perp\perp} = \{1\}$ we are through. Otherwise, suppose $1 \neq x \in C^{\perp\perp}$. Then x does not belong to $C^{\perp}$. Hence, w. r. t. x, there exists at least one $c_x \in C$ with $x \wedge c_x \neq 1$. Consequently any pair of positive elements of $C^{\perp\perp}$, different from 1, is not orthogonal, since C is linearly ordered . So from $R(a, b, a^\circ, b^\circ)$ it results $a^\circ = 1 \vee b^\circ = 1$. But hereby any two elements of $C^{\perp\perp}$ are comparable.

$(ii) \Longrightarrow (iii) \Longrightarrow (i)$ is evident. □

14. 1. 19 Corollary. *The linearly ordered polars of $\mathfrak{S}$ are exactly the maximal convex chains containing* 1*, in other words through* 1*.*

PROOF. Let P be a linearly ordered polar and $C \supseteq P$ a maximal convex chain. Then, according to 14.1.18, we get $C = C^{\perp\perp}$ and, according to 14. 1.17, we obtain $C = P$, since P is a polar and $C = C^{\perp\perp} \supseteq P$ is a minimal polar. □

14. 1. 20 Corollary. *Let C be a maximal convex chain through* 1*, and without upper bound, not belonging to C. Then $\mathfrak{C}$ is a c-monoid of $\mathfrak{S}$ and a direct factor.*

PROOF. Observe 14.1.12 □

As an example we give $\{p^n\}$ $(n \in \mathbf{N})^o$ with prime numbers p as a maximal convex chain of $(\mathbf{N}, \cdot, \mathrm{GGT})$ through 1.

If, however we adjoin the zero element 0, then there is an “outer” upper bound, and a direct decomposition is no longer possible.

On the other hand, that also *maximal chains with outer upper bound* may be direct factors, is shown by the boolean algebra. Here any convex chain of type $(1, p)$, where p is an atom, is a *proper* direct factor.

14. 1. 21 Corollary. *For strictly positive elements the following are pairwise equivalent:*

(i) *The interval* $[1, a]$ *is linearly ordered .*

(ii) $a^{\perp\perp}$ *is linearly ordered .*

(iii) a^c *is linearly ordered .*

This suggests to define:

14. 1. 22 Definition. Let $\mathfrak{S}$ be a d-monoid. We call $a \in S$ *basic* in $\mathfrak{S}$, if $[1, a]$ is linearly ordered .

Obviously any pair of basic elements is orthogonal or comparable. Furthermore – according to 14.1.9 and 14.1.2 – any basic element has exactly one value.

14.2 d-Monoids with a Base

14. 2. 1 Definition. Let $\mathfrak{S}$ be a d-monoid and B a subset of S. Then B is called *orthogonal*, if B satisfies:

(i) Any $b \in B$ is strictly positive.

(ii) Any two elements of B are orthogonal.

Obviously, by ZORNs lemma it holds:

14. 2. 2 Lemma. *Any orthogonal subset of $\mathfrak{S}$ admits an extension to a maximal orthogonal subset.*

Furthermore, without any difficulty, we get:

14. 2. 3 Lemma. *An orthogonal subset U is maximal iff $U^{\perp} = \{e\}$ or equivalently, iff $U^{\perp\perp} = S$ is satisfied.*

14. 2. 4 Definition. By a *base* we mean a maximal orthogonal subset B of S, whose elements are basic. Furthermore we call $\mathfrak{S}$ basic, if $\mathfrak{S}$ has a base.

The set of bases of $\mathfrak{S}$ is closely connected with the set of polars of $\mathfrak{S}$.

14. 2. 5 Proposition. *Let $\mathfrak{S}$ be a right normal d-monoid. Then the following are pairwise equivalent:*

(i) *$\mathfrak{S}$ has a base.*

(ii) *Any $a > 1$ majorizes at least one basic element.*

(iii) *The algebra of polars is atomic.*

(iv) *Any polar, different from S, is an intersection of maximal polars.*

(v) *$\{1\}$ is an intersection of maximal polars.*

PROOF. $(i) \Longrightarrow (ii)$. Let B be a base and let a not belong to B. Then, for at least one $b \in B$ it holds $a \not\perp b$, that is $1 \neq a \wedge b < b$ and thereby $(a \wedge b)^{\perp\perp} \subseteq b^{\perp\perp}$. Hence $(a \wedge b)^{\perp\perp}$ is linearly ordered , whence $a \wedge b$ is basic.

$(ii) \Longrightarrow (iii)$. Let A be a polar and let b be a basic element of A. Then it holds $b^{\perp\perp} \subseteq A$, and it is $b^{\perp\perp}$ a minimal polar, according to 14.1.17.

$(iii) \Longrightarrow (iv)$. Let $\mathfrak{B}$ be an arbitrary boolean algebra. Then $0 \neq a < \bigwedge m_i$, where $m_i = \overline{p_i}$ and p_i is an atom, would provide a prime element p with $p \leq \bigwedge (m_i \wedge \overline{a})$ and *co-atom* $\overline{p} \geq a$ & $\overline{p} \not\geq \bigwedge m_i$. Hence it holds $a = \bigwedge m_i$.

$(iv) \Longrightarrow (v)$ *a fortiori.*

$(v) \Longrightarrow (i)$. Let $P_i \ (i \in I)$ the family of the maximal polars. Then any $P_i{}^{\perp}$ is a linearly ordered $b_i{}^{\perp\perp}$. Hence any b_i is basic, and it is clear that any two different b_i , b_j are orthogonal.

So, it suffices to show, that the set $\{b_i\}$ of these elements forms a base, that is that $\{b_i\}^{\perp} = \{1\}$ is satisfied. To this end let $x \in b_i{}^{\perp}$ $(\forall i \in I)$ be satisfied. Then it follows $b_i{}^{\perp} = P_i$, because $b_i{}^{\perp} \supseteq P_i{}^{\perp\perp} = P_i$, and thereby $x \in \bigcap b_i{}^{\perp} = \bigcap P_i = \{1\}$. □

14.2.5 (ii) implies immediately:

14. 2. 6 Corollary. *A right normal d-monoid $\mathfrak{S}$ is basic iff its c-ideals are basic.*

Maximal polars are minimal prime c-ideals. Hence 14.2.5 tells that in any right normal d-monoid with a base there exists a family of prime c-ideals whose intersection is equal to $\{1\}$. This theorem is strengthened by

14. 2. 7 Proposition. *A right normal d-monoid $\mathfrak{S}$ is basic iff there exists a minimal family of prime c-ideals $P_i \ (i \in I)$ with*

$$\bigcap P_i \ (i \in I) = \{1\} \text{ and } \bigcap P_i \ (i \neq j \in I) \neq \{1\}\,.$$

PROOF. **(a)** Let the condition be satisfied.

First of all prime c-ideals P satisfy either $P^{\perp\perp} = P$ or $P^{\perp\perp} = S$. For, because $P \subseteq P^{\perp\perp}$ the bipolar $P^{\perp\perp}$ is prime according to 13.1.2. Hence $P^{\perp\perp}$ is equal to S or – according to proposition 14.1.17 – $P^{\perp\perp}$ is a maximal polar and thereby a minimal prime c-ideal of $\mathfrak{S}$.

Let now $\mathcal{F}$ be a minimal family in the sense of the theorem with $P \in \mathcal{F}$, and let D be the intersection of all Q of $\mathcal{F}$, different from P. Then, because $D \cap P = \{1\}$ it follows first $P^\perp \supseteq D \neq 1$, that is $P = P^{\perp\perp} \neq S$, whence next, according to 14.1.17, P is a maximal polar. Consequently $\mathcal{F}$ is a subfamily of the family of all maximal polars of $\mathfrak{S}$.

Let on the other hand C be a maximal polar, that is also a minimal prime c-ideal. Then there exists an element a with $C = a^\perp$ and some $P \in \mathcal{F}$ with $a \notin P$. But this implies $C = a^\perp \subseteq P$, that is $C = P$, since C is chosen maximal. Hence P is a polar. Consequently $\mathfrak{S}$ has a base.

(b) Let now $\mathfrak{S}$ have a base. Then by 14.2.5 (v) the set $\{1\}$ is equal to the intersection of all maximal polars, whence it remains only to prove, that the family of maximal polars is minimal in the sense of the theorem. But this follows, since the elements b_i, chosen below 14.2.5 in $(v) \Longrightarrow (i)$, form a base, that is satisfy the condition $b_i \in {b_j}^\perp$ $(j \neq i \in I)$, whence $b_i \in {P_j}^{\perp\perp} = P_j$ $(j \neq i \in I)$. □

In the remainder of this section, but only here, let $\mathfrak{S}$ be even a d-monoid with complementary cone. Then the congruences of $\mathfrak{S}$ correspond uniquely to the *invariant c-ideals*, which may be accepted by the reader here, and it holds:

14. 2. 8 Proposition. *A d-monoid $\mathfrak{S}$ with complementary cone has exactly one irreducible representation, if $\mathfrak{S}$ is representable and has a base.*

PROOF. Let $\mathfrak{S}$ be representable. Then the polars are invariant, and if in addition $\mathfrak{S}$ has a base, then, according to 14.2.7, there exists a 1-*disjoint family of invariant polars. Consequently there is an irreducible representation of $\mathfrak{S}$, recall 14.2.7.*

If, on the other hand, $\mathfrak{S}$ admits an irreducible representation, then there exists a minimal family P_i of prime c-ideals with $\bigcap P_i = \{1\}$. □

14. 2. 9 Corollary. *Let $\mathfrak{S}$ be a right normal d-monoid with complementary cone. Then any two irreducible representations are generated by the same c-ideals.*

14.3 Ortho-finite d-Monoids

14. 3. 1 Definition. Let $\mathfrak{S}$ be a right normal d-monoid. An element a is said ro have *height* n, if there exists a maximal chain of polars below $a^{\perp\perp}$ of length n

By the rules of *modularity* all maximal chains of the above type have length n, if one has length n .

14. 3. 2 Proposition. *Let $\mathfrak{S}$ be a right normal d-monoid. Then the following are pairwise equivalent:*

(i) *a has height n .*

(ii) *There exists a maximal chain*
$\{1\} \subset P_1 \subset P_2 \ldots \subset P_n = a^{\perp\perp}$ of polars P_i below $a^{\perp\perp}$.

(iii) *$a^{\perp\perp}$ has a base of length n .*

(iv) *a belongs to all minimal prime c-ideals except for at most n .*

(v) *If M is an orthogonal set below a then M contains at most n elements.*

PROOF. $(i) \Longrightarrow (ii)$ holds by definition.

$(ii) \Longrightarrow (iii)$. Assume (ii) and let $\{1\} \subset P_1 \subset \cdots \subset P_n = a^{\perp\perp}$ be a chain in the sense of the theorem. Then the sets $P_{i+1} \cap P_i{}^{\perp}$ are pairwise 1-disjoint and thereby linearly ordered. For, suppose that the elements x , $y \in P_{i+1} \cap P_i{}^{\perp}$ with $R(x, y, x^\circ y^\circ)$ are incomparable. Then, also x° and y° would belong to $P_{i+1} \cap P_i{}^{\perp}$, and the polar, generated by $P_i{}^{\perp}$ and x°, would lie strictly between P_i and P_{i+1}, since it would hold $P_i \subset (P_i \cup \{x\})^{\perp\perp} \subseteq P_{i+1} \backslash \{y\}$, the latter, since $y \neq 1$ belongs to $P_i{}^{\perp}$ and thereby does not belong to to $P_i{}^{\perp\perp}$.

$(iii) \Longrightarrow (iv)$. We show a bit more, namely: Let $(a_1, \ldots, a_n)$ be a base of $a^{\perp\perp}$. Then a does exactly not belong to the maximal polars and thereby minimal prime c-ideals $a_i{}^{\perp}$ $(1 \leq i \leq n)$.

So, let $(a_1, \ldots, a_n)$ be a base of $a^{\perp\perp}$. Then, for instance, the carrier of the submonoid generated by $(a_2, \ldots, a_n)$ is equal to $a_1{}^{\perp}$, that is to a polar, whence in case of $a \in a_1^{\perp}$ it must follow $a^{\perp\,\perp} \subseteq a_1^{\perp}$, a contradiction! Hence, a cannot belong to any $a_i{}^{\perp}$, which are maximal polars and thereby minimal prime c-monoids.

Let now M be minimal prime and $a \notin M$. Then $a^{\perp} \subseteq M$ and no a_i can belong to M, since $a_i \in M \Longrightarrow a_i^{\perp\perp} = M$ would lead to $a \in a^{\perp\perp} \subseteq a_i^{\perp}$.

$(iv) \Longrightarrow (v)$. Let $a_1, \ldots, a_m \leq a$ be pairwise orthogonal. We form the chain

$$a_1{}^{\perp}, (a_1 \vee a_2)^{\perp}, \ldots, (a_1 \vee a_2 \vee \ldots \vee a_m)^{\perp} .$$

This chain provides – analogously w. r. t. the procedure below $(ii) \Longrightarrow (iii)$ – m pairwise orthogonal basic elements with LUB, say b. Then, like below $(iii) \Longrightarrow (iv)$ we conclude, that b, and thereby also a does not belong to exactly m minimal prime c-ideals. This means $m \leq n$.

$(v) \Longrightarrow (i)$, since a chain in the sense of the proposition of a greater length than n would lead to more that n many pairwise orthogonal elements below a, consult the proof of $(ii) \Longrightarrow (iii)$. □

The next proposition concerns the case of a global n.

14. 3. 3 Proposition. *Let $\mathfrak{S}$ be a right normal d-monoid. Then the following are pairwise equivalent:*

- (i) *a is of finite height.*
- (ii) *Any z-ideal Z satisfies $a \in Z^{\perp\perp} \Longrightarrow a \in Z$.*
- (iii) *Any upper bounded orthogonal set is finite.*
- (iv) *The set of the special polars $P \supseteq a^{\perp\perp}$ satisfies the maximal condition.*
- (v) *The set of the polars, contained in $a^{\perp\perp}$, is finite.*

PROOF. $(i) \Longrightarrow (ii)$. Let a belong to $Z^{\perp\perp}$ and let $(a_1, \ldots, a_n)$ be a base of $a^{\perp\perp}$. Then it holds $a_i \in Z^{\perp\perp}$ $(1 \leq i \leq n)$, that is $a_i \notin Z^{\perp}$. Consequently for each $1 \leq i \leq n$ there exists an element $z_i \in Z$ with $1 < a_i \wedge z_i$. But a_i is basic. Hence ${a_i}^{\perp\perp}$ is a minimal polar. This leads next to $a_i \in {a_i}^{\perp\perp} = (a_i \wedge z_i)^{\perp\perp} \subseteq {z_i}^{\perp\perp} \subseteq Z$. Thus we get $a \in a^{\perp\perp} = (a_1 \vee \ldots \vee a_n)^{\perp\perp} \subseteq Z$.

$(ii) \Longrightarrow (iii)$. Let $\{a_i\}$ $(i \in I)$ be maximal in the set of all orthogonal sets upper bounded by a. We consider the union Z of all $b^{\perp\perp}$ with $b \in \bigvee {a_i}^c$. Then Z is the z-ideal, generated by the elements a_i, and by $a^{\perp\perp} \supseteq (\bigvee {a_i}^c)^{\perp\perp}$ it follows $a^{\perp\perp} = (\bigvee {a_i}^c)^{\perp\perp}$ since the polars form a boolean algebra, and this leads to $a \in a^{\perp\perp} = (\bigvee {a_i}^c)^{\perp\perp} = Z^{\perp\perp} \Longrightarrow a \in Z$. Hence there exists an element $b \in \bigvee {a_i}^c$ with $a \in b^{\perp\perp}$. On the other hand there exists a finite subset J of I with $b \in \bigvee {a_j}^c$ $(j \in J)$. But, this implies $I = J$. For, assume that a_k is an a_i with $k \notin J$. Then, on the one hand it would follow $b \in {a_k}^{\perp}$ and thereby on the other hand $a \in b^{\perp\perp} \subseteq {a_k}^{\perp}$, that is $a_k \in a^{\perp} \cap a^{\perp\perp}$.

$(iii) \Longrightarrow (iv)$. As shown above, any proper chain of polars provides an orthogonal set of at least as many elements as the chain has members.

$(iv) \Longrightarrow (v)$. The set of polars forms a boolean d-monoid, and the complement of a maximal polar is a minimal polar. So, if there are infinitely many minimal, and thereby atomic polars, then there exists also an infinite ascending chain of polars, a contradiction!

$(v) \Longrightarrow (i)$ is evident. □

14. 3. 4 Corollary. *For a right normal d-monoid $\mathfrak{S}$ the following are pairwise equivalent:*

(*i*) *Any positive a is of finite height.*

(*ii*) *Any upper bounded orthogonal set is finite.*

(*iii*) *Any z-ideal is a polar.*

Inspired by 14.3.3 we give:

14. 3. 5 Definition. A right normal d-monoid is called *ortho-finite*, if any upper bounded orthogonal set is finite.

14. 3. 6 Proposition. *Let $\mathfrak{S}$ be a right normal d-monoid. Then the following are pairwise equivalent:*

(*i*) *$\mathfrak{S}$ contains a finite base.*

(*ii*) *$\mathfrak{S}$ is equal to some $a^{\perp\perp}$ with an element a of finite height.*

(*iii*) *$\mathfrak{S}$ has only finitely many minimal prime c-ideals.*

(*iv*) *$\mathfrak{S}$ has only finitely many polars.*

(*v*) *Any orthogonal set of $\mathfrak{S}$ is finite.*

PROOF. $(i) \Longrightarrow (ii)$. Consult the preceding developments and 14.3.2.

$(ii) \Longrightarrow (iii)$ is again a consequence of 14.3.2.

$(iii) \Longrightarrow (iv)$, since any polar is the intersection of minimal prime c-ideals.

$(iv) \Longrightarrow (v)$, since, along with the elements a_i also the *bipolars* ${a_i}^{\perp\perp}$ are pairwise orthogonal.

$(v) \Longrightarrow (i)$. Choose a maximal orthogonal set $\{a_i\}$ $(1 \leq i \leq n)$ and put $a_1 \vee \ldots \vee a_n =: a$. This leads to $S = a^{\perp\perp}$ by 14.3.2. □

14.4 Projectable d-Monoids

14. 4. 1 Definition. A d-monoid $\mathfrak{S}$ is called *projectable*, if it satisfies:

(PR) $$a^\perp \times a^{\perp\perp} \;=\; S \;\; (\forall a \in S)\,,$$

that is if $\mathfrak{S}$ can be projected to any $a^{\perp\perp}$.

Furthermore $\mathfrak{S}$ is called *semi-projectable*, if $\mathfrak{S}$ satisfies:

(SP) $$(a \wedge b)^\perp \;=\; a^\perp \vee b^\perp\,.$$

14. 4. 2 Proposition. *Let $\mathfrak{S}$ be a projectable right normal d-semigroup. Then $\mathfrak{S}$ is also semi-projectable.*

PROOF. Choose some $a\,,\, b \in S$. Then it holds $a^\perp \times a^{\perp\perp} = S = b^\perp \times b^{\perp\perp}$ and thereby $a^\perp \vee a^{\perp\perp} = S = b^\perp \vee b^{\perp\perp}$. This implies

$$(a^\perp \vee b^\perp) \vee (a^{\perp\perp} \cap b^{\perp\perp}) = S = (a^\perp \vee b^\perp) \vee (a \wedge b)^{\perp\perp}$$

with 1-disjoint components.

Hence we get further $S = (a^\perp \vee b^\perp) \cdot (a \wedge b)^{\perp\perp}$ and thereby

$$a^\perp \vee b^\perp = (a \wedge b)^{\perp\perp\perp} = (a \wedge b)^\perp\,. \qquad \square$$

14. 4. 3 Proposition. *Any right normal projectable d-monoid is* representable .

PROOF. By definition we get $s \cdot a^\perp = a^\perp \cdot s$. Consider now

$xay \wedge ubv = x(a \wedge b)a^\circ y \wedge u(a \wedge b)b^\circ v$ with $a^\circ \in b^\perp, b^\circ \in a^\perp$. Then there are elements $a^* \in b^\perp, b^* \in a^\perp$ with

$$\begin{aligned} xay \wedge ubv &= x(a \wedge b)ya^* \wedge u(a \wedge b)vb^* \\ &\leq (x(a \wedge b)y \vee u(a \wedge b)v)(a^* \wedge b^*) \\ &\leq xby \vee uav\,. \end{aligned}$$

Thus according to the remark below 6.1.2 the proof is complete. $\square$

Semi-projectable d-monoids are defined by notions on polars. Corresponding to this definition we get for prime c-ideals

14. 4. 4 Proposition. *A right normal d-monoid $\mathfrak{S}$ is semi-projectable iff any proper prime c-ideal contains one and only one minimal prime c-ideal, namely* $\bigcup x^\perp \ (x \notin P) =: N$.

PROOF. Let $\mathfrak{S}$ be semiprojectable and let P be properly prime and containing the minimal primes A, B. Then there are elements a, b satisfying $a \in A\backslash B,\ b \in B\backslash A$, whence even an orthogonal pair $a^\circ \in A\backslash B,\ b^\circ \in B\backslash A$ exists with $a^{\circ\perp} \subseteq B$ and $b^{\circ\perp} \subseteq A$. But this leads to

$$S = (a^\circ \wedge b^\circ)^\perp \ = \ a^{\circ\perp} \vee b^{\circ\perp} = P$$

a contradiction! Hence the condition is necessary.

Now we show, that the condition is sufficient. To this end, observe, that it always holds $a^\perp \vee b^\perp \subseteq (a \wedge b)^\perp$. Suppose next that $x \notin a^\perp \vee b^\perp$ and let P be a value of x with $P \supseteq a^\perp \vee b^\perp$. Then – according to 13.4.2 – the union $N = \bigcup x^\perp \ (x \notin P)$ is the uniquely determined minimal prime c-ideal, contained in P. Since $a^\perp$ and $b^\perp$ are contained in P, it further follows $a\,,\, b \notin N$, that is $a \wedge b \notin N$ and thereby $(a \wedge b)^\perp \subseteq N \subseteq P$. So, by $x \notin P$ we are led to $x \notin (a \wedge b)^\perp$. Hence it holds condition **(SP)**. $\square$

It is our next aim to characterize the class of projectable d-monoids like we did w. r. t. the class of semi-projectable d-monoids.

14. 4. 5 Proposition. *Let P be a proper prime c-ideal. Then the union of all prime z-ideals, contained in P, is equal to the set of all $p \in P$ with $p^{\perp\perp} \subseteq P$.*

PROOF. Let p belong to some prime z-ideal, contained in P. Then by definition it follows $p^{\perp\perp} \subseteq P$. So, it remains to show that for each $p \in P$ with $p^{\perp\perp} \subseteq P$ there exists a prime z-ideal $Z \subseteq P$ with $p \in Z$.

To this end we define $\mathcal{F} := \{x^{\perp\perp} \,|\, x \notin P\}$. Then $\mathcal{F}$ forms a filter in the lattice of all bipolars of $\mathfrak{S}$, not containing $p^{\perp\perp}$. Hence, we are in the position to extend $\mathcal{F}$ to some maximal filter $\mathcal{H}$ of this type. We define furthermore $Z := \{z \,|\, z^{\perp\perp} \notin \mathcal{H}\}$ and shall verify, that this Z fits.

First we verify that Z is closed under the relevant operations. This is evident w. r. t. all operations except for the multiplication. So, choose some $a\,,\, b \in Z$.

Then w. r. t. multiplication we get:

$$\begin{array}{rcl} a, b \in Z & \rightsquigarrow & a^{\perp\perp}, b^{\perp\perp} \notin \mathcal{H} \\ & \Longrightarrow & \\ \exists\, x^{\perp\perp}, y^{\perp\perp} \in \mathcal{H} : & & a^{\perp\perp} \cap x^{\perp\perp} \subseteq p^{\perp\perp} \supseteq b^{\perp\perp} \cap y^{\perp\perp}, \end{array}$$

which, on the grounds of $s^{\perp\perp} = |\, s \,|^{\perp\perp}$ leads to

$$(ab)^{\perp\perp} \cap (|\, x \,| \wedge |\, y \,|)^{\perp\perp} \;=\; (a^{\perp\perp} \vee b^{\perp\perp}) \cap (x^{\perp\perp} \cap y^{\perp\perp}) \subseteq p^{\perp\perp}$$

and thereby to $(ab)^{\perp\perp} \notin \mathcal{H}$, that is $ab \in Z$. Hence Z is closed w. r. t. to its operations.

But, furthermore Z is a subset of P, because

$$z \in Z \Longrightarrow z^{\perp\perp} \notin \mathcal{H} \Longrightarrow z^{\perp\perp} \notin \mathcal{F} \Longrightarrow z \in P\,.$$

Thus Z is a prime z-ideal with $p \in Z \subseteq P$. □

Now we are in the position to show:

14. 4. 6 Proposition. *A right normal d-monoid $\mathfrak{S}$ is projectable iff any proper prime c-ideal P contains one and only one prime z-ideal, namely $N := \bigcup x^{\perp}$ $(x \notin P)$.*

PROOF. Let $\mathfrak{S}$ be projectable. Let Z be a prime sub-z-monoid of P. Then it holds $a \notin P \Longrightarrow a^{\perp} \subseteq Z$ and thereby furthermore $N \subseteq Z$. We consider some z with $1 \leq z \in Z$ and some s with $1 \leq s \notin P$. Then it holds $s = u \cdot v$ for some $u \in z^{\perp}, v \in z^{\perp\perp} \subseteq Z \subseteq P$ and thereby with $u \notin P$, which further leads to $z \in u^{\perp} \subseteq N$. Consequently it holds $Z = N$, whence the above condition is necessary.

The above condition is sufficient. For, if $a^{\perp} \times a^{\perp\perp} \neq S$, then there exists a proper $a^{\perp} \times a^{\perp\perp}$, and hence some $a^{\perp} \times a^{\perp\perp}$ containing proper prime c-ideal P. Consequently, if Z is the uniquely determined prime z-ideal contained in P, we get $a \in a^{\perp\perp} \subseteq Z \subseteq P$, and by assumption there must exist some $b \notin P$ with $a \in b^{\perp}$, whence we would get $b \notin P$ & $b \in a^{\perp} \subseteq P$, a contradiction! □

14.5 Lateral Completeness

14. 5. 1 Definition. A d-monoid is called *laterally complete*, if any orthogonal subset has a least upper bound.

Laterally complete is, for instance, any right normal d-monoid with finite base.

14. 5. 2 Proposition. *Let a d-monoid $\mathfrak{S}$ be a semigroup of ideal/filter isomorphisms. Then $\mathfrak{S}$ is laterally complete.*

PROOF. Let $\{\phi_i\}$ $(i \in I)$ be orthogonal. Then the *carrier* $T(\phi_i)$, that is the fixpoint-free components of the domains, are pairwise disjoint. We put $x\phi = x$, if $x \notin \bigcup T(\phi_i)$, and $x\phi = x\phi_i$ otherwise. Then it follows $\phi = \sup(\{\phi_i\})$. □

Thus we get:

14. 5. 3 Corollary. *Any right normal d-monoid admits an embedding into a laterally complete right normal d-monoid.*

Furthermore it holds:

14. 5. 4 Corollary. *Any direct product of linearly ordered d-monoid is laterally complete. Consequently any representable d-monoid admits a laterally complete extension.*

Finally we get:

14. 5. 5 Proposition. *A right normal d-monoid is a direct product of linearly ordered d-monoids iff it has a base, is projectable and is laterally complete.*

PROOF. It is nearly obvious, that any direct product of linearly ordered d-monoids satisfies the above conditions.

On the other hand, if the above conditions do hold, and $\{a_i\}$ $(i \in I)$ is a base, then $\mathfrak{S}$ is subdirectly decomposed by its polars ${a_i}^{\perp}$. Hence, in this case $\mathfrak{S}$ admits also a subdirect decomposition into the factors ${a_i}^{\perp\perp}$. But, each element of the direct product is supremum of the orthogonal set of its projections, and, by assumption $\mathfrak{S}$ is laterally complete. This means that $\mathfrak{S}$ is isomorphic with the direct product $\bigotimes\limits_{i \in I} {a_i}^{\perp\perp}$. □

Chapter 15

Real extensions

Real d-semigroups were introduced in the chapter on strictly archimedean d-semigroups. Here we will study subdirect products of these special types of d-semigroups.

15.1 Subdirect real Products

In this section we turn to the question, when an arbitrary d-semigroup admits an embedding into an extended cube, that is into some direct product of factors of type $\mathfrak{R}^\bullet$ or $\mathfrak{E}$ or $\mathfrak{E}^\bullet$.

15. 1. 1 Definition. Let $\mathfrak{S}$ be a d-semigroup and let J be an ideal of $\mathfrak{S}$. We call J *real archimedean*, if J satisfies:

$$u \cdot t^n \cdot v \in J \;\; (u, v \in S\,, \forall n \in \mathbf{N}) \;\&\; a \cdot b \in J \quad \Longrightarrow \quad a \cdot t \cdot b \in J.$$

Let now $\mathfrak{S}$ be as above and let F be a filter. We call F *real primary,* if F satisfies:

$$a \cdot t \cdot b \in F \quad \Longrightarrow \quad a \cdot b \in F \vee u \cdot t^n \cdot v \in F \;\; (\forall\, u, v \in S, n \in \mathbf{N})\;.$$

Obviously J is an irreducible real archimedean ideal iff its complement $S \backslash J$ is a real primary filter.

15. 1. 2 Proposition. *Let $\mathfrak{S}$ be a d-semigroup. Then the following are pairwise equivalent:*

(i) $\mathfrak{S}$ *is a subdirect product of real d-semigroups.*

(*ii*) $\mathfrak{S}$ *is a subdirect product of linearly ordered d-semigroups.*

(*iii*) *Any principal ideal is the intersection of irreducible real archimedean ideals.*

(*iv*) *Any principal ideal is the intersection of irreducible real primary filters.*

PROOF. $(i) \Longrightarrow (ii)$ is evident.

$(ii) \Longrightarrow (i)$ is equivalent to 9.3.8.

$(i) \vee (ii) \Longrightarrow (iii)\ \&\ (iv)$.

Let $\mathfrak{S}$ be a subdirect product of real d-semigroups. Then for each pair $a < b$ there exists an index i with $i(a) < i(b)$, and the ideal $P_i := \{x \mid i(x) \leq i(a)\}$ is irreducible and real archimedean. Dually the filter $F_i := \{x \mid i(x) \geq i(b)\}$ is irreducible and real primary. Hence there are enough ideals and enough filters, in order to verify (iii) and to verify (iv).

$(iii) \Longleftrightarrow (iv)$ follows nearly by definition 15.1.1. Observe: If I is an archimedean ideal, separating the elements a and b, then $S\backslash I$ is a primary filter separating a and b.

$(iii) \vee (iv) \Longrightarrow (i)\ \&\ (ii)$.

Let (iii) be satisfied. Then $\mathfrak{S}$ is archimedean and thereby commutative. For, in fact, $t \in \mathfrak{S}^+\ \&\ t^n \leq a\ (\forall n \in \mathbf{N})\ \&\ a < at$ would lead to the existence of some irreducible archimedean ideal P with $a \in P$ and thereby to $t^n \in P\ (\forall n \in \mathbf{N})$, but $at \notin P$.

Let now P be an irreducible real archimedean ideal of $\mathfrak{S}$ and suppose that $\overline{t}^n \leq \overline{c}\ (\forall n \in \mathbf{N})$ belong to $\overline{\mathfrak{S}} := \mathfrak{S}/P$. Then we get

$$(c \cdot s \in P \Rightarrow 1 \cdot t^n \cdot s \in P\ \ (\forall n \in \mathbf{N})) \implies (c \cdot s \in P \Rightarrow ct \cdot s \in P),$$

which leads to $\overline{c}\cdot\overline{t} = \overline{c}$. Thus we get $(iii) \Longrightarrow (ii)$ and thereby the implication $(iii) \Longrightarrow (i)\ \&\ (ii)$. □

We come back to 11.2.4 There it is shown that super-archimedean d-monoids are closely related to real function algebras. Moreover it turned out that super-archimedean d-semigroups always admit a subdirect decomposition into the factors $\mathfrak{C}(t)$ and $\mathfrak{S}/C(t)$, and it has been mentioned already that super-archimedean d-semigroups are representable. Here we will show, that right normal d-monoids satisfy much more, namely:

15. 1. 3 Proposition. *Let $\mathfrak{S}$ be a right normal d-monoid. Then the following are pairwise equivalent:*

(*i*) *$\mathfrak{S}$ is super-archimedean.*

(*ii*) *$\mathfrak{S}$ has a subdirect decomposition into real factors, such that the representing real functions satisfy:*

$$\forall f, g \geq id\ \exists n \in \mathbf{N} : \quad f(x)^n \geq g(x) \ \ (\forall x : f(x) > 0)\,.$$

(*iii*) *Any prime c-ideal is minimal.*

(*iv*) *Any $t \in S$ satisfies $\mathfrak{S} = \mathfrak{C}(t) \times \mathfrak{C}(t)^{\perp}$.* [1)]

PROOF. $(i) \Longrightarrow (ii)$. Recall that commutative subdirectly irreducible d-semigroups are 0-cancellative and that

$$\overline{t}^n < \overline{a} \ \ (\forall\, n \in \mathbf{N}) \Longrightarrow \exists\, m : (\overline{t}^m)^2 = \overline{t}^m\,.$$

$(ii) \Longrightarrow (iii)$. First $\mathfrak{S}$ is super-archimedean, according to (ii), as is easily seen.

Furthermore any prime c-ideal P contains a minimal prime c-ideal M. Assume now $M \neq P$. Then there exists an element $x \in S^+ \backslash P$, satisfying for any $y \in P^+$ in $\mathfrak{S}/M =: \overline{\mathfrak{S}}$

$$\overline{x} > \overline{y}^n \geq \overline{1} \ \ (\forall\, n \in \mathbf{N})\,.$$

But this leads to $\overline{y} = \overline{1}$, whence it results $y \in M$ and thereby $P = M$.

$(iii) \Longrightarrow (iv)$. Let $\mathfrak{C}(t) \times \mathfrak{C}(t)^{\perp} \neq \mathfrak{S}$ be satisfied. Then the direct product $\mathfrak{C}(t) \times \mathfrak{C}(t)^{\perp}$ is contained in a minimal prime c-ideal of $\mathfrak{S}$. But according to 13.4.2 any minimal prime c-ideal P of $\mathfrak{S}$ is of type $P = \bigcup x^{\perp} \ \ (x \notin P)$, a contradiction w. r. t. $t^{\perp} \subseteq P \ \&\ t \in P$!

$(iv) \Longrightarrow (i)$ finally, results nearly immediately. □

15.2 Direct real Sums

Next we turn to sums of real d-monoids.

15. 2. 1 Proposition. *Let $\mathfrak{S}$ be a d-monoid. Then the following are pairwise equivalent:*

[1)] In fact, in this case $\mathfrak{S}$ is even hyper normal.

(*i*) $\mathfrak{S}$ *is a direct sum of real d-monoids.*

(*ii*) *The c-ideal lattice of* $\mathfrak{S}$ *is boolean.*

(*iii*) $\mathfrak{S}$ *is ortho-finite and satisfies* $\mathfrak{S} = \mathfrak{C}(t) \times \mathfrak{C}(t)^{\perp}$.

PROOF. $(i) \Longrightarrow (ii)$ is nearly evident.

$(ii) \Longrightarrow (iii)$. If the c-ideal lattice is boolean, then any c-ideal is a direct factor.

But, $\mathfrak{S}$ is also ortho-finite, since $\mathfrak{C}(M)$ cannot be a direct factor, if M is an infinite set of pairwise orthogonal elements, upper bounded by $a \in S$, since otherwise we would get $a = a_1 \cdot a_2$ with $a_1 \in \mathfrak{C}(M)$ & $a_2 \in \mathfrak{C}(M)^{\perp}$ whence a_1 in this case would satisfy $a_1 \in \mathfrak{C}(M)$ & $a_1 \geq \mathfrak{C}(M)$.

$(iii) \Longrightarrow (i)$. Any $\mathfrak{C}(t)$ is a direct factor, therefore $\mathfrak{S}$ is super-archimedean, according to 11.2.4, whence $\mathfrak{C}(t)$ is archimedean.

Furthermore $\mathfrak{S}$ is normal. To get this, we start from $R(a,b,a',b')$ with positive elements a', b' . Then it follows $b' = b_1{}' \cdot b_2{}'$ with $b_1{}' \in C(a')$ and $b_2{}' \in C(a')^{\perp}$. This implies $b_1{}' \leq a'^{\,n}\,(\exists n \in \mathbf{N})$, which – by $x \leq ab \Longrightarrow x = x_1 \cdot x_2$ with $x_1 \leq a$, $x_2 \leq b$ – leads to $b_1{}' = b_{1,1}{}' \cdot b_{1,2}{}' \cdot \ldots \cdot b_{1,n}{}'$ with $b_{1,i}{}' \leq a' \wedge b'$ $(1 \leq i \leq n)$. Thus we get $(a \wedge b)b_1{}' = a \wedge b$ and thereby $(a \wedge b)a' = a$ & $(a \wedge b)b_2{}' = b$ with $a' \perp b_2{}'$.

Suppose now $1 < x, y < a^n$ & $x \not\leq y \not\leq x$. Then there would exist coprime elements $x^{\circ}, y^{\circ} \notin \{1\}$, whence $\mathfrak{C}(a)$ would admit a direct decomposition, say $\mathfrak{C}(x^{\circ}) \times \mathfrak{D}$. But this would lead to $\mathfrak{C}(a) = \mathfrak{C}(a_1) \times \mathfrak{C}(a_2)$, with $a_1 \perp a_2$, and thereby – after finitely many repetitions of the procedure – provide a direct decomposition $\mathfrak{C}(a) = \bigotimes \mathfrak{C}(x_i)$, where the direct factors $\mathfrak{C}(x_i)$ would be directly indecomposable and thereby linearly ordered. But $\bigotimes \mathfrak{C}(x_i)$ is unique, according to 13.5.11. Hence only finitely many linearly ordered $\mathfrak{C}(x)$ with $a \wedge x \neq 1$ are possible.

Thus, by the set of the linearly ordered $\mathfrak{C}(x)$, we get a family of strictly archimedean components in the sense of (*i*) . □

15.3 A general Cube Theorem

Recall: $\mathfrak{P}_1$ is the d-semigroup with carrier $\mathbf{E}$ and $a \circ b := \min(1, a+b)$ and $a \wedge b := \min(a,b)$. Hence ${\mathfrak{P}_1}^I$ is the $|\,I\,|$-dimensional cube, under pointwise

$\cdot$ and $\wedge$.

Furthermore: $\mathfrak{S}_n$ is formed by $S_n := \{0, 1, \ldots, n\}$ under the above operations, where n acts in the sense of 1 .

Obviously any $\mathfrak{S}_n$ is a sub-d-semigroup of $\mathfrak{P}_1$.

We wish to characterize *cube-semigroups*, i. e. those d-semigroups, which admit an embedding into some ${\mathfrak{P}_1}^I$. To this end we recall first that any positive d-semigroup has a natural extension by its filters or – equivalently – by its d-ideals. These extensions are not necessarily d-semigroups, but at least they are *cdl*-semigroups w. r. t. to the complex operations. Moreover any d-semigroup has a further natural extension by its v-ideals, which again need not be a d-semigroup, but which may be considered as a natural *infimum extension*. This suggests to characterize cube-semigroups by the interplay between d- and v-ideals. To this end, w. l. o. g. we may, of course, start from positive d-monoids.

15. 3. 1 Proposition. *A positive d-monoid $\mathfrak{S}$ is a cube-semigroup if and only if it satisfies for any filter A the implication:*

(CE) $$A^n \supseteq \mathsf{b} \ \ (\forall n \in \mathbf{N}) \Longrightarrow \mathfrak{a} \cdot \mathsf{b} = \mathsf{b} = \mathsf{b} \cdot \mathfrak{a}$$

PROOF. Necessity: If $\mathfrak{S}$ is embedded in ${\mathfrak{P}_1}^I$, for any $i \in I$ with $i(b) < 1$ we get
$$\inf(i(a)) \ \ (a \in A) = 0 \ ,$$
since otherwise there would exist some $\varepsilon > 0$ satisfying $i(a) \geq \varepsilon$ $(\forall\, a \in A)$, that is an $n \in \mathbf{N}$ with $i(x) > i(b)$ $(\forall\, x \in A^n)$, a contradiction, since proposition (2.4.1) implies

$$b \in A^n \leadsto b \geq {a_1}^n \wedge \ldots \wedge {a_k}^n = (a_1 \wedge \ldots \wedge a_k)^n \ \ (\exists a_i \in A, k \in \mathbf{N}).$$

This means furthermore

$$i(s) \leq i(a) + i(b) + i(t) \ \ (\forall\, a \in A) \quad \Longrightarrow \quad i(s) \leq i(b) + i(t) \ ,$$

that is $s \,|\, Ab \cdot t \Longrightarrow s \,|\, b \cdot t$ and thereby $\mathfrak{a} \circ \mathsf{b} = \mathsf{b} = \mathsf{b} \circ \mathfrak{a}$.

Sufficiency: First of all we get immediately that $\mathfrak{S}$ is archimedean, and thereby commutative. Let now $a < b$ be a critical pair. We consider the subsequent cases:

Case 1: $\exists\, x : \ ax \leq b \ \ \& \ \ ax \neq ax^2$
Case 2: $ax \leq b \ \Rightarrow \ ax = ax^2$.

As to Case 1: Obviously there is no e satisfying $ae = ax = axe$, since otherwise $ax = aex = ax^2$ would follow. Therefore we are through, if we are able to separate a and ax by $\overline{\mathfrak{S}} := \mathfrak{S}_{ax}/E(ax)$. So we may start from a completely integrally closed brick, recall 8.1.4.

To this end we prove a bit more by starting from an archimedean complementary d-semigroup $\mathfrak{S}$ with 0, and showing that $\mathfrak{S}$ admits some a , 0 separating d-semigroup homomorphism onto $\mathfrak{P}_1$. This will be done in the following by transferring the problem to the case $a^2 = 0$:

If $a^2 \neq 0$ holds, in case of $a \leq s \neq s^2 \neq s^3$ we turn to $\mathfrak{S}_{s^2}/E(s^2)$, in order to separate thus s and s^2, whereas in case of $a \leq s \Longrightarrow s^2 = s^3$ the mapping $\phi : z \longmapsto (az)^2$ provides a homomorphism of $(S, \cdot, \wedge)$ onto a distributive lattice, which leads to some a , 0 separating 2-element image, recall $(x \wedge y)^2 = x^2 \wedge y^2$.

So, let $\mathfrak{S}$ be archimedean, complementary and *bounded*, and let furthermore $a \neq a^2 = 0$ be satisfied. Then it holds $p := a * 0 \leq a$, and this yields a pair $x \in S$, $n \in \mathbf{N}$ with $p^n x = a$ & $p^{n+1} \not\leq a$, since $pa \neq a$.

We define $\overline{\mathfrak{S}}_1 := \mathfrak{S}/E(a)$. Here it results $\overline{p} * \overline{x} \wedge \overline{x} * \overline{p} = \overline{1}$. For it holds $(p \wedge x)(p * x \wedge x * p) = p \wedge x$, that is $p * x \wedge x * p \in E(a)$, and it holds $\overline{x} * \overline{p} \neq \overline{1}$, since otherwise it would follow $p^n x(x * p) = a(x * p) = a \rightsquigarrow p^{n+1} \leq a$. Hence the set $\overline{Y} := \{\overline{y} \,|\, \overline{x} * \overline{p} \wedge \overline{y} = \overline{1}\}$ forms a c-ideal in $\overline{\mathfrak{S}}_1$, according to 2.7.2, containing $\overline{p} * \overline{x}$, but not containing $\overline{p}$. Consequently in $\mathfrak{S}$ there exists a c-ideal M with $p * x \in M$ & $p \notin M$, which is maximal among all c-ideals with this property. But then $\mathfrak{S}/M$ cannot contain any proper c-ideal, and since $p^{n+2} \equiv p^n pp(p * x) \equiv p^n px(x * p) \equiv 0\,(M)$ and since together any proper c-ideal of $\mathfrak{S}/M$ must contain $\overline{p}$.

We consider $\overline{\mathfrak{S}}_2 := \mathfrak{S}/M$. Here we get first $\overline{t} \neq \overline{1} \Longrightarrow \exists\, n \in \mathbf{N} : \overline{t}^n = \overline{0}$. Suppose now $\overline{u} \neq \overline{0} \neq \overline{v}$ and $(\overline{u} \wedge \overline{v})\overline{u}\,' = \overline{u}$, $(\overline{u} \wedge \overline{v})\overline{v}\,' = \overline{v}$. Then we get next $\overline{u}\,' \wedge \overline{v}\,' = \overline{1}$, because $(\overline{u} \wedge \overline{v})(\overline{u}\,' \wedge \overline{v}\,') = \overline{u} \wedge \overline{v}$ and $E(\overline{u} \wedge \overline{v}) = \{\overline{1}\}$. But – according to 2.7.2 – in case of $\overline{v}\,' \neq \overline{1}$ this implies $\overline{u}\,' = \overline{u}\,' \wedge \overline{0} = \overline{u}\,' \wedge \overline{v}\,'^m = \overline{1}$, whence $\overline{\mathfrak{S}}_2$ is linearly ordered .

Hence – in Case 1 – $\mathfrak{S}$ is strictly archimedean, that is a sub-d-semigroup of $\mathfrak{P}_1$ – recall Hölder/Clifford.

AS TO CASE 2: We consider the different situations;

(a) $a^2 \wedge b = a$

(b) $a^2 \wedge b \neq a$.

Ad **(a)**. $\overline{\mathfrak{S}} := \mathfrak{S}_b$ is an image, in which $\overline{a} = \overline{a}^2$ is satisfied and thereby – we are studying case 2 – $(\overline{a} \cdot \overline{x})^2 = \overline{a} \cdot \overline{x}$ for all $\overline{a} \cdot \overline{x}$. But, by $\overline{\mathfrak{S}} \cdot \overline{a}$ this provides a distributive lattice as homomorphic image, from which we get again some a, b separating 2-element image.

Ad **(b)** Let $b = ay$, that is $a^2 > a^2 \wedge b = a(a \wedge y) =: c > a$. Then a and b are separated if a and c are separated. So we may start from $a < c \leq a^2$, in order to separate a and c.

This means in a first step, that the filter $X := \{x \mid ax \geq c\}$ cannot be idempotent since $a \in X^n$ would imply $\mathsf{a} = \mathsf{a}\mathfrak{x} = \mathsf{c}$. Therefore X must contain at least one $p \leq a$, which cannot be decomposed into two factors belonging to X, that is, which satisfies:

$$p = qr \ \&\ aq \geq c \Longrightarrow ar \not\geq c \, , \tag{15.2}$$

and we may assume $ap = c$, since this property is carried over to all $p_i \leq p$ with $ap_i \geq c$. Furthermore we may assume, that no $p_i \leq p$ has a higher exponent in a than p. Otherwise we could form a chain $p > p_1 > \ldots > p_m > \ldots$ in such a way that each $n \in \mathbf{N}$ would be majorized by some exponent of some p_i in a, and this would mean that a would belong to any power of the filter generated by the elements p_i, that is, we would get $\mathsf{a} = \mathsf{a} \circ \mathsf{p} = \mathsf{c}$, a contradiction.

Let now p be of the above type, in particular let $p^n x = a \ \&\ p \not\leq x$ be satisfied and define:

$$U := \{e \mid p = eq \ \&\ aq \geq c \ \ (\exists q \in S)\} \, . \tag{15.3}$$

Then p cannot divide any xe with $e \in U$, since this, in case of $(p \wedge x)p' = p$, would lead to

$$p \leq xe \Longrightarrow p = (p \wedge x)(p' \wedge e) = (p \wedge x)f(\text{with } f := p' \wedge e \in E) \, . \tag{15.4}$$

But because $f \leq e$ from this would follow the existence of some g with $fg = p \ \&\ ag \geq c$ leading – in case of $(p \wedge x \wedge g) \cdot g' = g$ – to the equation

$$p = fg = f(p \wedge x \wedge g)g' \overset{(15.4)}{=} fgg' \wedge fgg' = pg' \, . \tag{15.5}$$

Consequently, by $p \leq a$, we finally would get

$$a(p \wedge x) \geq a(p \wedge x \wedge g) = a(p \wedge x \wedge g)g' = ag \geq c \tag{15.6}$$

and thereby $p \wedge x \in X$, although the exponent of $p \wedge x$ in a is less than or equal to the exponent of p in a, a contradiction.

Now we consider the c-ideal I, generated by U. We shall show first, that the complex product aU is equal to the complex product aI:

By definition, U is an order ideal, that is U satisfies $x \leq u \in U \Longrightarrow x \in U$.

Furthermore U is even a lattice ideal. For, together with u and v also $u \vee v$ belongs to U, observe

$$\begin{matrix} us = p \ \&\ as \geq c \\ \\ vt = p \ \&\ at \geq c \end{matrix} \quad \Longrightarrow \quad (u \vee v)(s \wedge t) = p \ \&\ a(s \wedge t) \geq c\,. \tag{15.7}$$

But it holds $a(u \wedge v) \leq c$, because $ap = c$ and $u, v \leq p$, and from this it results (we are studying Case 2)

$$a(u \wedge v) = a(u \wedge v)^2 \tag{15.8}$$

and thereby

$$a \cdot uv = a(u \wedge v)(u \vee v) = a(u \vee v)\,, \tag{15.9}$$

that is $aI = aU$. In particular this means, that not only $p \not\leq xe \ \ (\forall e \in U)$, as shown above, but that even $p \not\leq xe \ \ (\forall e \in I)$ is satisfied, that is that in $\overline{\mathfrak{S}} := \mathfrak{S}/I$ it holds $\overline{p} \not\leq \overline{x}$.

We study $\overline{\mathfrak{S}}$. First we get $\overline{p} = \overline{a} * \overline{c} = \overline{a} * \overline{ap}$. For in case of $\overline{a} \cdot \overline{y} \geq \overline{c}$, say $c \leq aye$, it follows $a(p \wedge ye) = c$ – i.e. $f(p \wedge ye) = p$ – with $f \in U$, leading to

$$p = (p \wedge ye)f \equiv p \wedge ye \equiv p \wedge y\,. \tag{15.10}$$

Consequently, $\overline{a} \cdot \overline{x} \geq \overline{c}$ cannot hold, since otherwise $p \leq xe \ (\exists e \in I)$ would follow, so if $\overline{J}$ is the c-ideal, generated by $\overline{x}$ in $\overline{\mathfrak{S}}$, then $\overline{p}$ cannot belong to $\overline{J}$, since $\overline{ax} \cdot \overline{x} = \overline{ax}$ – recall we are studying Case 2.

So, if $\overline{x} \in \overline{M}$ is valid for some maximal $\overline{M}$ in the set of c-ideals of $\overline{\mathfrak{S}}$ containing $\overline{x}$, but not containing $\overline{p}$, then $\overline{\mathfrak{S}}/\overline{M} =: \overline{\overline{\mathfrak{S}}}$ provides a decomposition with

$\overline{\overline{a}} \neq \overline{\overline{c}}$, in which $\overline{\overline{p}}$ is an atom satisfying $\overline{\overline{p}}^{\,m} = \overline{\overline{a}}$ & $\overline{\overline{c}} = \overline{\overline{p}}^{\,m+1}$, since in case of $\overline{\overline{1}} \neq \overline{\overline{z}} \leq \overline{\overline{p}}$ it must hold $\overline{\overline{z}} = \overline{\overline{p}}$, because otherwise – again, we are studying CASE 2 – it would result

$$\overline{p} = \overline{a} * \overline{c} \rightsquigarrow \overline{\overline{p}} = \overline{\overline{a}} * \overline{\overline{c}} \rightsquigarrow \overline{\overline{a}} \cdot \overline{\overline{z}} = \overline{\overline{a}} \cdot \overline{\overline{z}}^n \neq \overline{\overline{c}}\,, \tag{15.11}$$

that is a contradiction to the maximality of $\overline{M}$!

Hence, in this final case the d-semigroup $\overline{\overline{\mathfrak{S}}}$ is a homomorphic image of type $\mathfrak{S}_{m+1}$, separating the elements a and c. □

Proposition 15.3.1 implies nearly immediately:

15. 3. 2 Corollary. *Any $\bigwedge$-complete positive d-monoid is a cube semigroup.*

PROOF. Let A be a filter with $A^n \supseteq \mathsf{b}$. Then we get $\bigwedge A^n = (\bigwedge A)^n \leq b$, that is $(\bigwedge A)b = b$, and thereby $\mathfrak{a} \cdot \mathsf{b} = \mathsf{b} = \mathsf{b} \cdot \mathfrak{a}$. □

This implies furthermore

15. 3. 3 Proposition. *Let $\mathfrak{S}$ be a positive d-monoid. Then $\mathfrak{S}$ admits a complete extension, if $\mathfrak{S}$ admits an embedding into a cube ${\mathfrak{P}_1}^I$, and this is possible iff the set of (d-ideals), here the set of filters, satisfies*

$$A^n \supseteq \mathsf{b} \;\; (\forall n \in \mathbf{N}) \Longrightarrow \mathfrak{a} \cdot \mathsf{b} = \mathsf{b} = \mathsf{b} \cdot \mathfrak{a} \tag{CE}$$

The reader should take into account that thereby a positive d-semigroup, admitting a complete d-semigroup extension what kind ever, admits even an optimal such extension, that is a complete extension satisfying all rules of distributivity, stated so far.

15.4 Continuous Cube Extensions

On the one hand theorem 15.3.1 in a certain sense is satisfactory, on the other hand, central questions remained open, of course, above all, under which conditions existing bounds are respected.

15. 4. 1 Proposition. *A positive $\bigwedge$-complete d-monoid $\mathfrak{S}$ admits a continuous cube extension, if for any pair a, b with $b \not\leq a$ there exists a $\vee$-irreducible element p with $p \leq b$ & $p \not\leq a$.*

PROOF. **(a)** If $\mathfrak{S}$ admits an embedding in the sense of the proposition, then there exists an index i with $i(b) > i(a)$. But then $p = \bigwedge x\ (i(x) \geq i(b))$ is $\vee$-irreducible with $p \leq b\ \&\ p \not\leq a$.

(b) Suppose now $a < b$ and w. l. o. g. $\mathfrak{S} = \mathfrak{S}_b$. Since p is $\vee$-irreducible the relation

(15.13) $$u \equiv v\ (p)\ :\Longleftrightarrow\ ux \geq p \Leftrightarrow vx \geq p$$

defines an S-respecting congruence, which proves to be linearly ordered – recall 6.1.2 – since p is $\vee$-irreducible.

Let now $\mathfrak{S} = \mathfrak{S}_b$ be as above, but linearly ordered.

We consider the set of all x with $x^n \neq b\ (\forall n \in \mathbf{N})$. This set obviously forms a prime c-Ideal P, and it is easily checked that the decomposition according to this P provides an a, b separating homomorphic image of the required type. □

As an implication we get:

15. 4. 2 Corollary. *Any* infimum-algebraic *d-monoid* $\mathfrak{S}$ *, admits an infimum respecting embedding into some cube.*

PROOF. Let c be compact and suppose $a \leq c\ \&\ b \not\leq c$. Then the infimum p of any b containing maximal chain $b_i\ (i \in I)$ with $b_i \not\leq c\ (\forall i \in I)$ is a $\vee$-irreducible element with $p \leq b\ \&\ p \not\leq a$, since by the chain maximality on the one hand and the compactness property of c on the other hand we get $u, v < p \Longrightarrow u, v \leq c \Longrightarrow u \vee v \leq c < p.$ □

Next we characterize the complete sub-d-semigroups of the cube.

15. 4. 3 Proposition. *A positive conditionally complete d-monoid* $\mathfrak{S}$ *is a complete sub-d-semigroup of some cube iff it satisfies* (SVD)*, meaning the joint axioms* (S), (V) *and* (D)*, and in addition any proper interval of* $I(S)$ *has a* jump.

PROOF. NECESSITY : Let $\mathfrak{S}$ admit an embedding in the sense of the theorem. Then, by evidence, condition (SVD) is satisfied. Furthermore in case of $a < b\ \&\ a = a^2, b = b^2$ it holds at least at one place $i \in I\ i(a) = 0\ \&\ i(b) = 1$, whence the elements

$$\begin{aligned} u &:= \bigwedge x\ \ (\, i(x) = 1\ \ \&\ \ x = x^2 \geq a\,) \\ v &:= \bigvee y\ \ (\, i(y) = 0\ \ \&\ \ y = y^2 \leq b\,) \end{aligned}$$

provide a jump $[\,u \wedge v, u\,]$ in $I(S)$.

SUFFICIENCY: We may suppose that $\mathfrak{S}$ is a monoid and start from $a < b$. Furthermore $E(a)$ may be supposed to contain only the identity, since $E(a)$ has in any case an idempotent maximum through which we otherwise could divide. So we get $a = 1$ or $a < a^2$.

Now we consider the situation $1 \leq a \leq x \leq x^2$ & $x \leq b$.

Here we are through, if b is an atom or if all x with $1 < x < b$ are idempotent, because of the gap-requirement.

Otherwise we are through once we have settled the case $c < c^2$ & $c \leq b$ that is w.l.o.g. the case $a < a^2$ & $a \leq b$. So we have to settle

CASE 1: $a^2 \wedge b = a$

CASE 2: $a^2 \wedge b \neq a$.

AS TO CASE 1: $b = ax$ implies $a = a(a \wedge x)$, that is $a \wedge x = 1$. Thus we get in $\overline{\mathfrak{S}} := S_{x^2}$ first $\overline{a} = \overline{1}$ and $\overline{x} \leq \overline{b}$, and the classes $\overline{a}$ and $\overline{b}$ can be separated, if all y between 1 and x are idempotent. So, in CASE 1 we may even start from some $\mathfrak{S}_{y^2}$, satisfying $\overline{1} = \overline{a} \leq \overline{y} < \overline{y}^2 \leq \overline{b} = \overline{0}$ and (SVD).

AS TO CASE 2: Let again $b = ax$. Then we get $a < c := a(a \wedge x) \leq a^2$, whence we may start from some $\mathfrak{S}_c$, satisfying $\overline{1} < \overline{a} < \overline{a}^2 = \overline{c} = \overline{0}$ and (SVD).

So, we are through, if we succeed in showing, that by (SVD) we find some boundary respecting homomorphism onto $\mathfrak{P}_1$ of $\mathfrak{S}_0$ with $\overline{a} \neq \overline{a}^2 = \overline{0}$, since then in CASE 1 the elements $\overline{y}$ and $\overline{y}^2$ and in case CASE 2 the elements $\overline{a}$ and $\overline{c}$ are separated.

So let $\mathfrak{S}_0$ satisfy $a \neq a^2 = 0$ and let w.l.o.g. a be free from units except 1. By assumption $\mathfrak{S}$ is complementary, and by 2.8.9 we know, that along with u and v also $u * v$ is idempotent. This leads to $au = 0$ & $u = u^2 \Longrightarrow u = 0$, for, since a is free from non trivial units $au = 0$ & $u^2 = u$ implies first $au * 0 = a * (u * 0) = 1$ and next, since $u * 0$ is idempotent, $a(u * 0) = a$, that is $u * 0 = 1$ and $u = 0$, respectively.

Now we define:

$$\mathcal{P} := \Big\{(u, v)\,\Big|\, u = u^2 \;\&\; v = v^2 \;\&\; u * 0 = v \;\&\; v * 0 = u\Big\} \tag{15.14}$$

and consider – influenced by TARSKI [95] – all intersections $\bigwedge u_i$, picking one element out of each of these pairs. If then p is such an intersection element, then p must be the identity element 1 or some atom in the lattice $(I(S_0), \wedge, \vee)$ of all idempotents.

OBSERVE: First, in case of $1 \leq u = u^2 \leq p = p^2$, by $(u * 0)^2 = u * 0$ and $((u * 0) * 0)^2 = (u * 0) * 0$ we obtain:

$$\begin{array}{rrcl} & \underline{(u*0)} * \underline{((u*0)*0)} & = & (u*0)^2 * 0 = \underline{(u*0)*0} \\ \& & \underline{((u*0)*0)} * \underline{(u*0)} & = & u((u*0)*0)*0 = \underline{u*0} \\ \rightsquigarrow & (u*0, (u*0)*0) & \in & \mathcal{P} \\ \rightsquigarrow & p \leq u*0 & \bigvee & p \leq (u*0)*0\,. \end{array}$$

So, $p \leq u * 0$ would imply $(u * 0) = p(u * 0) = u(u * 0) = 0$ and thereby, recall $a * 0 \leq a$,

$$\begin{array}{rrcl} & a*0 & = & (a*au)(au*0) \\ & & = & (a*(a\vee u))(a*(u*0)) \\ & & = & (a*u)(a*0) \\ \rightsquigarrow & a*u & = & 1 \\ \rightsquigarrow & u & = & 1\,. \end{array}$$

Consequently it holds

$$(15.15) \qquad 1 \neq u = u^2 \leq p = p^2 \Longrightarrow p \leq (u*0)*0 \leq u \rightsquigarrow u = p\,.$$

Hence p is an atom, which leads to a boundary respecting subdirect decomposition of $\mathfrak{S}_0$ into components $\mathfrak{S}_i$ satisfying axiom (SVD), being free from non trivial idempotents except $0, 1$, and containing a maximum.

HINT: Decompose any x into the components $x \wedge p_i$.

BUT! Any "SVD-d-monoid" without non trivial idempotents is linearly ordered, observe: $(x \wedge y)(x * y \wedge y * x) = x \wedge y \neq 0$ implies $x * y \wedge y * x = 1$, since otherwise $x \wedge y$ would have a maximal unit $u \neq 1$ which would lead to $x * y = 1 \bigvee y * x = 1$, observe

$$(15.16) \qquad c \neq 1 \neq d \;\&\; c \wedge d = 1 \rightsquigarrow 1 \neq \bigvee c^{\perp} = (\bigvee c^{\perp})^2 \neq 0\,.$$

This implies further, that any $t \neq 1$ of $\mathfrak{S}_i$ is nilpotent in $\mathfrak{S}_i$, since otherwise all powers of t would be placed below $p_i \wedge a$, whence $\bigvee t^n = (\bigvee t^n)^2$ would be a unit of a, different from 1, a contradiction!

So, any $\mathfrak{S}_i$ is continuous and linearly ordered with

$$1 \neq t \Longrightarrow t^n = 0_i := p_i \,,$$

that is any $\mathfrak{S}_i$ admits a boundary respecting embedding into $\mathfrak{P}_1$, recall Hölder/Clifford.

Thus our proof is complete. □

15.5 Lattice Cubes

Two natural questions remained open, sofar.

First of all the question, under which conditions $\mathfrak{S}$ admits not only a cube extension but even *a lattice cube extension,* that is a cube extension, whose factors are of type $\mathfrak{S}_n$ for a suitable $n \in \mathbf{N}$.

Furthermore the question is interesting, which consequences result, if we strengthen condition (W) to the requirement, that the filter semigroup be archimedean, that is a property, stronger than **(CE)**, which follows immediately from $\mathsf{b} = \mathsf{b} \cdot A \Longrightarrow \mathsf{b} = \mathsf{b} \circ \mathfrak{a}$.

15. 5. 1 Proposition. *A positive d-monoid $\mathfrak{S}$ is a lattice-cube-semigroup if and only if it satisfies for any filter A the implication:*

$$\textbf{(LC)} \qquad A^n \supseteq \mathsf{b} \;\; (\forall n \in \mathbf{N}) \Longrightarrow A \cdot \mathsf{b} = \mathsf{b} = \mathsf{b} \cdot A$$

that is if and only its filter semigroup has the archimedean property.

PROOF. Since necessity is nearly obvious, we restrict our consideration to the verification of

SUFFICIENCY. According to 15.3.1 $\mathfrak{S}$ satisfies the conditions of a cube (d-) semigroup. Hence it remains to show, that $\mathfrak{S}$ is even a lattice cube semigroup. To this end we need enough homomorphic images of type $\mathfrak{S}_n$.

So, let $a < b$ be a critical pair and K a maximal c-ideal w. r. t. $a \not\equiv b \ (I)$. Then the set theoretic complement P of K is a prime filter.

But from the proof of 6.2.6 we know that each $\overline{x} \leq \overline{b}$ is comparable with each $\overline{z}$ and that

$$\text{(15.18)} \qquad \overline{x} \cdot \overline{u} \equiv \overline{x} \leq \overline{b} \Longrightarrow \overline{u} = \overline{1} \Longrightarrow u \in K$$

is satisfied. Moreover $\overline{P}$ is a filter of $\overline{\mathfrak{S}}$. We discuss the cases:

CASE 1: $a \in P$ & $b \in P$

CASE 2: $a \in K$ & $b \in P$.

AS TO CASE 1 : Any filter A with $A \supset P$ is generated by a base of elements $p \wedge a_i{}' =: a_i$ with $a_i \notin P$ $(\forall\, i \in I)$. Since P is prime, this leads to $a_i{}^d \cdot P = a_i{}^d \cap P$ $(\forall\, i \in I)$, and hence to

$$\begin{aligned} AP &= (\textstyle\sum a_i{}^d) \cdot P \ \ (i \in I) \\ &= \textstyle\sum (\, a_i{}^d \cap P\,) \\ &= (\textstyle\sum a_i{}^d\,) \cap P \\ &= P\,. \end{aligned}$$

So we get next:

$$\begin{aligned} P^n \supseteq AB \ \&\ P \not\supseteq A &\implies P \supseteq B \ \&\ P^n \supseteq AB \\ &\implies P \supseteq B \ \&\ P^n = P^n + AB \\ &\implies P \supseteq B \ \&\ P^n = P^n + (A + P^n)B \\ &\implies P \supseteq B \ \&\ P^n \supseteq (P + A)^n \cdot B \\ &\implies P^n \supseteq B\,, \end{aligned}$$

the final implication by $P + A \supset P \supseteq B$ and the archimedean property.

But, (in the present CASE 1) it holds $\overline{P} \ni \overline{a}$ and in case of $\overline{P}^n \supseteq \overline{a}$, there exists an element $e \in K = S\backslash P$ with $p^n \le ae$ $(\exists p \in P)$. So by the preceding development it even results $P^n \supseteq a^d$. And this means, that there must exist an element m with $\overline{P}^m \not\ni \overline{a}$, since otherwise $P \cdot a^d = a^d$ would be satisfied, implying the existence of some $p \in P$ with $ap = a$, that is by (15.18) an element p with $p \in K$ & $p \in P = S\backslash K$, a contradiction!

Consequently there exists an element m satisfying $\overline{P}^m \not\supseteq \overline{a}$, by which it results in particular $\overline{a} \le \overline{x}^m$ $(\forall\, \overline{x}$ with $P \ni x)$, recall that $\overline{a}$ is comparable with each $\overline{x}$ $(x \in P)$.

Now we choose some $\overline{x} \le \overline{a}$. If $\overline{x}$ is properly decomposable into $\overline{y} \cdot \overline{z}$, then because of linearity of $\overline{\mathfrak{S}}$ not only these divisors but also at least one square of these divisors, say $\overline{y}^2$, satisfies $\overline{y}^2 \le \overline{a}$, and we are in the position to continue the procedure until, recall $P^m \not\supseteq a$, we arrive at some indecomposable and thereby prime element $\overline{p}$ which must be even an atom, apply (15.18).

Consider, now, the set of all powers $\overline{p}^n$. It exceeds $\overline{a}$, whence for all $\overline{x}$

$$\overline{x} = \overline{p}^\ell \ \ (\exists \ell \in \mathbf{N}) \vee \overline{p}^n \,|\, \overline{x} \ \ (\forall n \in \mathbf{N})\,,$$

recall $\overline{p}$ is the only atom and thereby even completely prime.

Thus we arrive at $\overline{a} \leq \overline{p}^k < \overline{b}$ $(\exists k \in \mathbf{N})$, and the set of all $\overline{x} > \overline{a}$ forms a prime p-ideal in $\overline{\mathfrak{S}}$, since each $\overline{z}$ between $\overline{a}$ and $\overline{b}$ is comparable with each $\overline{y}$. Hence we may identify the elements $\overline{x} > \overline{a}$ thus getting $\overline{O}$, say. This provides an a, b separating homomorphic image $\overline{\overline{\mathfrak{S}}}_m$.

As to Case 2: (a) Let now $a \in K$ and $b \in P$ be fulfilled, that is $\overline{a} = \overline{1} < \overline{b}$. If then there exists an element $\overline{c}$ strictly between $\overline{1}$ and $\overline{b}$, then, by evidence, K is maximal also w. r. t. $c \not\equiv b$ (I), and we may continue as above.

(b) Otherwise $\overline{b}$ is the only atom in $\overline{\mathfrak{S}}$, and, again, the set of all $\overline{x} > \overline{a}$ forms a prime filter.

So under each of the assumptions (a) and (b), we may continue as below Case 1.

Thus our proof is complete. $\square$

Chapter 16

Representable d-semigroups

16.1 Foundation

In the chapter on congruences it was shown that completely distributive lattice monoids are representable iff they satisfy:

$$\text{(O)} \qquad xay \wedge ubv \ \leq \ xby \vee uav\,.$$

Obviously condition (O) is also necessary in the general case. Furthermore the proof above works as well in case that $\mathfrak{S}$, extended by an identity, satisfies condition (O) . Consequently we may start from the basic result:

16. 1. 1 Proposition. *A lattice semigroup is representable if it is completely distributive and if it satisfies in addition condition* (O) *for all elements* $x, y, u, v \in S \cup \{1\}$.

It turns out that commutative completely distributive d-monoids are always representable. But the above theorem does not hold in the general*cdl*-case, as was shown by Repnitzkii in [84]. In case of a d-semigroup $\mathfrak{S}$, however, (O) operates always, since $\mathfrak{S}$ contains enough private units.

In this chapter we study *representable* d-semigroups with the goal to simplify and to replace (O) by other equations or structure properties, respectively. This will lead us to some *representation results,* in particular to an ℓ-group result, proved by Fuchs, (compare. [49]), telling that for ℓ-groups (O) may be replaced by

$$(16.2) \qquad eae \wedge faf \ = \ (e \wedge f)a(e \wedge f)\,.$$

To be as general as possible we start from a *cdl-semigroup.* In this context we tacitly apply notions and results of d-semigroup theory if these are free from axiom (A4). For instance, the reader gets immediately that 2.2.3 and (2.14) are of this type.

Representability heavily depends on certain substructures, in particular it is influenced strongly by the structure of the lattice ideal semigroup.

The present chapter interacts with all other chapters, presenting representations of which type ever. Nevertheless its kernel is based merely on elementary arithmetic.

16.2 The general Case

First of all some structure theorems for arbitrary d-semigroups.

16. 2. 1 Proposition. *Let $\mathfrak{S}$ be a d-semigroup. Then the following are pairwise equivalent:*

- (i) $\mathfrak{S}$ *is representable.*
- (ii) $\mathfrak{S}$ *satisfies* $xay \wedge ubv \leq xby \vee uav$.
- (iii) $\mathfrak{S}^+$ *is representable.*
- (iv) $\mathfrak{S}^{1^+}$ *is representable.*
- (v) $\mathfrak{S}$ *satisfies* $ax \wedge yb \leq ay \vee xb$.
- (vi) $\mathfrak{S}$ *satisfies* $eae \wedge faf = (e \wedge f)a(e \wedge f)$.

PROOF. $(i) \Longleftrightarrow (ii)$ results from 6.1.2

$(ii) \Longleftrightarrow (iii)$. It suffices to verify $(iii) \Longrightarrow (ii)$. To this end suppose that $\mathfrak{S}^+$ satisfies (iii). We consider in $\mathfrak{S}$

$$xay \wedge ubv \quad \text{and} \quad xby \vee uav.$$

Obviously (ii) is valid, if it is valid in case of $a, b \in S^+$, since it holds with suitable $(a'', b'' \in S^+)$

$$\begin{array}{rcl} xay \wedge ubv & = & xa''(a \wedge b)y \wedge ub''(a \wedge b)v \\ & \text{and} & \\ xby \vee uav & = & xb''(a \wedge b)y \vee ua''(a \wedge b)v \end{array}$$

Next let $a, b, x', u', y'', v'' \in S^+$ satisfy

$$(a \wedge u)x' = x, (x \wedge u)u' = u, y''(y \wedge v) = y, v''(y \wedge v) = v\,.$$

Then by multiplying from the left with $x \wedge u$ and from the right with $y \wedge v$ we get

$$x'ay'' \wedge u'bv'' \leq x'by'' \vee u'av'' \leadsto xay \wedge ubv \leq xby \vee uav\,,$$

that is all at all $(iii) \Longrightarrow (ii)$.

$(iii) \Longleftrightarrow (iv)$ is an immediate consequence of the fact that $\alpha\,,\,\beta \in \Sigma$ are equal if and only if they satisfy the equation $x \cdot \alpha = x \cdot \beta \ \ (\forall x \in S^+)$. This is verified by the more general result, telling that any equation, holding in $\mathfrak{S}^+$, is valid in $\sum^+$, too, which results by the implication:

$$\begin{array}{rcl} xe & = & x \\ & \Longrightarrow & \\ x \cdot f(\alpha_1, \ldots, \alpha_n) & = & x \cdot f(\alpha_1 e, \ldots, \alpha_n e)\,. \end{array}$$

We continue by considering (ii), (v), (vi).

$(ii) \Longrightarrow (v)$ is evident – and –

$(v) \Longrightarrow (vi)$ results *via*

$$\begin{array}{rcl} eae \wedge faf \leq eaf \vee eaf = eaf & \& & faf \wedge eae \leq fae \vee fae = fae \\ & \leadsto & \\ (e \wedge f)a(e \wedge f) & = & eae \wedge eaf \wedge fae \wedge faf\,. \\ & = & eae \wedge faf\,. \end{array}$$

It remains to verify

$(vi) \Longrightarrow (ii)$. Since $(ii) \Longleftrightarrow (iii)$ it suffices to study the positive case. So, we may start from a positive subdirectly irreducible $\mathfrak{S}$ with hyper-atom h.

We consider $R = R(h)$ and $L = L(h)$. It holds $L \subseteq R$ or $R \subseteq L$ and thereby $C = L$ or $C = R$, recall C the set of cancellable elements. In order to prove this we assume $L \not\subseteq R \not\subseteq L$. Then there exist elements e, f with $e \in L \backslash R$ and $f \in R \backslash L$.

This means

$$eh = h = hf \quad \& \quad he = 0 = fh\,,$$

leading to:

$$h = (e \wedge f)h(e \wedge f) \;=\; ehe \wedge fhf = 0\,,$$

a contradiction!

Hence, C is an irreducible c-ideal, whence $p \perp q \Longrightarrow p \in C \vee q \in C$. On the other hand we may restrict our attention to orthogonal pairs $x \perp u$, $a \perp b$, $y \perp v$, since the elements x', u', a'', b'', y'', v'', constructed below $(iii) \Longrightarrow (ii)$ fulfil this condition, if $x, a, y, u, b, v \leq h$, whereas in case of $0 \in \{x, a, y, u, b, v\}$ condition (iii) follows *a fortiori.*

So, let's start from

$$x \perp u\,,\ a \perp b\,,\ y \perp v\& \qquad \text{w.l.o.g.} \qquad a \in C\ (!)$$

For the sake of further reduction, observe, that we may start even from

$$(x \wedge a) \wedge y \;=\; 1\,,$$

This can be shown as follows: It holds

$$x \wedge a \wedge y \wedge ubv \stackrel{(2.19)}{=} 1\,.$$

Suppose now

$$\begin{aligned} (x \wedge a \wedge y) \cdot x^\circ &= x \\ (x \wedge a \wedge y) \cdot a^\circ &= a \\ (x \wedge a \wedge y) \cdot y^\circ &= y\,. \end{aligned}$$

Then by

$$(x \wedge a \wedge y) \cdot (x^\circ \wedge a^\circ \wedge y^\circ) = (x \wedge a \wedge y) \in C\,,$$

it results:

$$x^\circ \wedge a^\circ \wedge y^\circ = 1\,,$$

recall $a \in C$, and we get moreover:

$$x^\circ a^\circ y^\circ \wedge ubv \stackrel{(2.19)}{=} xay \wedge ubv\,,$$

recall $x \wedge a \wedge y \perp ubv$. Hence in case of

$$x^\circ a^\circ y^\circ \wedge ubv \;\leq\; x^\circ by^\circ \vee ua^\circ v$$

it holds as well:
$$\begin{aligned} xay \wedge ubv &= x^\circ a^\circ y^\circ \wedge ubv \\ &\leq x^\circ b y^\circ \vee u a^\circ v \leq xby \vee uav. \end{aligned}$$

So, let's start from

$$x \perp u \ \&\ a \perp b \ \&\ y \perp v \ \&\ a \wedge x \perp y \ \&\ a \in C\,. \tag{16.3}$$

Then by symmetry it suffices to settle the cases:

CASE 1 . $\quad x, y \in C\,.$

CASE 2 . $\quad x, v \in C\,.$

CASE 3 . $\quad u, v \in C\,.$

To this end we remark first of all: Let d and g be coprime. Then it follows

$$\begin{aligned} c \in C &\implies cd \wedge gc \leq dcd \wedge gcg = c \\ &\implies c(d \wedge c * gc) = c \\ &\implies d \perp c * gc\,, \end{aligned}$$

recall that $c * gc$ and $c : gc$ are uniquely determined. So, by duality we are led to the implication:

$$\begin{aligned} c \in C &\implies d \perp g \\ &\implies d \perp c * gc \ \&\ d \perp cg : c\,, \end{aligned} \tag{L}$$

that is: in case of $d \perp g$ and $c \in C$ there exists a pair $s \perp d$ with $cs = gc$ and a pair $t \perp d$ with $cg = tc$.

Now we are in the position to clear the CASES 1, 2, 3.

AS TO CASE 1. Since $x, y \in C$ we get by (L) and (*vi*) with orthogonal elements a°, b°

$$\begin{aligned} xay \wedge ubv &= a^\circ xy \wedge uvb^\circ \\ &\leq a^\circ(xy \vee uv)a^\circ \wedge b^\circ(xy \vee uv)b^\circ \\ &= xy \vee uv. \\ &= xby \vee uav. \end{aligned}$$

AS TO CASE 2. On the same grounds as in CASE 1 according to (2.19) we get with orthogonal elements a°, b°

$$\begin{aligned} xay \wedge ubv &= xay \wedge (u \wedge xay)b(v \wedge xay) \\ &= xya^\circ \wedge (u \wedge xay)(v \wedge xay)b^\circ \\ &\leq (xy \vee uv)a^\circ \wedge (xy \vee uv)b^\circ \\ &= xby \vee uav\,. \end{aligned}$$

As to Case 3. First by (vi) we get

$$\begin{aligned} a^2 \wedge x^2 &= a \cdot 1 \cdot a \wedge x \cdot 1 \cdot x \\ &= (a \wedge x)^2 \,, \end{aligned}$$

which by cancellation leads to:

$$(x * a)(a : x) \wedge (a * x)(x : a) = 1 \,.$$

Consequently the elements $a*x$ and $a : x$ commute. Furthermore the elements $a \wedge x$ and y commute, recall (16.3). So we can calculate:

$$\begin{aligned} xay \wedge ubv &= (x \wedge a)(a * x)(a : x)(a \wedge x)y \wedge ubv \\ &= (x \wedge a)(a : x)(a * x)y(x \wedge a) \wedge uvb^\circ \quad (b^\circ \perp a, \text{ recall (L)}) \\ &\leq (x \wedge a)(a : x)(xy \vee uv)(x \wedge a)(a : x) \wedge b^\circ(xy \vee uv)b^\circ \\ &\leq xy \vee uv \,. \\ &\leq xby \vee uav \,. \end{aligned}$$

Thus the proof is complete. □

16.3 d-Monoids

Sofar we have studied d-semigroups in general. We now turn to d-monoids. This enables us to apply well known notions of ℓ-group theory, introduced by pioneers like Jaffard and Conrad (cf. [49],[45]) and well discussed above all in the most deserving lecture note of Bigard-Keimel-Wolfenstein, compare [11].

In particular representable d-semigroups were characterized by equations.

Now we are going to characterize representable d-semigroups by special substructure properties. Here we will succeed above all, since according to proposition 16.2.1, we may restrict our studies to the (positive) cone.

16. 3. 1 Proposition. *Let $\mathfrak{S}$ be a positive d-monoid and let J be a co-regular ideal of $\mathfrak{S}$. Then the following are pairwise equivalent:*

(i) *$\mathfrak{S}$ is representable.*

(ii) $\ker(J) := \{k \mid s \cdot 1 \cdot t \in J \Longrightarrow s \cdot k \cdot t \in J\}$ *is irreducible .*

(*iii*) *The set of c-ideals between* $\ker(J)$ *and* J *forms a chain under* $\subseteq$.

(*iv*) $X^\perp := \{y \mid x \wedge y \in \ker(J)\}$ *and* $X^{\perp\perp} := \{z \mid \forall y \in x^\perp : y \wedge z \in \ker(J)\}$ *satisfy the equation* $X^\perp \cup X^{\perp\perp} = S$.

(*v*) $X^\perp$ *and* $X^{\perp\perp}$ *satisfy the equation* $X^\perp \cdot X^{\perp\perp} = S$.

PROOF. (*i*) $\Longrightarrow$ (*ii*). If $\mathfrak{S}$ is representable, then $\mathfrak{S}/J$ is totally ordered, whence $\{\overline{1}\}$ is $\wedge$-irreducible. But, $\ker(J)$ is the inverse image of $\{\overline{1}\}$. Hence $\ker(J)$ is irreducible, too.

(*ii*) $\Longrightarrow$ (*i*). If $\ker(J)$ is irreducible, then in $\mathfrak{S}/J$ the identity $\{\overline{1}\}$ is $\wedge$-irreducible. Consequently $\mathfrak{S}/J$ is totally ordered according to 5.4.5.

(*i*) $\Longrightarrow$ (*iii*). Let J be a co-regular ideal. Then $\mathfrak{S}/J$ is subdirectly irreducible and thereby normal according to 5.4.5.

Now we consider two different c-ideals A and B between $\ker(J)$ and J and choose w.l.o.g. an element $a \in A \backslash B$ and an element $b \in B$. Since $\mathfrak{S}/J$ is totally ordered, $\ker(J)$ is irreducible. Hence, choosing orthogonal elements a°, b° with $R(a, b, a^\circ, b^\circ)$, we get $a^\circ \wedge b^\circ \in \ker(J)$. Consequently this implies $b^\circ \in \ker(J)$ and thereby $(a \wedge b)b^\circ = b \in A \cap B$. So B is contained in A.

(*iii*) $\Longrightarrow$ (*i*). By (*iii*) the kernels of co-regular ideals are irreducible. So, it suffices to show, that there are enough co-regular ideals. But this is evident, since there are enough filters.

(*i*) $\Longrightarrow$ (*iv*). Let $\mathfrak{S}$ be representable and let J be a co-regular ideal. Then $\mathfrak{S}/J =: \overline{\mathfrak{S}}$ is totally ordered, and it holds $\overline{X}^\perp \cup \overline{X}^{\perp\perp} = \overline{S}$, which implies condition (*iv*).

(*iv*) $\Longrightarrow$ (*i*). Let $\overline{\mathfrak{S}}$ be defined as below (*i*) $\Longrightarrow$ (*iv*) and assume that $\overline{\mathfrak{S}}$ is not totally ordered. Then there exist incomparable elements $\overline{x}, \overline{y}$ properly between $\overline{1}$ and $\overline{h}$ and consequently there exist also orthogonal elements $\overline{x}^\circ, \overline{y}^\circ$ properly between $\overline{1}$ and $\overline{h}$. This leads to $\overline{x}^{\circ\perp} < \overline{h}$ and thereby also to $\overline{x}^{\circ\perp\perp} < \overline{h}$, a contradiction!

(*i*) $\Longrightarrow$ (*v*). Recall the proof of (*i*) $\Longrightarrow$ (*iv*).

(*v*) $\Longrightarrow$ (*i*). Let J be a co-regular ideal of $\mathfrak{S}$ and suppose that $\mathfrak{S}/J =: \overline{\mathfrak{S}}$ is not totally ordered. Then – according to (*v*) – the hyper-atom $\overline{h}$ of $\overline{\mathfrak{S}}$, is a product of some orthogonal pair $\overline{x}, \overline{y}$. This leads next to $\overline{x}^2 \leq \overline{h}$, $\overline{y}^2 \leq \overline{h}$ and thereby further to the contradiction

$$\overline{h} = \overline{x} \cdot \overline{y} = \overline{x} \vee \overline{y} = \overline{x}^2 \vee \overline{y}^2 = \overline{x}^2\overline{y}^2 = \overline{h}^2 = \overline{0}.$$

Thus the proof is complete. □

16. 3. 2 Definition. Let $\mathfrak{S}$ be a d-monoid. We call $\mathfrak{S}$ *finitely valued*, if any $a \in S$ has at most finitely many values.

16. 3. 3 Proposition. *Let $\mathfrak{S}$ be a d-monoid. Then the following are pairwise equivalent:*

(i) *$\mathfrak{S}$ is a direct sum $\sum^* \mathfrak{S}_i \ (i \in I)$ of totally ordered $\mathfrak{S}_i$.*

(ii) *$\mathfrak{S}$ is finitely valued and semi-projectable.*

(iii) *$\mathfrak{S}$ is ortho-finite and projectable.*

(iv) *Any z-monoid of $\mathfrak{S}$ is a direct factor.*

PROOF. First we prove $(i) \Longrightarrow (ii) \Longrightarrow (iii) \Longrightarrow (i)$. Thereafter we shall verify $(i) \Longrightarrow (iv) \Longrightarrow (iii)$.

$(i) \Longrightarrow (ii)$ is left to the reader.

$(ii) \Longrightarrow (iii)$. According to 14.4.4 any proper prime c-ideal contains exactly one minimal prime c-ideal.

Furthermore, similarly to the first part of that proof we get that $\mathfrak{S}$ is ortho-finite, since in case of $1 \leq a_i \leq a \ (i \in I)$ finitely valued means that I is finite or at least that there exists some value M of a, containing ${a_j}^{\perp}$ and ${a_k}^{\perp} \ (j \neq k)$. But this leads to a contradiction, recall 14.4.4.

Next we see that any $M \in \mathrm{val}\,(a)$ is the uniquely determined value w. r. t. some suitable element c . To this end we start from the family $\{M_i \,|\, i \in I\}$ of all minimal prime c-ideals of $\mathfrak{S}$, not containing a . This family is finite since by 14.4.4 any M_i is uniquely associated with some value of a . Hence it holds:

$$\begin{aligned} \{M_i \,|\, i \in I\} \;&=\; \{M_0, M_1, \ldots, M_n\} \\ \text{with} \qquad & M_0 \subseteq M \ \&\ M_i \not\subseteq M \ \ (1 \leq i \leq n)\,. \end{aligned}$$

Choose now elements $c_i \in M_i \backslash M \ \ (1 \leq i \leq n)$ for all $i \in I$ and consider a value W of $c := a \wedge c_1 \wedge c_2 \wedge \ldots \wedge c_n$. W can be extended to some value of a. But W doesn't contain any $M_i \ (1 \leq i \leq n)$. Consequently any value of c must contain the minimal prime c-ideal M. Hence there can exist only one value of c , since different values, according to 13.1.2, contain different minimal prime c-ideals.

Now we are in the position to verify $S = a^\perp \times a^{\perp\perp}$.

To this end we assume $S \neq a^\perp \times a^{\perp\perp}$. Then $a^\perp \times a^{\perp\perp}$ is contained in some M with $\{M\} = \mathrm{val}\,(c)$. But it holds $a^{\perp\perp} = \bigcap h^\perp \ (h \in a^\perp)$. Hence there exists at least one $h^\perp$, not containing c, and thereby admitting an extension to M. So it is contained in M. But, since $h^\perp \supseteq a^{\perp\perp}$ this leads to $h \in h^{\perp\perp} \subseteq a^\perp \rightsquigarrow a \perp h$ and consequently to the contradiction:

$$S \neq M \supseteq a^\perp \vee h^\perp = (a \wedge h)^\perp = S.$$

Thus it has been shown $(ii) \Longrightarrow (iii)$.

$(iii) \Longrightarrow (i)$. Choose some $a \in S^+$ and suppose that $a^{\perp\perp}$ is not totally ordered. Then there exists an element x in $a^{\perp\perp}$ with $\{1\} \neq x^{\perp\perp} \subseteq a^{\perp\perp}$, but $x^{\perp\perp} \neq a^{\perp\perp}$. This leads to

$$a^{\perp\perp} = x^{\perp\perp} \times (x^\perp \cap a^{\perp\perp}) \qquad (13.5.9)$$

and thereby to $a = a_1 \cdot a_2$ with $a_1 \in x^{\perp\perp}$ and $a_2 \in x^\perp \cap a^{\perp\perp}$. So, we get $a_1 \perp a_2$. We will show: $a_1 \neq a \neq a_2$. To this end we assume first that $a_1 = a$. This implies $x^{\perp\perp} = a^{\perp\perp}$, a contradiction! Let now $a_2 = a$ be satisfied. This leads to

$$a \in x^\perp \Longrightarrow a^\perp \supseteq x^{\perp\perp} \Longrightarrow x \in a^\perp \cap a^{\perp\perp},$$

again a contradiction!

Hence the decomposition of a is proper. So, continuing this procedure of decomposing, after finitely many steps we arrive at $a = a_1 \cdot a_2 \cdot \ldots \cdot a_n$ with pairwise orthogonal elements a_i, each of which generates a totally ordered bipolar ${a_i}^{\perp\perp}$.

Let now $x^{\perp\perp} \neq y^{\perp\perp}$ be two totally ordered bipolars. Then any positive $x^+ \in x^{\perp\perp}$ must satisfy $x^{+\perp\perp} = x^{\perp\perp}$, since otherwise there would exist a decomposition of $x^{\perp\perp}$ of the above type, and, of course the same must be true for $y^{\perp\perp}$. Hence we get $x^{\perp\perp} \cap y^{\perp\perp} = \{1\}$, because $|x \wedge y|^{\perp\perp} \neq 1 \Longrightarrow |x \wedge y|^{\perp\perp} = x^{\perp\perp} = y^{\perp\perp}$.

Consequently the family of totally ordered bipolars $x^{\perp\perp}$ provides a decomposition of $\mathfrak{S}$ in the sense of (i).

Now we turn to $(i) \Longrightarrow (iv) \Longrightarrow (iii)$:

$(i) \Longrightarrow (iv)$. Suppose $\mathfrak{S} = \sum^* \mathfrak{S}_i \ (i \in I)$ and let $\mathfrak{Z}$ be a z-submonoid of $\mathfrak{S}$. Then it follows $\mathfrak{Z} = \sum^* (\mathfrak{S}_i \cap \mathfrak{Z}) \ (i \in I)$. We assume $S_i \cap Z \neq \{1\}$ and consider some s with $s_i \in S_i \cap Z$. It follows $S_i = s_i{}^{\perp\perp} \subseteq Z$. Hence Z is of type $\sum^* S_j \ (j \in J \subseteq I)$.

$(iv) \Longrightarrow (iii)$. By (iv) any z-monoid of $\mathfrak{S}$ is a polar. Therefore $\mathfrak{S}$ is orthofinite, recall proposition 14.3.3. Furthermore any $s^{\perp\perp}$ is a z-monoid and thereby a direct factor. Hence $S = s^{\perp} \times s^{\perp\perp}$.

This completes the proof. □

16.4 Hyper-normal d-Monoids

In this section we specialize the notion of normality in such a way that the structure of commutative ring ideal semigroups is simulated in a fruitful manner. To this end, first of all, observe that in any ring-principal-ideal-monoid it holds

$$\langle a\rangle\langle u\rangle = \langle a\rangle \ \&\ \langle a\rangle\langle y\rangle = \langle b\rangle \Longrightarrow \exists \langle v\rangle \perp \langle u\rangle : \langle a\rangle\langle v\rangle = \langle b\rangle \tag{16.5}$$

inde$d$-monoid!hyper-normal

SINCE

$$\begin{aligned} \langle a\rangle\langle u\rangle = \langle a\rangle \ \&\ \langle a\rangle\langle y\rangle = \langle b\rangle &\Longrightarrow a(ux) = a \ \&\ a(ys) = b \ \ (\exists x, s) \\ &\Longrightarrow a(ux - 1 + uxys) = b\,, \end{aligned}$$

with $\langle u\rangle \perp \langle ux - 1 + uxz\rangle =: \langle v\rangle$, and observe furthermore that (16.5) holds also in any ℓ-group-cone.

16. 4. 1 Definition. A d-monoid is called *hyper-normal* here if it satisfies:

$$\begin{aligned} x, y \in S^+ \ \&\ ax \wedge ay = a &\Longrightarrow \exists\, z \perp x : ay = az \\ x, y \in S^+ \ \&\ xa \wedge ya = a &\Longrightarrow \exists\, z \perp x : ya = za\,. \end{aligned}$$

In particular for d-monoids with zero definition 16.4.1 implies

$$au = a \Longrightarrow \exists v \perp u : av = 0\,, \tag{16.6}$$

that is a property which is valid in every commutative principal ring ideal monoid.

16. 4. 2 Lemma. *A d-monoid is already hyper-normal if it satisfies:*

$$\begin{aligned} e \in S^+ \ \&\ ae = a \leq b &\Longrightarrow \exists\, x \perp e : b = ax \\ e \in S^+ \ \&\ ea = a \leq b &\Longrightarrow \exists\, x \perp e : b = xa\,. \end{aligned}$$

PROOF. Suppose $ax \wedge ay = a$. We replace y by an element $y^* \perp x \wedge y$. Consequently $z := y^* \wedge y$ satisfies $az = ay \ \ (z \perp x)$. □

$$ax \mid a \Longrightarrow a = axy \quad \& \quad a(xy - 1 + xyz) = az\,.$$

16. 4. 3 Lemma. *Let $\mathfrak{S}$ be a hyper-normal d-monoid and let J be an* invariant c-ideal of $\mathfrak{S}$. Then $\mathfrak{S}/J$ is hyper-normal, too.

PROOF. Suppose that $\overline{au} = \overline{a} \leq \overline{b}$ and $b = a \vee b$. Then it follows $au \leq ae \leq be \ \ (e \in J)$ and thereby $a(u \wedge e) = a(u \wedge e)u' \ \ (u' \in S^+)$. Hence, with a suitable positive x we get:

$$be = a(u \wedge e)x \;\; = \;\; a(u \wedge e)y' \quad (y' \perp u')\,.$$

From this it results furthermore:

$$\overline{b} = \overline{a} \cdot \overline{(u \wedge e)y'} \;\; \text{with} \;\; \overline{(u \wedge e)y'} = \overline{y} \perp \overline{u}\,.$$

The rest follows by duality. □

16.4.3 obviously implies that $\mathfrak{S}/J$ is 0-cancellative, if $\mathfrak{S}/J$ is totally ordered. Next we show:

16. 4. 4 Proposition. *For a positive hyper-normal d-monoid $\mathfrak{S}$ the following are pairwise equivalent:*

(i) *$\mathfrak{S}$ is representable.*

(ii) *$\mathfrak{S}$ satisfies $xa \wedge bx \leq x(a \wedge b) \vee (a \wedge b)x$.*

(iii) *$\mathfrak{S}$ satisfies $a \wedge b = 1 \;\; \Longrightarrow \;\; xa \wedge bx = x$.*

(iv) *$\mathfrak{S}$ satisfies $xa^{\perp} = a^{\perp} x$.*

(v) $a, b \in S^+ \;\&\; xa \wedge bx = x$
$$\Longrightarrow \quad \exists\, c, d \in S^+ : \begin{cases} c \perp a \;\;\&\;\; cx = bx \\ d \perp b \;\;\&\;\; xd = xa \end{cases}$$

(vi) *Any minimal prime submonoid of $\mathfrak{S}$ is invariant.*

(vii) *If J is regular w. r. t. invariant c-ideals, then J is prime w. r. t. invariant c-ideals.*

PROOF. (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii) is evident.

$(iii) \Longrightarrow (iv)$. Suppose $a \perp b$ and $bx = xc$. Then it follows

$$xa \wedge bx = \ x \ = xa \wedge xc = x(a \wedge c).$$

But this implies $xc = xc^*$ with $c^* \perp c \wedge a$, whence $z = c^* \wedge c$ satisfies $z \perp a$ & $bx = xz$. This way we get $a^\perp x \subseteq xa^\perp$ and dually it follows $xa^\perp \subseteq a^\perp x$.

$(iv) \Longleftrightarrow (v)$. Suppose $xa \wedge bx = x$. We get $bx = xu$ and thereby

$$\begin{aligned} xa \wedge bx = x \ &\Longrightarrow \ xa \wedge xu = x \\ &\Longrightarrow \ xu = xu^* \qquad\qquad (u^* \perp a) \\ &\Longrightarrow \ bx = xu^* = cx \qquad (c \perp a)\,. \end{aligned}$$

Hence it follows (v) from (iv).

Let now (v) be satisfied and suppose $a \perp b$ and $xb = dx$. Then we get $xa \wedge dx = x$, whence according to (v) there exists an element c satisfying $a \perp c$ and $cx = dx = xb$. But this implies $xa^\perp \subseteq a^\perp x$ and (dually) $a^\perp x \subseteq xa^\perp$, that is axiom (iv).

$(iv) \Longleftrightarrow (vi)$. Since according to 13.4.2 any minimal prime c-Ideal is a union of polars, it holds $(iv) \Longrightarrow (vi)$.

On the other hand, in case of (vi), any a, b separating c-ideal of $\mathfrak{S}$ contains an invariant minimal prime sub-c-monoid of $\mathfrak{S}$. Thus (vi) implies (i) and thereby (iv).

$(iv) \Longrightarrow (vii)$. Observe that invariant c-ideals J carry over condition (iv) from $\mathfrak{S}$ to $\mathfrak{S}/J$, since $R(a, b, a^\circ, b^\circ)$ implies:

$$a \wedge b \in J \ \Longrightarrow \ xb = x(a \wedge b)b^\circ = cx(a \wedge b) \quad (c \perp a^\circ)$$

and thereby $\overline{x}\overline{b} = \overline{c}\overline{x}$ $(\overline{a} \perp \overline{c})$.

Consequently $\overline{J} = \overline{1}$ is a prime c-ideal, which follows along the proof-lines of 4.1.3 Hence J itself is a prime c-ideal, too. This means that (iv) implies (vii).

Finally we get $(vii) \Longrightarrow (i) \Longrightarrow (iv)$. $\square$

16. 4. 5 Corollary. *A hyper-normal d-monoid is representable, if its cone satisfies the conditions of* 16.4.4 .

Of course, the conditions of 16.4.4 might also be formulated independent from the cone, for instance by applying the absolute values. However, approaching by the cone seems to be more transparent.

ADDED in May, 14^{th} 2010:

16. 4. 6 Proposition. *Let $\mathfrak{S}$ be a positive and hyper-normal d-semigroup, and let $\mathfrak{i}$ be any d-ideal. Then $\mathfrak{S}/\mathfrak{i}$ is hyper-normal, too.*

PROOF. Suppose w.l.o.g. that $x \in \mathfrak{p}$ and that $x \wedge au = x \wedge a$ & $x \wedge a \leq x \wedge b$. The we obtain:

$$\begin{aligned}
\overline{a} \cdot \overline{u} = \overline{a} \leq \overline{b} &\implies x \wedge au = x \wedge a \leq x \wedge b \ \ (\exists x \in \mathfrak{i}) \\
&\implies (x \wedge a)x' \wedge (x \wedge a)u = x \wedge a \leq x \wedge b \\
&\implies (x \wedge a)(x' \wedge u) = x \wedge a \leq x \wedge b \\
&\implies (x \wedge a)v = x \wedge b \quad (x' \wedge u \wedge v = 1) \\
&\implies (x \wedge a)(x' \wedge v) = x \wedge (x \wedge a) \cdot v = x \wedge b \\
&\implies x \wedge a(x' \wedge v) = x \wedge b \\
&\implies \overline{a} \cdot (\overline{x}' \wedge \overline{v}) = \overline{b} \text{ with } \overline{x}' \wedge \overline{v} \perp \overline{u}\,.
\end{aligned}$$

□

16. 4. 7 Proposition. *Let $\mathfrak{S}$ be a positive and hyper-normal d-semigroup, and let $\mathfrak{p}$ be a prime d-ideal. Then*

$$\overline{a} \cdot \overline{b} = \overline{0} \Longrightarrow \overline{a} = \overline{0} \vee \overline{b} = \overline{0}. \tag{16.7}$$

16. 4. 8 Proposition. *Let $\mathfrak{S}$ be a positive and hyper-normal d-semigroup, and let $\mathfrak{p}$ be a prime d-ideal. Then*

$$\overline{a} \neq \overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{y} \Longrightarrow \overline{x} = \overline{y}. \tag{16.8}$$

PROOF.
$$\begin{aligned}
\overline{a} \neq \overline{0} \ \& \ \overline{a} \cdot \overline{u} = \overline{a} &\implies \exists \overline{v} \perp \overline{u} : \overline{a} \cdot \overline{v} = \overline{0} \\
&\implies \overline{v} = \overline{0} \ \& \ \overline{0} \perp \overline{u} \\
&\implies \overline{u} = \overline{1}\,.
\end{aligned}$$

Hence
$$\begin{aligned}
\overline{a} \cdot \overline{x} \neq \overline{0} \ \& \ \overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{y} &\implies \overline{a(x \wedge y)} \cdot \overline{x}\,' = \overline{a(x \wedge y)} \\
&\implies \overline{x}\,' = \overline{1} \\
&\implies \overline{x} \leq \overline{y}\,.
\end{aligned}$$

This proves the assertion by duality. □

UNPUBLISHED SOFAR :

ADDED in May, 15^{th} 2010:

Clearly, if $\mathfrak{p}$ is a d-ideal, then $a \in \mathfrak{p} \Longrightarrow a \equiv 0$. Observe $a \wedge 0 = a = a \wedge a$.

Furthermore: Given two elements a, b, there exists an element c with $c \notin$ d-ideal $\mathfrak{a}$ iff $a \not\equiv b$ mod $\mathfrak{a}$.

16. 4. 9 Proposition. *If $\mathfrak{S}$ is hyper-normal with radical $\{0\}$ and has the above property, then $\mathfrak{S}$ owns a subdirect decomposition into ℓ-group-cones with zero, and vice versa.*

So, commutative radical free hyper-normal d-semigroups are separative, compare the next chapter.

ADDED in May, 27^{th} 2010:

16. 4. 10 Proposition. *Let $\mathfrak{S}$ be a hyper-normal d-monoid, and let its radical R be a prime d-ideal. Then $S \backslash R$ is a cancellative d-monoid, and any $x \in S\backslash R$ divides any element $a \in R$.*

PROOF. First of all it holds

$$a^m = 0 \Longrightarrow a^{\perp} = \{1\}, \tag{16.9}$$

sine any b divides $0 = a^m$. Next

$$\begin{aligned} a \in R \;\&\; x \notin R \;\&\; R(x, a, x', a') &\Longrightarrow (x \wedge a)(x' \wedge a') = x \wedge a \\ &\Longrightarrow \exists u \perp (x' \wedge a') \;\&\; (a \wedge x)u = 0 \\ &\Longrightarrow \exists u \in R \;\&\; u \perp x' \wedge a' \\ &\Longrightarrow x' \wedge a' = 1 \Longrightarrow x' = 1\,. \end{aligned}$$

Let finally $a, x, y \in S\backslash R. ax = ay$. Then

$$\begin{aligned} ax = ay &\Longrightarrow a(x \wedge y) = a(x \wedge y)x' \\ &\Longrightarrow \exists u \perp x' :\; a(x \wedge y)u = 0 \\ &\Longrightarrow \exists u \in R : u \perp x' \Longrightarrow x' = 1\,. \end{aligned}$$

□

At this place it is a pleasure for the author to thank for a dedication and to give a hint to the three-men-paper [3] of Ánh, Márki, Vámos. There the close connection of hyper-normal d-monoids to ideal monoids of Bézout rings is investigated from the topological point of view.

As to subdirect decompositions of complementary semigroups into idempotent and cancellative ones see also [14], and [34].

Chapter 17

Separative d-semigroups

A semigroup is called *inverse*, if there exists for any element a a uniquely determined element a^{-1} satisfying

$$(17.1) \qquad a \cdot a^{-1} \cdot a = a \quad \text{and} \quad a^{-1} \cdot a \cdot a^{-1} = a^{-1}\,.$$

Hence the inverse semigroup is a common abstraction of *group* and *semilattice.*

A d-semigroup $\mathfrak{S}$ is called inverse, if $(S, \cdot)$ is inverse. Consequently the inverse d-semigroup is a common abstraction of ℓ-group and d-lattice.

Let $\mathfrak{S}$ be an inverse d-monoid. Then $G_e := \{x \,|\, xx^{-1} = e\}$ is equal with the set of all ec with $e \wedge (1 \vee c)(1 \wedge c)^{-1} = 1$ and $cc^{-1} = 1$. So any inverse d-semigroup is a semilattice of ℓ-groups $\mathfrak{G}_u$ with $u \leq v \Longrightarrow (\mathfrak{G}_u)v = \mathfrak{G}_v$.

As a most natural generalization of the inverse d-semigroup will turn out the *separative* d-semigroup, defined by

$$(17.2) \qquad (ab = aa \;\&\; ba = bb) \bigvee (ab = bb \;\&\; ba = aa) \Longrightarrow a = b\,.$$

The main result of this chapter will be that a d-semigroup admits an embedding into an inverse d-semigroup iff it is separative.

According to Clifford any inverse d-semigroup is structured in a canonical manner, starting from some distributive lattice $\mathfrak{D}$ and a system $\mathfrak{G}_\alpha$ ($\alpha \in D$) of ℓ-groups together with homomorphisms $\phi_{\alpha,\alpha\vee\beta} : \mathfrak{G}_\alpha \longrightarrow \mathfrak{G}_{\alpha\vee\beta}$ and $\psi_{\alpha,\alpha\wedge\beta} : \mathfrak{G}_\alpha \longrightarrow \mathfrak{G}_{\alpha\wedge\beta}$.

For the sake of a most general approach to the theory of inverse d-semigroups we start from a separative d-semigroup. In particular we will go ahead as follows:

First of all we study the subsemigroup $\mathfrak{E}\cdot\mathfrak{C}$ of arbitrary d-semigroups $\mathfrak{S}$. This structure will turn out – in some sense – as a canonical sub-d-semigroup of $\mathfrak{S}$. Moreover from the methodical point of view we will go ahead in such a manner, that a representation theorem of McAlister for inverse d-semigroups is subsumed as a special case.

In a second paragraph we present a series of conditions, equivalent with separativeness, showing that a d-semigroup is separative iff it is a subdirect product of cancellative d-semigroups with or without 0. This will be the fundament for characterizing the *finest separative congruence* and thereby describing the *largest separative image* of arbitrary d-semigroups $\mathfrak{S}$.

In the next chapter we then will apply the above results to inverse d-semigroups.

17.1 The Structure of E·C

In this section we continue the study of arithmetic – recall Chapter 1 – that is, we investigate, how $\mathfrak{C}$ and $\mathfrak{E}$ interact one with another. Since cancellative elements can exists only in d-monoids, let in this section $\mathfrak{S}$ always be a d-monoid. Recall 5.2.7. It is our goal to apply the congruences ρ and σ w. r. t. clearing the structure of d-monoids. As a first result of this type we get:

17. 1. 1 Proposition. *Let $\mathfrak{S}$ be a d-monoid. Then $\mathfrak{E}\cdot\mathfrak{C}$ is a* Clifford-*structure over a distributive lattice.*

PROOF. Let e be idempotent. Then obviously eC is operatively closed and since by $ec\cdot x = ed$ also $(ec)(ex) = ed$ is satisfied, $\mathfrak{E}\cdot\mathfrak{C}$ is a union of sub-d-monoids with e in the role of an identity.

Furthermore these substructures $e\mathfrak{C}$ are pairwise disjoint. For, consider some $ua = vb$ with idempotent factors u, v and cancellable factors a, b. Then in the quotient hull $\mathfrak{Q}$ it follows $u = vba^{-1}$, leading to $vu = u$ and hence by symmetry also to $uv = v$. Consequently $E\cdot C$ is the *disjoint union* of the subsets eC $(e = e^2)$. So, the set of all eC forms a distributive lattice .

Finally, it is clear, that the mappings

$$\phi_e : a \longmapsto ea \tag{17.3}$$

for idempotent u, v forms a *directed set* of homomorphisms

$$\phi_{u,u\vee v}: \quad u\cdot\mathfrak{C} \longrightarrow (u\vee v)\cdot\mathfrak{C} \tag{17.4}$$

that is of homomorphisms $\phi_{u,u\vee v}$ satisfying

$$\phi_{u\wedge v,v}\cdot\phi_{v,u\vee v} \;=\; \phi_{u\wedge v,u\vee v}\,. \tag{17.5}$$

In particular this implies:

$$\begin{array}{rcl} a\in uC & \& & b\in vC \\ & \Longrightarrow & \\ a=ux & \& & b=vy \\ & \Longrightarrow & \\ ab=uva\cdot uvb & = & a\,\phi_{u,u\vee v}\cdot b\,\phi_{v,u\vee v}\,. \end{array}$$

Consequently $\mathfrak{E}\cdot\mathfrak{C}$ is a *Clifford-semigroup* over a distributive lattice. □

We now shall introduce the operation σ_e. To this end recall the definitions of a^+, a^-, a^* and $|\,a\,|$. In particular recall:

$$|\,a\,|\perp|\,b\,| \iff a^+\perp b^+\perp a^* \;\&\; b^+\perp a^+\perp b^*\,.$$

17. 1. 2 Proposition. *Let $\mathfrak{S}$ be a d-monoid. Then the decomposition according to* 5.2.7 induced by *e is even an* inner direct decomposition *of* $\mathfrak{C}$ *into the induced kernels of σ and ρ.*

PROOF. We show first that any $c\in C$ has a decomposition into $c=c_1\cdot c_2$ with $c_1\ \rho\ c\ \sigma\ c_2$.

OBSERVE: Since – according to 2.7.13 – coprime elements commute one with another and thereby also with the corresponding inverses, we get first:

$$\begin{array}{rcl} c & = & c^+\cdot c^- \\ & = & (e\wedge c^+)(e*c^+)\cdot((e\wedge c^*)(e*c^*))^{-1} \\ & = & (e\wedge c^+)(e*c^+)\cdot(e*c^*)^{-1}(e\wedge c^*)^{-1} \\ & = & (e\wedge c^+)(e\wedge c^*)^{-1}\cdot(e*c^+)(e*c^*)^{-1} \\ & =: & c_1\cdot c_2 \end{array}$$

with $c_1 \,\rho\, c$, since
$$\begin{array}{rcl} e \wedge c^* e \wedge c^* c^+ & = & e \wedge c^+ e \wedge c^+ c^* \\ & \rightsquigarrow & \\ c^*(e \wedge c^+) & \rho & c^+(e \wedge c^*) \\ & \rightsquigarrow & \\ c_1 = (e \wedge c^+)(e \wedge c^*)^{-1} & \rho & c^+ c^{*\,-1} = c\,, \end{array}$$

and $c_2 \,\sigma\, c$, since
$$\begin{array}{rcl} e(e * c^+) = ec^+ & = & ecc^* = ec(e * c^*) \\ & \rightsquigarrow & \\ e * c^+ & \sigma & c(e * c^*) \\ & \rightsquigarrow & \\ c_2 = (e * c^+)(e * c^*)^{-1} & \sigma & c\,. \end{array}$$

Furthermore we get

$$\begin{array}{rl} & C_\sigma := \{c \in C \mid ce = e\} = \ker \sigma \\ \& & C_\rho := \{c \in C \mid e \perp |\, c\,|\,\} = \ker \rho\,. \end{array}$$

Observe: The first assertion is evident and the second one follows from $c \in C_\rho \Longrightarrow c \,\rho\, 1$ – since

$$\begin{array}{lrcl} & c & \rho & 1 \\ & & \Longrightarrow & \\ & c^+ & \rho & c^* \\ \Longrightarrow & es^+s^- \wedge c^+ & = & es^+s^- \wedge c^* \quad (\exists\, s \in S) \\ \Longrightarrow & es^+ \wedge c^+s^* & = & es^+ \wedge c^*s^* \\ & & = & es^+ \wedge c^+s^* \wedge c^*s^* \\ & & = & es^+ \wedge (c^+ \wedge c^*)s^* \\ & & = & es^+ \wedge s^* \\ & & = & e \wedge s^* \qquad\qquad (2.19) \\ \Longrightarrow & (e \wedge c^+)(e \wedge s^*) & \leq & e \wedge s^* \in C \\ \Longrightarrow & (e \wedge c^+)(e \wedge s^*) & = & 1 \cdot (e \wedge s^*) \in C \\ \Longrightarrow & e \wedge c^+ & = & 1\,, \end{array}$$

since by duality this implication provides $c \,\rho\, 1 \Longrightarrow e \wedge c^* = 1$, that is $c \,\rho\, 1 \Longrightarrow c \in V$. So by 2.7.13 we get for any $c \in C$:

$$\begin{array}{rcl} c & = & (e \wedge c^+)(e \wedge c^*)^{-1} \cdot (e * c^+)(e * c^*)^{-1} \\ & = & c_1 \cdot c_2 \quad (c_1 \in C_\sigma\,,\, c_2 \in C_\rho) \end{array}$$

and thereby according to 5.2.7

(17.6) $$C_\sigma \cap C_\rho = \{1\} \quad \& \quad C_\sigma \cdot C_\rho = C\,.$$

But – by 13.5.2 – this leads to: $\mathfrak{C} = \mathfrak{C}_\sigma \otimes \mathfrak{C}_\rho$.

Thus the proof is complete. $\square$

Next we get:

17. 1. 3 Proposition. *Let $\mathfrak{S}$ be an arbitrary d-monoid and let $u, v \in S$ be idempotent. Then any $a \in u \cdot C$ admits a unique decomposition of type $a = u \cdot c_a$ with $u \perp |\, c_a \,| \in C$, and in case of $a = u \cdot c_a$, $b = v \cdot c_b$ there hold the equations:*

$$\begin{array}{lrcl} & uc_a \cdot vc_b & = & uv \cdot (v * c_a^+)(v * c_a^*)^{-1}(u * c_b^+)(u * c_b^*)^{-1} \\ (\mathbf{P}) & & \textit{with} & \\ & uv & \perp & \left|\, (v * c_a^+)(v * c_a^*)^{-1}(u * c_b^+)(u * c_b^*)^{-1} \,\right| \\ & uc_a \wedge vc_b & = & (u \wedge v) \cdot (u \wedge (c_b : c_a))(v \wedge (c_a : c_b))(c_a \wedge c_b) \\ (\mathbf{D}) & & \textit{with} & \\ & (u \wedge v) & \perp & |\, (u \wedge (c_b : c_a))(v \wedge (c_a : c_b))(c_a \wedge c_b) \,| \end{array}$$

PROOF. Let $w \cdot c$ be an element with $w = w^2$ and $c \in C$. Then it holds $w = w(w \wedge c^*) = w(w \wedge c^+)$ and thereby

$$\begin{array}{rrcl} & wc & = & w \cdot (w \wedge c^+)(w \wedge c^*)^{-1}(w * c^+)(w * c^*)^{-1} \\ & & = & w \cdot (w * c^+)(w * c^*)^{-1} \\ \text{with} & w & \perp & \left|\, (w * c^+)(w * c^*)^{-1} \right| . \end{array}$$

In addition this product is uniquely determined, since:

$uc = vd$ & $u \perp |\, c \,|, v \perp |\, d \,|$ leads to $u(c : d) = v(d : c)$ that is $c : d \leq v$ and $d : c \leq u$ – recall (2.19) – and thereby to $u(d : c)(c : d) = v(c : d)(d : c)$, meaning $u = v$, by cancellation. So, we get $u \cdot cc^*d^* = u \cdot dc^*d^*$ leading to $cc^*d^* = dc^*d^*$ – recall again (2.19) – that is $c = d$.

Next we turn to **(D)**. Here the first line follows from (2.17) while the second line follows from 2.7.2.

So, let's turn to **(P)** and suppose that $u \perp |\, c_a \,|$. Then $u * c_a^+ = c_a^+$. As an example we obtain

$$uv * c_a^+ \;=\; v * (u * c_a^+) = v * c_a^+ \tag{17.9}$$

and thereby – in general – the asserted *product formula.*

Finally the asserted orthogonality results according to 2.7.13.

This leads to property **(P)** whereby the proof is complete. □

Now we are in the position to prove a first crucial result in the context of separatively.

17. 1. 4 Proposition. *Let $\mathfrak{S}$ be an arbitrary d-monoid. Then $\mathfrak{E}\cdot\mathfrak{C}$ is a separative sub-d-monoid of $\mathfrak{S}$.*

PROOF. As just shown, $E\cdot C$ is operatively closed. Furthermore axiom (A4) is satisfied, since cancellative elements a,b with $R(a,b,a^\circ,b^\circ)$ fulfil:

$$\begin{aligned} ua \leq vb &\Longrightarrow ua^\circ \leq vb^\circ \\ &\Longrightarrow a^\circ \leq v \\ &\Longrightarrow (ua^\circ)(vb^\circ) = vb^\circ \\ &\Longrightarrow (ua)(vb^\circ) = vb\,. \end{aligned}$$

So it remains to verify that $E\cdot C$ is separative. To this end choose elements $u,v\in E$ and $a,b\in C$ and suppose $u\perp|\,a\,|$, $v\perp|\,b\,|$, and

$$\begin{aligned} ua\cdot ua &= ua\cdot vb \\ vb\cdot vb &= vb\cdot ua\ . \end{aligned}$$

Then it follows:
$$\begin{array}{ccc} ua = uvb & \& & vb = uva \\ & \leadsto & \\ ua \geq vb & \& & vb \geq ua\,. \end{array}$$ □

Let now with each idempotent element e be associated the function ψ_e defined by

$$\psi_e:\ \ ec \ \longmapsto\ (e*c^+)(e*c^*)^{-1}\,. \tag{17.10}$$

ψ_e maps any ec to its uniquely determined cancellable and in addition e-orthogonal part. In particular this leads to monomorphisms $\phi_{e,1}$.

Recall: different elements ex, ey have different components $\psi_e(ex)$, $\psi_e(ey)$ and the homomorphism property by definition results from the above proposition 17.1.3.

The general relevance of this definition stems from the fact that it concerns all $u\cdot\mathfrak{C}$ $(u\in E)$, since $u\cdot\mathfrak{S}$ is a d-semigroup with identity u. So, in case of $u,v\in E$ the mapping

$$\psi_{u,u\wedge v}: uc \ \longmapsto\ (u\wedge v)\cdot\psi_u(uc) \tag{17.11}$$

provides a monomorphism of $u\mathfrak{C}$ onto $(u\wedge v)\mathfrak{C}$, and the set of these monomorphisms is directed, that is it satisfies

$$\psi_{u,u\wedge v}\circ\psi_{u\wedge v\,,\,u\wedge v\wedge w} \;=\; \psi_{u\,,\,u\wedge v\wedge w}\,. \tag{17.12}$$

Now we turn to the interplay of the homomorphisms

$$\phi_{u,u\vee v} \quad \text{and} \quad \psi_{u,u\wedge v}\,.$$

As a first equation we get:

$$\psi_{u,u\wedge v}\circ\phi_{u\wedge v,u} \;=\; \phi_{u,u}\;, \tag{17.13}$$

and it follows as a second equation:

$$\psi_{u,u\wedge v}\circ\phi_{u\wedge v,v} \;=\; \phi_{u,u\vee v}\circ\psi_{u\vee v,v}\,. \tag{17.14}$$

PROOF. Let $u\in E$, $c\in C$ be chosen with $u\perp|\,c\,|$, in particular suppose $u*c^+=c^+$ and $u*c^*=c^*$. Then – recall that v is central – according to $uv=u\vee v$ and $v(v*c^*)=vc^*\rightsquigarrow v(v*c^*)^{-1}=vc^{*-1}$ it follows:

$$\begin{aligned}
uc\,\phi_{u,u\vee v}\circ\psi_{u\vee v,v} &= vu\cdot c\,\phi_{u\vee v,v}\\
&= (uv\wedge v)\cdot(uv*c^+)(uv*c^*)^{-1}\\
&= v\cdot(v*(u*c^+))(v*(u*c^*))^{-1}\\
&= v\cdot(v*c^+)(v*c^*)^{-1}\\
&= v\cdot c\\
&= v\cdot(u\wedge v)c\\
&= v(u\wedge v)(u*c^+)(u*c^*)^{-1}\\
&= uc\,\psi_{u,u\wedge v}\circ\phi_{u\wedge v,v}\,.
\end{aligned}$$

□

Thus a semigroup theoretical approach to [78] is realized.

17.2 Separative congruences

17. 2. 1 Definition. A semigroup $\mathfrak{S}$ is called *separative,* cf. [38], if it satisfies:

$$\textbf{(S)}\qquad \begin{matrix} ab=aa\\ \&\\ ba=bb\end{matrix} \quad\vee\quad \begin{matrix} ab=bb\\ \&\\ ba=aa\end{matrix} \quad\Longrightarrow\quad a=b\,.$$

In particular any inverse d-semigroup is separative, which follows immediately from $a = aa^{-1}a = a^{-1}aa = a^{-1}a \cdot b \Longrightarrow a \geq b$.

17. 2. 2 Proposition. *A semigroup $\mathfrak{S}$ is separative if and only if it satisfies one of the following conditions:*

$$(\mathbf{S}') \qquad \begin{array}{ccc} aba & = & aaa \\ & \& & \\ bab & = & bbb \end{array} \Longrightarrow \quad a = b \qquad .$$

$$(\mathbf{S}'') \qquad \begin{array}{l} aa = ab = bb \Longrightarrow a = b \\ \& \quad axa = aya \Longrightarrow ax = ay \;\&\; xa = ya \end{array}$$

$$(\mathbf{S}''') \qquad \begin{array}{l} aa = ab = bb \Longrightarrow a = b \\ \& \quad axb = ayb \Longrightarrow abx = aby \;\&\; xab = yab\,. \end{array}$$

PROOF. $(\mathbf{S}) \Longrightarrow (\mathbf{S}')$, since by $(\mathbf{S})$ it follows:

$$aba = aaa \quad \Longrightarrow \quad \begin{array}{ccc} aa \cdot ba & = & aa \cdot aa \\ & \& & \\ ba \cdot aa & = & ba \cdot ba \end{array} \quad \Longrightarrow \quad aa = ba\,,$$

that is – by symmetry – axiom $(\mathbf{S}')$.

$(\mathbf{S}') \Longrightarrow (\mathbf{S}'')$, since $(\mathbf{S}')$ implies first:

$$aa = ab = bb \quad \Longrightarrow \quad \begin{array}{ccc} aba & = & aaa \\ & \& & \\ bab & = & bbb \end{array} \quad \Longrightarrow \quad a = b\,,$$

and thereby:

$$axa = aya \quad \Longrightarrow \quad \begin{array}{ccc} ax \cdot ay \cdot ax & = & ax \cdot ax \cdot ax \\ & \& & \\ ay \cdot ax \cdot ay & = & ay \cdot ay \cdot ay\,. \end{array} \quad \Longrightarrow \quad ax = ay\,,$$

which leads – again by symmetry – to axiom $(\mathbf{S}'')$.

$(\mathbf{S}'') \Longrightarrow \mathbf{S}''')$, since from $(\mathbf{S}'')$ it follows first $xa = ya \Longleftrightarrow ax = ay$, and hereby furthermore

$$\begin{array}{rrcl}
 & axb & = & ayb \\
\Longrightarrow & xb \cdot a & = & yb \cdot a \\
\Longrightarrow & bx \cdot ba & = & by \cdot ba \\
\Longrightarrow & ba \cdot bx & = & ba \cdot by \\
\Longrightarrow & b \cdot abxa & = & b \cdot abya \\
\Longrightarrow & ab \cdot x \cdot ab & = & ab \cdot y \cdot ab \\
\Longrightarrow & ab \cdot x & = & ab \cdot y \\
 & & \& & \\
 & x \cdot ab & = & y \cdot ab \,,
\end{array}$$

leading to **(S‴).**

(S‴) $\Longrightarrow$ (S), since we get first

$$\begin{array}{rcl}
ab = aa & \& & ba = bb \\
 & \Longrightarrow & \\
bab & = & bbb \\
 & \Longrightarrow & \\
a \cdot bb & = & bb \cdot a
\end{array}$$

and thereby according to **(S‴)**

$$\begin{array}{rcl}
ab = aa & \& & ba = bb \\
 & \Longrightarrow & \\
ab \cdot ab & = & ab \cdot ba \\
 & = & bb \cdot aa \\
 & = & bb \cdot ba \\
 & = & ba \cdot ba \\
 & \Longrightarrow & \\
aa = & ab & = bb \\
 & \Longrightarrow & \\
a & = & b \,.
\end{array}$$

This leads – again by symmetry – to condition **(S).** □

17. 2. 3 Lemma. *A d-monoid $\mathfrak{S}$ is separative iff its cone $\mathfrak{P}$ is separative.*

PROOF. Let $ab = aa$ & $ba = bb$. We multiply from right with $(a \wedge b)^*$ and from left with suitable positive elements x, y satisfying.

$$xa = a(a \wedge b)^* \quad \text{and} \quad yb = b(a \wedge b)^* .$$

Thus we get

$$xa \cdot b(a \wedge b)^* = xa \cdot a(a \wedge b)^* \ \& \ yb \cdot a(a \wedge b)^* = yb \cdot b(a \wedge b)^*$$

that is

$$a(a\wedge b)^* \cdot b(a\wedge b)^* = a(a\wedge b)^* \cdot a(a\wedge b)^* \ \& \ b(a\wedge b)^* \cdot a(a\wedge b)^* = b(a\wedge b)^* \cdot b(a\wedge b)^* ,$$

which implies

$$a(a \wedge b)^* \;=\; b(a \wedge b)^* .$$

Let e now be a common identity of a, b and suppose that $e = u(e \wedge (a \wedge b))$. Then we obtain

$$\begin{aligned} a &= a \cdot u(e \wedge (a \wedge b))(a \wedge b)^*(e \wedge (a \wedge b)) \\ &= b \cdot u(e \wedge (a \wedge b))(a \wedge b)^*(e \wedge (a \wedge b)) = b . \end{aligned}$$ □

17. 2. 4 Lemma. *If $\mathfrak{S}$ is a separative d-monoid, then its* 1*-Extension* $\sum$ *is separative, too.*

PROOF. Each element of $\sum^+ \backslash S^+$ is cancellative and of type 1, or of type $(1 \wedge b)^{-1}$, or of type $(1 \wedge a)(1 \wedge b)^{-1}$. □

The next result is based on proposition 5.3.4.

17. 2. 5 Proposition. *Let $\mathfrak{S}$ be a d-semigroup. Then the following are pairwise equivalent:*

- (i) *$\mathfrak{S}$ is separative*
- (ii) *$\mathfrak{S}$ is a (distributive) lattice of cancellative lattice semigroups.*
- (iii) *If η is the finest idempotent congruence, then any η-class is cancellative.*

PROOF. $(i) \Longrightarrow (ii)$. If $\mathfrak{S}$ is separative then $a \equiv b \Longleftrightarrow ax = ay \Longleftrightarrow bx = by$ defines a congruence with operatively closed cancellative classes.

Clearly $\equiv$ is an equivalence relation and the congruence property for multiplication follows immediately, since $\mathfrak{S}$ is assumed to be separative.

Assume now $b \equiv c$. Then by (A4) it follows again immediately:

$$\begin{aligned}(a \wedge b)x = (a \wedge b)y &\Longrightarrow ax = ay \;\&\; bx = by\\ &\Longrightarrow ax = ay \;\&\; cx = cy\\ &\Longrightarrow (a \wedge c)x = (a \wedge c)y\,,\end{aligned}$$

leading to $a \wedge b \equiv a \wedge c$.

In a similar manner we get that the classes are closed under $\wedge$. A bit more difficult it is to show that the classes are also closed and cancellative under multiplication. To this end we start from $a \equiv b$. By $(\mathbf{S}''')$ this implies S/σ is a homomorphic image of the wanted type, and assume – for the sake of convenience – that $\mathfrak{S}$ itself is (already) the considered image.

We get first: Any non cancellable element x generates a proper separative congruence by $c \equiv d :\Longleftrightarrow cx = dx$. Clearly this is a congruence – recall (S'''). Moreover $\equiv$ is separative, because – choose a common unit x of u and v

$$\begin{array}{rcl} uv \equiv uu & \& & vu \equiv vv\\ & \Longrightarrow & \\ uv \cdot xx = uu \cdot xx & \& & vu \cdot xx = vv \cdot xx\\ & \Longrightarrow & \\ ux \cdot vx = ux \cdot ux & \& & vx \cdot ux = vx \cdot vx\\ & \Longrightarrow & \\ ux & = & vx\,,\\ & \Longrightarrow & \\ u & = & v\,. \end{array}$$

But on the one hand this means that at least one of the elements a, b is cancellative – whence $\mathfrak{S}$ is a monoid – since otherwise it would result $aa = ba$ & $ab = bb$, and on the other hand this means that any $x \notin C$ satisfies $ax = bx$. Consequently $S = C$ or $S \backslash C$ must be a d-ideal because

$$\begin{aligned} x, y \in S\backslash C &\Longrightarrow a(x \wedge y) = b(x \wedge y)\\ &\Longrightarrow x \wedge y \in S\backslash C\\ &\quad\;\&\;\; sx \in S\backslash C \qquad (\forall\, s \in S)\,. \end{aligned}$$

Hence in case of $S \neq C$ we are in the position to decompose $\mathfrak{S}$ by $\mathfrak{o} := S\backslash C$, and it will turn out that this congruence is separative. Idea: $S\backslash C$ collapses to zero and the elements of C remain cancellable.

In order to verify this, we start from $x \in \mathfrak{o}$, $c \in C$, $(x \wedge c)x' = x$, and $s, t \in S^+$. Then it follows $x' \in \mathfrak{o}$ and

$$\begin{array}{rcl} x \wedge cs & = & x \wedge ct \\ & \Longrightarrow & \\ (x \wedge c)(x' \wedge s) & = & (x \wedge c)(x' \wedge t) \\ & \Longrightarrow & \\ x' \wedge s & = & x' \wedge t \\ & \Longrightarrow & \\ s & \equiv & t \bmod \mathfrak{o}\,. \end{array}$$

Thus, by $axb = ayb \Longrightarrow abx = aby$, we get first for negative elements $s, t \in S$

$$\begin{array}{rcl} c \cdot s \equiv c \cdot t & \Longrightarrow & c \cdot st^{-1} \equiv c \cdot tt^{-1} \\ & \Longrightarrow & c \cdot t^{-1}s \equiv c \\ & \Longrightarrow & c \cdot t^{-1} \equiv c \cdot s^{-1} \\ & \Longrightarrow & s \equiv t \end{array}$$

and thereby for arbitrary elements s, t

$$c \cdot s \equiv c \cdot t \Longrightarrow c \cdot (1 \vee s) \equiv c \cdot (1 \vee t) \ \&\ c \cdot (1 \wedge s) \equiv c \cdot (1 \wedge t) \Longrightarrow s \equiv t\,.$$

Therefore we are through once we have shown that the congruence modulo $\mathfrak{o}$ separates a, b. For, in this case $\mathfrak{S}$ itself is a cancellative d-semigroup, with or without zero element.

So, let us assume that x belongs to $\mathfrak{o}$ and satisfies $x \wedge a = x \wedge b$ and – see above – $ax = bx$. Then in case $R(a, b, a', b')$ it follows

$$\begin{array}{lrcll} & (a \wedge b) \cdot a'x & = & (a \wedge b) \cdot b'x & \\ \leadsto & a' \cdot x & = & b' \cdot x & (a \wedge b \in C) \\ \leadsto & (b \wedge x) \cdot a' & = & (a \wedge x) \cdot b' & (ab' = ba' \ \&\ S'') \\ \leadsto & (a \wedge b \wedge x) \cdot a' & = & (a \wedge b \wedge x) \cdot b' & (a \wedge x = b \wedge x) \\ \leadsto & a' & = & b' & \\ \leadsto & a & = & b\,. & \end{array}$$

This completes the proof. □

The preceding proposition entails

17. 2. 6 Corollary. *Let $\mathfrak{S}$ be a d-semigroup. Then the following are pairwise equivalent:*

(*i*) $\mathfrak{S}$ *is separative*

(*ii*) $\mathfrak{S}$ *is a subdirect product of cancellative d-semigroups with or without zero*

(*iii*) $\mathfrak{S}$ *admits an embedding into an inverse d-monoid.*

Finally we are in the position to characterize the *finest separative congruence* on arbitrary d-semigroups.

17. 2. 7 Proposition. *The finest separative congruence of a d-semigroup* $\mathfrak{S}$ *is equal to the intersection of all congruences of type*

$$a\,\sigma\,b \Longleftrightarrow xay \equiv xby\,(\,\mathfrak{p}\,) \quad (x, y \notin\ \mathfrak{p}, \quad \mathfrak{p}\, a \text{ prime } d\text{-ideal}).$$

intersected with the finest cancellative congruence κ*.*

PROOF. First of all the congruences under consideration are separative. So they contribute to the intersection of all separative congruences.

It remains to verify that each pair a, b that is separated by some separative congruence, is (already) separated by a congruence of the given type. To this end observe:

If a and b are separated by a separative congruence ρ, then – according to 17. 2.6 – a and b are also separated in some $\mathfrak{S}/\sigma$, cancellative with or without zero.

Clearly, if $\mathfrak{S}/\sigma$ is cancellative, then a and b are separated by κ.

And, if otherwise $\mathfrak{S}/\sigma$ is cancellative with a zero element 0, then the inverse image of 0 in $\mathfrak{S}$ is a prime d-ideal, generating a congruence in the sense of the theorem, finer than σ. □

Chapter 18

Inverse divisibility structures

18.1 Inverse left d-semigroups

To begin with, we study a problem of McAlister, answered in a theorem of Billhardt. In [78] McAlister puts the question, whether in the inverse case it suffices to require merely left quotients, that is to replace (A4) by

$$\text{(A4')} \qquad a \leq b \implies \exists x :\ ax = b\,.$$

Clearly: If $\mathfrak{S}$ is *inverse,* then it holds

$$a|_\ell\, b \Longleftrightarrow aa^{-1}bb^{-1} = bb^{-1} \Longleftrightarrow aa^{-1}|_\ell\, bb^{-1}\,.$$

In order to show that along with $a\,|_\ell\, b$ also $a\,|_r\, b$ is satisfied, it suffices to verify, that idempotents are central, since in this case we get first

$$aa^{-1} = aa^{-1}aa^{-1} = a^{-1}a \cdot aa^{-1} = aa^{-1} \cdot a^{-1}a = a^{-1}a \cdot a^{-1}a = a^{-1}a$$

and thereby furthermore

$$a \leq b \Longrightarrow a\,|_\ell\, b \Longrightarrow b = aa^{-1} \cdot b = b \cdot aa^{-1} = ba^{-1} \cdot a \Longrightarrow a|_r\, b\,.$$

Consequently the McAlister question is answered once it is verified that inverse right-d-semigroups have central idempotents.

A first proof verification of this fact was given by Billhardt, however, in his unpublished paper he applied a *subdirect decomposition* (by Zorns lemma), after verifying that $\mathfrak{S}$ is a *cdl*-semigroup. Furthermore his note requires $a \leq ae \wedge ea$ for all idempotents.

Here we give an *elementary proof* due to the author, presented first in [**?**] and published later in [32].

To this end we start with some rules of arithmetic, developed for inverse semigroups, satisfying the axioms (A1),...,(A3) and (A4') and show first of all, that idempotent elements are positive.

Let $u = u^2$ & $v = v^2$. Then by calculation we get:

$$(u \wedge v)^2 = (u \wedge v)^3 = ... = (u \wedge v)^n ...... \tag{18.2}$$

and furthermore

$$(u \wedge v) \cdot (u \wedge v)(u \wedge v)^{-1} = (u \wedge v)(u \wedge v)^{-1} \cdot (u \wedge v)\,. \tag{18.3}$$

But $(u \wedge v) \cdot (u \wedge v)^{-1} \cdot (u \wedge v)$ is a left divisor of u. Hence we get:

$$\begin{aligned} u &= (u \wedge v)(u \wedge v)^{-1}(u \wedge v) \cdot x \;\; (\exists x \in S) \\ &= (u \wedge v)(u \wedge v)(u \wedge v)^{-1} \cdot x \\ &= (u \wedge v)(u \wedge v)(u \wedge v)(u \wedge v)^{-1} \cdot x \\ &= (u \wedge v)(u \wedge v)(u \wedge v)^{-1}(u \wedge v) \cdot x \\ &= (u \wedge v)u \\ &= u(u \wedge v)\,, \end{aligned} \tag{18.4}$$

that is, by symmetry,

$$(u \wedge v)^1 = (u \wedge v)^2 \tag{18.5}$$

and moreover

$$\begin{aligned} u \cdot (u \wedge v) &= u \wedge uv = u \\ &\rightsquigarrow u \leq uv = vu\,. \end{aligned} \tag{18.6}$$

By $a = (aa^{-1}) \cdot a = a \cdot (a^{-1}a)$, this means further, that idempotent elements e are positive, that is satisfy $se \wedge es \geq s$, and moreover this means for positive elements a:

$$\begin{aligned} a^{-1} \leq a \cdot a^{-1} &\rightsquigarrow aa^{-1} = a^{-1}x \;\; (\exists x \in S) \\ &\rightsquigarrow a^{-1}a \cdot aa^{-1} = aa^{-1} \\ &\rightsquigarrow a^{-1}a \leq aa^{-1} \end{aligned} \tag{18.7}$$

Now we are in the position to show:

18. 1. 1 Lemma. *The positive elements a of $\mathfrak{S}$ satisfy – even*

$$a \cdot a^{-1} = a^{-1} \cdot a\,.$$

PROOF.
$$\begin{aligned} a \cdot a^{-1} &\overset{(18.7)}{=} aa^{-1}a^{-1} \cdot aaa^{-1} \\ &= (aaa^{-1})^{-1} \cdot (aaa^{-1}) \\ &= (aaa^{-1} \wedge aa)^{-1} \cdot (aaa^{-1} \wedge aa) \\ &= ((aaa^{-1}a^{-1} \wedge a)a)^{-1} \cdot (aaa^{-1}a^{-1} \wedge a)a \\ &= a^{-1} \cdot \big(aaa^{-1}a^{-1} \wedge a\big)^{-1} \cdot \big(aaa^{-1}a^{-1} \wedge a\big) \cdot a \\ &\overset{(18.7)}{\leq} a^{-1} \cdot \big(aaa^{-1}a^{-1} \wedge a\big) \cdot \big(aaa^{-1}a^{-1} \wedge a\big)^{-1} \cdot a \\ &= a^{-1} \cdot aa^{-1} \cdot a \\ &= a^{-1} \cdot a \\ &\overset{(18.7)}{\leq} a \cdot a^{-1} \end{aligned}$$
□

Let next u be idempotent and x be positive. Then, by 18.1.1, we obtain:

$$\begin{aligned} x \in P(S) \quad &\rightsquigarrow \quad xu \cdot ux^{-1} = ux^{-1} \cdot xu \\ &\rightsquigarrow \quad xux^{-1}x = x^{-1}xux \\ &\overset{(18.7)}{\rightsquigarrow} \quad xu = ux\,. \end{aligned}$$

the final implication by $x^{-1}x = xx^{-1}$.

Let now again a be positive and let e be an idempotent unit of a, for instance choose $a^{-1}a$. Then it follows

$$(e \wedge a)(e \wedge a)^{-1} \cdot a = a \text{ with } (e \wedge a)^{-1} \cdot (e \wedge a) \leq (e \wedge a)^{-1} \cdot a\,.$$

Thus a is *splitted* into $e \wedge a$ and a *positive* factor. So, we are through once we have shown that idempotent elements commute with any $e \wedge a$ of the given type. Here we get:

$$\begin{aligned} (e \wedge a) \leq e \;\rightsquigarrow\; &(e \wedge a)(e \wedge a)^{-1} \leq e(e \wedge a)^{-1} = ((e \wedge a) \cdot e)^{-1} \\ \rightsquigarrow\; &(e \wedge a)(e \wedge a)^{-1} \leq (e \wedge a)^{-1}\,. \end{aligned}$$

Consequently $(e \wedge a)^{-1}$ is positive and therefore an element commuting with all idempotents. Therefore all idempotent elements are central, since $u = u^2 \;\&\; us^{-1} = s^{-1}u \Longrightarrow su = us$, recall $(ab)^{-1} = b^{-1}a^{-1}$.

Henceforth $\mathfrak{S}$ is assumed to be an inverse d-semigroup.

Since the idempotents of a d-semigroup are *central*, a d-semigroup $\mathfrak{S}$ is even inverse whenever it is regular, i. e. if $\mathfrak{S}$ for any $a \in S$ contains an element a' satisfying $a \cdot a' \cdot a = a$. Suppose now $axa = a$. Then the element $z = xax$ even satisfies $aza = a$ & $zaz = z$. And by the d-property we get in addition that, given two elements x, y satisfying $axa = a = aya$ and $xax = x$, $yay = y$, are equal because $(ax)^2 = ax$ and $(ay)^2 = ay$ lead to

$$x = xaxax = xayax = xaxay \ = \ xayay = yaxay = yayay = y \ .$$

Before continuing, recall that inverse d-semigroups satisfy $aa^{-1} = a^{-1}a$ which leads to $a \,|_\ell\, b \Longleftrightarrow aa^{-1} \leq bb^{-1} \Longleftrightarrow a \,|_r\, b$.

Now we give a first structure theorem for inverse d-semigroups.

18. 1. 2 Proposition. *A d-semigroup $\mathfrak{S}$ is inverse if it satisfies $\mathfrak{S} = \mathfrak{E} \cdot \mathfrak{C}$.*

PROOF. If C is empty we are through. Otherwise $\mathfrak{S}$ is a monoid, and it follows $a = (1 \vee a)(1 \wedge a)$ with $1 \vee a = a^+$. Hence we may restrict our attention to positive elements. We get:

$$\begin{aligned} a = a^+ \ &\Longrightarrow \ aa^{-1} \leq a \\ &\Longrightarrow \ aa^{-1} = a(1 \wedge a^{-1}) \\ &\Longrightarrow \ a = aa^{-1} \cdot (1 \wedge a^{-1})^{-1} \,, \end{aligned}$$

where aa^{-1} is idempotent and $(1 \wedge a^{-1})^{-1}$ is cancellable. $\square$

As two further formulas we present

$$aa^{-1} \wedge bb^{-1} \ = \ (a \wedge b)(a \wedge b)^{-1} \tag{18.8}$$

$$aa^{-1} \vee bb^{-1} \ = \ (a \vee b)(a \vee b)^{-1} \,, \tag{18.9}$$

where (18.8) holds, since the right side is obviously contained in the left side and since by the equation $a \wedge b = a \wedge bb^{-1}a \wedge b \wedge aa^{-1}b = (aa^{-1} \wedge bb^{-1})(a \wedge b)$ the left side is contained in the right side, hint: multiply from right with $(a \wedge b)^{-1}$,

and where (18.9) holds, since the left side L is obviously contained in the right side and since by $a \vee b = ab'$ with $b' \,|_r\, b$ we get

$$(a \vee b)(a \vee b)^{-1} = (ab')(b'^{-1}a^{-1}) = aa^{-1} \cdot b'b'^{-1}$$

whence also the right side R is contained in the left side, hint: $LR = L$.

Observe furthermore, that 18.8 holds already if in $(S, \cdot, \wedge)$ only left divisors are required!

18.2 Representation

First of all we consider the coarsest congruence with *operationally closed cancellative classes.* This congruence admits a most elementary description, since by defining $ax = ay \Longleftrightarrow xa = ya$ and $xx^{-1} = x^{-1}x$ we are led to the equivalence:

$$ax = ay \Longleftrightarrow bx = by \ \text{ iff } \ aa^{-1} = bb^{-1} \ . \tag{18.10}$$

This is evident from the right to the left side, and starting from the left side it follows for any common unit e of a and b

$$aaa^{-1} = ae \Longrightarrow baa^{-1} = be \ \Longrightarrow \ b^{-1}b \cdot aa^{-1} = b^{-1}b \Longrightarrow aa^{-1} \,|\, bb^{-1} \ ,$$

which completes the proof by duality.

It was shown already below 5.4.1 that a subdirectly irreducible d-semigroup contains at most two idempotent elements. This implies nearly directly the inverse pendant to 17.2.6:

18. 2. 1 Proposition. *Any inverse d-semigroup is a subdirect product of ℓ-groups with or without an zero element.*

PROOF. Any homomorphic image $\mathfrak{S}$ of an inverse d-semigroup is inverse.

Let now a, b be a critical pair. Then $aa^{-1} \wedge bb^{-1}$ is an a, b separating idempotent, and hence the identity of $\mathfrak{S}$. If in addition $aa^{-1} \wedge bb^{-1}$ is the only idempotent then $\mathfrak{S}$ an ℓ-group.

Otherwise there exists exactly one further idempotent, acting as zero element. So in this case $\mathfrak{S}$ is an ℓ-group with zero. □

Thus the pendant of 17.2.6 turns out as an easy consequence of the general proposition 5.4.1.

Let now $\mathfrak{S}$ be even a subdirect product of ℓ-groups and d-lattices. Then the lattice components on the one hand and the ℓ-group components on the other hand may be combined to an ℓ-group $\mathfrak{G}$ and to a d-lattice $\mathfrak{L}$, respectively. Hence, in this case $\mathfrak{S}$ is representable as a subdirect product $\mathfrak{L} \,|\, \mathfrak{G}$ of $\mathfrak{L}$ and $\mathfrak{G}$.

But it holds more, in fact in the above situation it holds even $\mathfrak{S} = \mathfrak{L} \otimes \mathfrak{G}$. In particular:

18. 2. 2 Proposition. *Let $\mathfrak{S}$ be an inverse d-semigroup. Then the following are pairwise equivalent:*

(*i*) $\mathfrak{S}$ *is a subdirect product of some d-lattice* $\mathfrak{L}$ *and some ℓ-group* $\mathfrak{G}$.

(*ii*) $\mathfrak{S}$ *is a direct product of some d-lattice* $\mathfrak{L}$ *and some ℓ-group* $\mathfrak{G}$.

(*iii*) $\mathfrak{S}$ *satisfies:* $(aa^{-1} \wedge (b \vee cc^{-1}))^2 = aa^{-1} \wedge (b \vee cc^{-1})$.

PROOF. $(i) \Longrightarrow (ii)$. Start from $(u \,|\, r)$ and $(v \,|\, s)$. It has to be shown w. l. o. g. that also $(u \,|\, s)$ is contained in the subdirect product $\mathfrak{V} \,|\, \mathfrak{G}$. We succeed as follows:

$$\begin{aligned}
(u \,|\, r), (v \,|\, s) \in V \,|\, G &\Longrightarrow (u \,|\, r^{-1}), (v \,|\, s^{-1}) \in V \,|\, G \\
&\Longrightarrow (u \,|\, 1), (v \,|\, 1) \in V \,|\, G \\
&\Longrightarrow (u \wedge v \,|\, 1 \wedge s^{-1}), (u \,|\, 1) \in V \,|\, G \\
&\Longrightarrow (u \wedge v \,|\, 1 \vee s), (u \wedge v \,|\, 1 \wedge s) \in V \,|\, G \\
&\Longrightarrow (u \wedge v \,|\, s) \in V \,|\, G \\
&\Longrightarrow (u \,|\, 1)(u \wedge v \,|\, s) \in V \,|\, G \\
&\Longrightarrow (u \,|\, s) \in V \,|\, G.
\end{aligned}$$

$(ii) \Longrightarrow (iii)$. By evidence, the equation (iii) is satisfied in both, in d-lattices and in ℓ-groups.

$(iii) \Longrightarrow (i)$.

Consider some subdirectly irreducible component. If this component has only one idempotent, then this idempotent is its identity, and the component is an ℓ-group.

Otherwise there exists a zero element 0 different from the identity element 1 . We put in (iii) $a = 1$ and $b = 0$. This implies that all positive elements are idempotent. Consequently in this case this component is a distributive lattice. □

It has already been shown that inverse d-semigroups satisfy $\mathfrak{S} = \mathfrak{E} \cdot \mathfrak{C}$.

Let $\mathfrak{S}$ be an inverse d-semigroup. Then by the introduced functions $\phi_{u,u\vee v}$ and $\psi_{u,u\wedge v}$ we have available two directed systems of homomorphisms $\phi_{\alpha,\alpha\vee\beta}$ and $\psi_{\alpha,\alpha\wedge\beta}$, which facilitates a characterization of inverse d-semigroups by means of special substructures, more precisely by the underlying lattice of idempotents and the groups associated with these idempotents, that is a characterization as it was given for Clifford-semigroups by Clifford. Here one part has already been verified, namely

18. 2. 3 Proposition. *Any inverse d-semigroup satisfies*

(A) $$\phi_{\alpha,\alpha\vee\beta}\circ\psi_{\alpha\vee\beta,\beta}=\psi_{\alpha,\alpha\wedge\beta}\ \circ\ \phi_{\alpha\wedge\beta,\beta}$$

(B) $$x\in G_\alpha\Longrightarrow x\,\psi_{\alpha,\alpha\wedge\beta}\,\phi_{\alpha\wedge\beta,\alpha}=x$$

(C) $$\ker\phi_{\alpha\wedge\beta,\alpha}\cap\ker\phi_{\alpha\wedge\beta,\beta}=\{\alpha\wedge\beta\}\ .$$

Now we will show, that the system (A), (B), (C) is not only necessary but also sufficient.

18. 2. 4 Proposition. *Let* $\mathfrak{D}$ *be a distributive lattice with minimum* 1, *let* $\mathfrak{G}_\alpha$ $(\alpha\in D)$ *be a family of pairwise disjoint* ℓ*-groups and let* $\phi_{\alpha,\alpha\vee\beta}$ *be a family of directed surjective homomorphisms* $\mathfrak{G}_\alpha\longrightarrow\mathfrak{G}_{\alpha\vee\beta}$ *and let* $\psi_{\alpha,\alpha\wedge\beta}$ *be a family of directed homomorphisms* $\mathfrak{G}_\alpha\longrightarrow\mathfrak{G}_{\alpha\wedge\beta}$ *such that the following conditions hold:*

(A) $$\phi_{\alpha,\alpha\vee\beta}\ \circ\ \psi_{\alpha\vee\beta,\beta}=\psi_{\alpha,\alpha\wedge\beta}\ \circ\ \phi_{\alpha\wedge\beta,\beta}$$

(B) $$x\in G_\alpha\Longrightarrow x\,\psi_{\alpha,\alpha\wedge\beta}\,\phi_{\alpha\wedge\beta,\alpha}=x$$

(C) $$\ker\phi_{\alpha\wedge\beta,\alpha}\cap\ker\phi_{\alpha\wedge\beta,\beta}=\{\alpha\wedge\beta\}$$

Then defining for $a\in\mathfrak{G}_\alpha$, $b\in\mathfrak{G}_\beta$

$$\begin{aligned} a\cdot b &:= a\,\phi_{\alpha,\alpha\vee\beta}\cdot b\,\phi_{\beta,\alpha\vee\beta}\\ a\vee b &:= a\,\phi_{\alpha,\alpha\vee\beta}\vee b\,\phi_{\beta,\alpha\vee\beta}\end{aligned}$$

$\bigcup G_\alpha\ \ (\alpha\in D)=:S$ *becomes an* inverse semiring $\mathfrak{S}=(S,\cdot,\vee)$ *such that any* $\mathfrak{G}_\alpha$ *is embedded in* $\mathfrak{S}$, *such that* $\mathfrak{G}_1$ *is the cancellative kernel, and such that the set of the idempotents of* $\mathfrak{G}_\alpha$ *forms the idempotent kernel.*

PROOF. That $(S,\cdot)$ defines a semigroup and $(S,\vee)$ is a semilattice follows nearly by definition and was first noticed by CLIFFORD. Furthermore the reader verifies easily that multiplication distributes over $\vee$, whence in particular multiplication is isotone. So, $\mathfrak{S}$ is a *semilattice semigroup* satisfying $x(a\vee b)y=xa\vee xby$. The corresponding partial order is given by $a\le b\Longleftrightarrow a\cdot\beta\le b$. This should be kept in mind. Furthermore the reader should recall that by construction the elements α, $\beta\dots$ are idempotent and thereby central.

Finally, elements $a \in G_\alpha$ are positive in $\mathfrak{S}$ iff they are positive in $\mathfrak{G}_\alpha$. In particular the identity elements of the various $\mathfrak{G}_\alpha$ are positive. □

Now we identify the identity elements of $\mathfrak{G}_\alpha$ with α. Then $\alpha \wedge \beta$ in $\mathfrak{D}$ will remain the infimum of α and β in $\mathfrak{S}$.

SINCE: Given a positive $c \leq \alpha, \beta$, then with $\gamma := cc^{-1}$ it follows on the one hand $c\,\phi_{\gamma,\alpha} \leq \alpha$ and on the other hand $c\,\phi_{\gamma,\beta} \leq \beta$. This means that $c\,\phi_{\gamma,\alpha\wedge\beta} \vee (\alpha \wedge \beta)$ belongs to the kernel of $\phi_{\alpha\wedge\beta,\alpha}$ and also to the kernel of $\phi_{\alpha\wedge\beta,\beta}$. And this means that $c\,\phi_{\gamma,\alpha\wedge\beta} \vee (\alpha \wedge \beta)$ is equal to $\alpha \wedge \beta$.

Finally, by evidence, $\mathfrak{G}_1$ is the cancellative kernel of $\mathfrak{S}$.

We will detect the structure under consideration as an inverse d-monoid. To this end we remark first that $\mathfrak{S}$ is $\wedge$-closed iff its cone $\mathfrak{S}^+$ is $\wedge$-closed. This is done as follows:

Since cancellable elements are invertible we get:

18. 2. 5 Lemma. *Provided* $\inf(a, b)$ *exists and* $c \in S$ *is cancellative then there exists also* $\inf(c \cdot a, c \cdot b)$ *and it holds:*

$$\inf\,(c \cdot a, c \cdot b) = c \cdot \inf\,(a, b) \ \textit{and} \ \inf\,(a \cdot c, b \cdot c) = \inf\,(a, b) \cdot c\,.$$

PROOF. By assumption $d \leq a \cdot c\,,\, b \cdot c$ is equivalent with $d \cdot c^{-1} \leq a\,,\, b$, whence we succeed by duality. □

Furthermore any element is a product of some positive and some invertible element of type $\alpha \cdot (1 \vee c)(1 \wedge c)$. Hence if $(S^+\,, \vee)$ is $\wedge$-closed we multiply the elements $\alpha \cdot (1 \vee c)(1 \wedge c)$ and $\beta \cdot (1 \vee d)(1 \wedge d)$ from the right with $((1 \wedge c)(1 \wedge d))^{-1}$, construct the infimum of the products in $\mathfrak{S}^+$, and find the wanted $\inf\,(a, b)$ by finally re-multiplying (with $(1 \wedge c)(1 \wedge d)$).

Therefore, let's restrict our considerations to positive elements.

$$\mathfrak{G}_1 \;=\; \ker \phi_{1,\alpha} \otimes \operatorname{im} \psi_{\alpha,1}\,. \tag{18.17}$$

PROOF. Since $\mathfrak{G}_1$ is a group, the elements $c \in G_1$ satisfy,

$$c \;=\; c(c\phi_{1,\alpha}\psi_{\alpha,1})^{-1} \cdot (c\phi_{1,\alpha}\psi_{\alpha,1})\,. \tag{18.18}$$

But by applying the operator $\phi_{1,\alpha}$ the left side and according to (A), (B) also the second component is transferred to $c\phi_{1,\alpha}$.

So the first component is transferred to α, whence $\mathfrak{G}_1 = \ker\phi_{1,\alpha} \cdot \mathrm{im}\,\psi_{\alpha,1}$.

Finally let $a = u \cdot v$ with $u \in \ker\phi_{1,\alpha}$, $v \in \mathrm{im}\,\psi_{\alpha,1}$. Then we get the equation $v = v\phi_{1,\alpha}\psi_{\alpha,1} = a\phi_{1,\alpha}\psi_{\alpha,1}$. Thereby the second component and hence also the first component are uniquely determined, whence it even holds $\mathfrak{G}_1 = \ker\phi_{1,\alpha} \otimes \mathrm{im}\,\psi_{\alpha,1}$. □

The preceding proposition concerns the structure of $\mathfrak{G}_1$, but it is immediately clear that this restriction is negligible since $\mathfrak{G}_\alpha$ is the cancellative part of the homomorphic image $\mathfrak{G}\alpha$ of $\mathfrak{G}$.

It has already been shown, that idempotent elements take along their meet from $\mathfrak{D}$ to $\mathfrak{S}$. We now will show that the set of all pairs $\alpha \cdot c$ with positive and cancellative factor c is inf-closed, which will lead us easily to infima in general. We start with:

18. 2. 6 Lemma. *Under the assumptions of proposition* 18.2.4 *an inverse d-semigroup* $\mathfrak{S}$ *for all pairs* α, c *with* $\alpha \in D$, $c \in C^+$ *satisfies:*

$$c_1 = c \cdot (c\,\phi_{1,\alpha}\,\psi_{\alpha,1})^{-1} = \inf(\alpha,\, c)\,.$$

PROOF. First we get straightforwardly $c_1\alpha = \alpha$, which means $c_1 \le \alpha$, and furthermore it holds $c_1 \le c$, since together with c also $c\phi_{1,\alpha}\,\psi_{\alpha,1}$ is positive.

Suppose now $d \le \alpha, c$. Then it results $1 \vee d \le \alpha, c$, whence d may be assumed to be positive.

So, the decompositions $d_1 \cdot d_2$ and $c_1 \cdot c_2$ – in the sense of (18.18) – on the one hand satisfy $d_1 \le c_1$ and on the other hand satisfy $d_2 = d\phi_{1,\alpha}\,\psi_{\alpha,1} = \alpha\psi_{\alpha,1} = 1$.

Thus the proof is complete □

18. 2. 7 Corollary. *Any pair of elements* $\alpha \cdot \beta$ *and* $\alpha \cdot c$ *with* $c \in C$ *has an infimum.*

PROOF. Consider $(S\alpha, \cdot, \vee)$. This is a monoid with α as identity. □

Now we are in the position to verify as a first principal result:

18. 2. 8 Lemma. *Let* $\mathfrak{S}$ *fulfill the assumptions of* 18.2.4*. Then for any pair* α, a *,* β, b *with* $\alpha, \beta \in D$ *and* $a, b \in C$ *we obtain:*

$$\alpha \cdot a \wedge \beta \cdot b \;=\; (\alpha \wedge \beta) \cdot (\alpha \wedge b) \cdot (\beta \wedge a)(a \wedge b)\,.$$

PROOF. We may start from the special case $\alpha \cdot a$, $\beta \cdot b$ with cancellable and coprime elements a, b – observe:

$$(\alpha a'' \wedge \beta b'')(c \wedge d) \;=\; \alpha c \wedge \beta d\,.$$

But in that case it suffices to show that any $\gamma \cdot c$ with cancellable c, that divides $\alpha \cdot a$ and $\beta \cdot b$ as well, is a divisor of $(\alpha \wedge \beta) \cdot (\alpha \wedge b) \cdot (\beta \wedge a)$. So let $\gamma \cdot c$ be of this type with cancellative c. Then it holds $\gamma \leq \alpha \wedge \beta$, and c is a product of type $c_\alpha \cdot c_a$ with $c_\alpha \leq \alpha$, $c_a \leq a$, recall (18.18). This leads to the further decompositions $c_\alpha = c_{\alpha,\beta} \cdot c_{\alpha,b}$ and $c_a = c_{a,\beta} \cdot c_{a,b}$ with $c_{\alpha,\beta} \leq \alpha \wedge \beta$, $c_{\alpha,b} \leq \alpha \wedge b$, $c_{a,\beta} \leq a \wedge \beta$ and $c_{a,b} \leq a \wedge b = 1$.
Thus the proof is complete. □

It remains to verify (A3) w. r. t. $\wedge$ for idempotent left factors.

18. 2. 9 Lemma. *By* (A), (B), (C) *the structure* $(S^+, \vee)$ *satisfies for all triples* $c \in C$, $\alpha, \beta \in D$ *:*

$$\alpha \cdot (\beta \wedge c) = \alpha \cdot \beta \wedge \alpha \cdot c\ .$$

PROOF. Since $\mathfrak{G}_1$ is an ℓ-group the mappings $\phi_{1,\alpha}$ are also $\wedge$-homomorphisms. Recall again $\alpha \cdot c = c\,\phi_{1,\alpha}$. Hence by 18.2.6 according to 18.2.7 we obtain:

$$\begin{aligned} \alpha \cdot (\beta \wedge c) &= \alpha \left(c \cdot (c\,\phi_{1,\beta}\,\psi_{\beta,1})^{-1}\right) \\ &= (\alpha \cdot c) \cdot (\alpha \cdot (c\,\phi_{1,\beta}\,\psi_{\beta,1}))^{-1} \\ \text{and} \qquad \alpha \cdot \beta \wedge \alpha \cdot c &= (\alpha \cdot c) \cdot ((\alpha \cdot c)\,\phi_{\alpha,\alpha\vee\beta}\,\psi_{\alpha\vee\beta,\alpha})^{-1}\ . \end{aligned}$$

But it holds:

$$\begin{aligned} \alpha \cdot (c\,\phi_{1,\beta}\,\psi_{\beta,1}) &= c\,\phi_{1,\beta}\,\psi_{\beta,1}\,\phi_{1,\alpha} \\ &= c\,\phi_{1,\beta}\,\psi_{\beta,\alpha\wedge\beta}\,\psi_{\alpha\wedge\beta,1}\,\phi_{1,\alpha\wedge\beta}\,\phi_{\alpha\wedge\beta,\alpha} \\ &= c\,\phi_{1,\beta}\,\psi_{\beta,\alpha\wedge\beta}\,\phi_{\alpha\wedge\beta,\alpha} \\ &= c\,\phi_{1,\beta}\,\phi_{\beta,\alpha\vee\beta}\,\psi_{\alpha\vee\beta,\alpha} \\ &= c\,\phi_{1,\alpha}\,\phi_{\alpha,\alpha\vee\beta}\,\psi_{\alpha\vee\beta,\alpha} \\ &= (\alpha \cdot c)\,\phi_{\alpha,\alpha\vee\beta}\,\psi_{\alpha\vee\beta,\alpha}\ . \end{aligned}$$

This completes the proof. □

Now, applying 18.2.9, in case of $a, b \in C$ and $\gamma, \alpha, \beta \in D$ we obtain:

$$\gamma \cdot (\alpha \cdot a \wedge \beta \cdot b) \;=\; \gamma \cdot \alpha \cdot a \wedge \gamma \cdot \beta \cdot b\,. \tag{18.19}$$

PROOF. According to 18.2.5 and 18.2.9 we infer – recall (2.17)

$$\begin{array}{rl} & \gamma\cdot(\alpha\cdot a\wedge\beta\cdot b) \\ = & \gamma\cdot(\alpha\cdot a''\wedge\beta\cdot b'')\cdot(a\wedge b) \\ = & \gamma\cdot(\alpha\wedge\beta)\cdot(\alpha\wedge b'')\cdot(\beta\wedge a'')\cdot(a\wedge b) \\ = & (\gamma\alpha\wedge\gamma\beta)\cdot(\gamma\alpha\wedge\gamma b'')\cdot(\gamma\beta\wedge\gamma a'')\cdot(a\wedge b) \\ \geq & (\gamma\alpha\wedge\gamma\beta)\cdot(\gamma\alpha\wedge b'')\cdot(\gamma\beta\wedge a'')\cdot(a\wedge b) \\ \geq & (\gamma\alpha\cdot a''\wedge\gamma\beta\cdot b'')\cdot(a\wedge b) \\ = & \gamma\cdot\alpha\cdot a\wedge\gamma\cdot\beta\cdot b\,. \end{array}$$

$\square$

So, summarizing we have arrived at:

18. 2. 10 A Theorem of McAlister. *Under the assumptions of* 18.2.4 *the lattice semigroup* $(S,\cdot,\vee)$ *forms even an* (*inverse*) *d-semigroup.*

But the identity element 1 is irrelevant. So we may formulate in general:

18. 2. 11 Proposition. *There are no inverse d-semigroups apart from those, constructed below* 18.2.4.

Chapter 19

Axiomatical outlook

19.1 Some Axiomatic

The question arises, whether in the inverse case further formal reductions are possible. So in this section we give some examples of inverse structures near to inverse d-semigroups, in order to prevent useless attempts on the one hand, but maybe to motivate interesting trials of generalization – on the other hand.

To this end let us start from a *completely distributive lattice ordered semigroup,* for short a *cdl-semigroup,* again, that is *a distributive lattice ordered semigroup* $\mathfrak{S}$ in which *multiplication distributes over meet and join.* Recall, d-semigroups are of this type, and consequently normal complementary semigroups are of this type, too. Since $(S, \wedge, \vee)$ is distributive, the set E of all lattice endomorphisms of $\mathfrak{S}$ forms a *cdl*-semigroup under pointwise building of $\wedge$ and $\vee$.

19. 1. 1 Proposition. *Let $\mathfrak{S}$ be a cdl-semigroup and let $\mathfrak{E}$ be the semigroup of all lattice endomorphisms under composition. Then w. r. t.*

$$a\,.\,\alpha \circ b\,.\,\beta \quad = \quad a \wedge \alpha b\,.\,\alpha\beta\,.$$

$$\textit{and} \qquad a\,.\,\alpha \subseteq b\,.\,\beta \ :\Leftrightarrow\ a \leq b, \alpha \leq \beta$$

$\mathsf{L_E} := \{a\,.\,\alpha \mid a, \alpha \in S \times \mathsf{E}\}$ *forms a distributive ℓ-semigroup $\mathfrak{L}_\mathsf{E}$ whose multiplication $\circ$ distributes over $\wedge$.*

PROOF. First of all L_E forms a semigroup under $\circ$ and a lattice under

$$a\,.\,\alpha \cap b\,.\,\beta := (a \wedge b)\,.\,(\alpha \wedge \beta) \quad \text{and} \quad a\,.\,\alpha \cup b\,.\,\beta := (a \vee b)\,.\,(\alpha \vee \beta)\,,$$

as is easily checked by the reader. Next it results:

$$\begin{aligned}(a\,.\,\alpha \cap b\,.\,\beta) \cup c\,.\,\gamma &= (a \wedge b\,.\,\alpha\ \wedge\ \beta) \cup c\,.\,\gamma \\ &= (a \wedge b) \vee c\,.\,(\alpha \wedge \beta) \vee \gamma) \\ &= (a \vee c) \wedge (b \vee c)\,.\,((\alpha \vee \gamma) \wedge (\beta \vee \gamma)) \\ &= (a \vee c)\,.\,(\alpha \vee \gamma) \wedge (b \vee c)\,.\,(\beta \vee \gamma) \\ &= (a\,.\,\alpha \cup c\,.\,\gamma) \cap (b\,.\,\beta \cup c\,.\,\gamma)\,.\end{aligned}$$

So the lattice under consideration is distributive.

The rest, that is the equations

$$a\,.\,\alpha \circ (b\,.\,\beta \wedge c\,.\,\gamma) = a\,.\,\alpha \circ b\,.\,\beta \wedge a\,.\,\alpha \circ c\,.\,\gamma \tag{19.1}$$

$$(a\,.\,\alpha \wedge b\,.\,\beta) \circ c\,.\,\gamma = a\,.\,\alpha \circ c\,.\,\gamma \wedge b\,.\,\beta \circ c\,.\,\gamma\,. \tag{19.2}$$

follow straightforwardly. □

19. 1. 2 Proposition. *Let $\mathfrak{S}$ be a totally ordered semigroup and let A be the semigroup of all chain automorphisms with id =: ε. Then A forms an ℓ-group under pointwise* max *and* min *– as is clearly well known to the insiders since* Birkhoff [13], *and* $\Sigma := \{a.\alpha \,|\, a \in S, \alpha \in A\}$ *forms a semi-lattice ordered semigroup Σ w. r. t.*

$$a\,.\,\alpha \subseteq b\,.\,\beta \ :\Longleftrightarrow\ a \le b\,.\,\alpha \le \beta$$

and an e-unitary partially ordered inverse ℓ-semigroup w. r. t.

$$a\,.\,\alpha \circ b\,.\,\beta = (a \vee \alpha b)\,.\,\alpha\beta$$

satisfying

$$a\,.\,\alpha \subseteq b\,.\,\beta \implies a\,.\,\alpha \,|_{\,\ell}\, b\,.\,\beta$$

on the one hand and satisfying on the other hand:

$$a\,.\,\alpha \circ (b\,.\,\beta \cap c\,.\,\gamma) = a\,.\,\alpha \circ b\,.\,\beta \cap a\,.\,\alpha \circ c\,.\gamma\,, \tag{DML}$$

$$(a.\alpha \cup b.\beta) \circ c.\gamma = a.\alpha \circ c.\gamma \cup b.\beta \circ c.\gamma\,, \tag{DJR}$$

$$a\,.\,\alpha \circ (b\,.\,\beta \cup c\,.\,\gamma) = a\,.\,\alpha \circ b\,.\,\beta \cup a\,.\,\alpha \circ c\,.\,\gamma\,. \tag{DJL}$$

PROOF. First of all, $(\Sigma, \circ)$ is a semigroup, which follows straightforwardly. Next $(\Sigma, \circ)$ is regular with $\alpha^{-1}a.\alpha^{-1}$ in the role of $(a.\alpha)^{-1}$. Next, exactly the elements of type $a.\varepsilon$ are idempotent because

$$\begin{array}{rcl} (a\,.\,\alpha)^2 = a\,.\,\alpha & \Longrightarrow & (a \vee \alpha a)\,.\,\alpha^2 = a\,.\,\alpha \\ & \Longrightarrow & \alpha^2 = \alpha \Rightarrow \alpha = \varepsilon \\ & \& & \\ a\,.\,\varepsilon \circ a\,.\,\varepsilon & = & a\,.\,\varepsilon\,. \end{array}$$

Hence idempotents commute, that is $(\Sigma, \circ)$ is even inverse, and moreover $(\Sigma, \circ)$ is e-unitary by the implication $a\,.\,\varepsilon \circ b\,.\,\beta = c\,.\,\varepsilon \Longrightarrow \beta = \varepsilon\,.$

We now turn to order properties. First of all we get

$$\begin{array}{rcl} a\,.\,\alpha & \subseteq & b\,.\,\beta \\ & \Longrightarrow & \\ a\,.\,\alpha \circ \alpha^{-1}b\,.\,\alpha^{-1}\beta & = & b\,.\,\beta \end{array}$$

I remains to verify (DML), (DMR), (DJL), again a sake of routine and left to the reader. □

In particular the preceding proposition shows that condition (DMR) is essential in order that a distributively lattice ordered semigroup with right quotients be a d-semigroup.

Constructing new *ℓ-semigroups* from known ones is along the lines of general algebra. So we take this chance to present some further constructions which might be interesting.

This in mind we turn to regarding the case of inverse d-semigroups, together with their elements b considered as lattice endomorphisms $\phi_b =: \beta\,.$

19. 1. 3 Proposition. *Let $\mathfrak{S}$ be an inverse d-semigroup and $\mathsf{L_E}$ the set of all lattice endomorphisms of type $\beta := \phi_b$ and let Σ be the set of all $a\,.\,\beta$ in the sense above endowed with $\circ$ defined by*

$$a\,.\,\alpha \circ b\,.\,\beta := a \wedge \alpha b\,.\,\alpha\beta\,.$$

and

$$a\,.\,\alpha \cap b\,.\,\beta := a \wedge b\,.\,\alpha \wedge \beta\,.$$

We consider $S \times S$ with respect to the operations of proposition 19.1.2 Then the corresponding structure $\sum := (S \times S\,,\,\circ,\,\wedge)$ is an inverse $\cap$-semilattice ordered structure $\sum$ satisfying (DML) *and* (DJL).

Furthermore, $\sum$ *is e-unitary, iff* $\mathfrak{G}$ *is e-unitary.*

PROOF. $\sum$ is regular by

$$a\,.\,\alpha \circ \alpha^{-1}a\,.\,\alpha^{-1} \circ a\,.\,\alpha = a\,.\,\alpha \tag{19.6}$$

$$(a\,.\,\alpha)^2 = a\,.\,\alpha \Leftrightarrow \alpha = \alpha^2 \tag{19.7}$$

$$\alpha = \alpha^2 \;\&\; \beta = \beta^2 \implies (\alpha\beta)^2 = \alpha\beta\,, \tag{19.8}$$

recall: in d-semigroups idempotents are central.

So $\sum$ is e-unitary if $\mathfrak{G}$ is e-unitary.

Finally, (DML) and (DJL) are verified by routine. $\square$

The fundamental idea is, of course, to consider elements as operators with respect to the underlying lattice. This ensures that the resulting structure is always an inverse semigroup if we consider an ℓ-group.

19. 1. 4 Proposition. *Let* $\mathfrak{G}$ *be a cdl-semigroup. Then the set* $\Sigma := \{a\,.\,\alpha \mid a, \alpha \in S\}$ *forms a* $\wedge$*-distributive lattice ordered band under*

$$\begin{aligned} a\,.\,\alpha \cap b\,.\,\beta &= a \wedge b\,.\,\alpha \wedge \beta \\ a\,.\,\alpha \cup b\,.\,\beta &= a \vee b\,.\,\alpha \vee \beta \end{aligned}$$

and

$$a\,.\,\alpha \circ b\,.\,\beta = a \vee (\alpha \wedge b)\,.\,\alpha \wedge \beta\,.$$

with (DML) *and* (DJL) *and* $a\,.\,\alpha \subseteq b\,.\,\beta \Longrightarrow b\,.\,\beta \circ a\,.\,\alpha = b\,.\,\beta\,.$ *Moreover, denoting the pairs* $a\,.\,\alpha$ *by* A*,* $b\,.\,\beta$ *by* B *we get* $ABA = AB\,.$

PROOF. Straightforward. $\square$

19. 1. 5 Proposition. *Let* $\mathfrak{G}$ *be an* ℓ*-group and* $a, b, \alpha, \beta \in G\,.$ *Define a multiplication on* $G \times G$ *by* $A \circ B = a\,.\,\alpha \circ b\,.\,\beta = a \vee (\alpha \wedge b)\,.\,\alpha \wedge \beta$ *and put*

$$xA := (xax^{-1}\,.\,x\alpha x^{-1})\,.$$

Define next $\Sigma := \{A\,.\,x \mid a, \alpha, x \in G\}\,.$ *Then* $\sum$ *forms a regular semigroup and a lattice under*

$$\begin{aligned} (A.x) \odot (B.y) &:= (A \circ xB\,.\,xy). \\ \&\ (A.x) \cap (B.y) &:= (A \cap B\,.\,x \wedge y)\,, \end{aligned}$$

satisfying (DML) *and* (DJL).

PROOF. First of all we get the equations

$$x(U \circ V) = xU \circ xV. \tag{19.9}$$
$$x(U \cap V) = xU \cap xV \tag{19.10}$$
$$x(U \cup V) = xU \cup xV. \tag{19.11}$$

Next $\odot$ is associative because

$$\begin{aligned}(A\,.\,x) \odot ((B\,.\,y) \odot (C\,.\,z)) &= (A\,.\,x) \odot (B \circ yC\,.\,yz)\\ &= A \circ x(B \circ yC)\ .\ xyz\\ &= A \circ (xB \circ (xy)C\ .\ xyz\\ &= (A \circ xB) \circ ((xy)C)\,.\,xyz)\\ &= ((A\,.\,x) \odot (B\,.\,y)) \odot (C\,.\,z)\,.\end{aligned}$$

and $\odot$ is regular since

$$(A\,.\,x) = (A\,.\,x) \odot (x^{-1}A\,.\,x^{-1}) \odot (A\,.\,x)\,.$$

Next idempotent are exactly all pairs (A . 1), since

$$(A\,.\,x)^2 = (A\,.\,x) \implies x^2 = x = 1.$$

Finally we get (DML) and (DJL) which – for example – is shown here for (DML) by

$$\begin{aligned}(A.x) \odot ((B\,.\,y) \cap (C\,.\,z)) &= (A\,.\,x) \odot ((B \cap C\,.\,y \wedge z))\\ &\overset{(19.9)}{=} A \circ (xB \cap xC)\ .\ x(y \wedge z)\\ &= A \circ xB \cap A \circ xC\ .\ x(y \wedge z)\\ &= A \circ xB \cap A \circ xC\ .\ xy \wedge xz\\ &= (A\,.\,x)(B\,.\,y) \cap (A\,.\,x)(C\,.\,z)\end{aligned}$$

and which follows for (DJL) by analogy. $\square$

Bibliography

[1] Abel, N.H.: *Untersuchung der Funktionen zweier unabhängig veränderlicher Größen x und y, wie $f(x,y)$, welche die Eigenschaft haben, daß $f(z,(f(x,y))$ eine symmetrische Funktion von z,y und x ist.* J. f. d. reine u. angew. Mathem. **1** (1826), 11 - 15.

[2] Anderson, D. D.: *Multiplication ideals, Multiplication rings, and the ring $R(X)$.* Canad. J. Math. **XXVIII** (1976), 760 - 768.

[3] Ánh, P.N., Márki, L.and P. Vámos.: *Divisibility Theory in commutative Rings: Bezout Monoids.* Transactions AMS **364**, 3967 - 3992, 2012.

[4] Arnold, I.: *Ideale in kommutativen Halbgruppen.* Math. Sb. **36** (1929), 401 - 407.

[5] Banaschewski, B.: *On lattice-ordered groups.*Fund. Math. **55** (1964), 113 - 122.

[6] Bernau, S. J.: *Orthocompletion of lattice groups.* London Math. Soc. (3) **16** (1966), 107 - 130.

[7] Bigard, A.: *Contribution á la théorie des groupes réticulés.* Thése Sci. Math., Paris 1969.

[8] Bigard, A.: *Sur les z-sous-groupes d'un groupe réticulé.* C. R. Acad. Sc. Paris **266** (1968), 261 - 262.

[9] Bigard, A.: *Groupes archimédiens et hyperarchimédiens.* Sem. Dubreil - Pisot **2**, 1967 - 1968.

[10] Bigard, A., Conrad, P. F., and S. Wolfenstein: *Compactly generated lattice-ordered groups.* Math. Z. **107** (1968), 201 - 211.

[11] Bigard, A., Keimel, K., and S. Wolfenstein. *Groupes et Anneaux Réticulés.* Lecture Notes in Mathematics: Springer-Verlag Berlin-Heidelberg-New York 1977.

[12] Birkhoff, G.: *Lattice-ordered groups.* Ann. Math. **43** (1942), 298 - 331.

[13] Birkhoff, G.: *Lattice theory.* Amer. Math. Soc. Coll. Publ. 1967.

[14] Bosbach, B.:*Komplementäre Halbgruppen. Axiomatik und Arithmetik.* Fund. Math. **64** (1969), 257 - 287.

[15] Bosbach, B.:*Komplementäre Halbgruppen. Kongruenzen und Quotienten.* Fund. Math. **69** (1970), 1 - 14.

[16] Bosbach, B.:*Komplementäre Halbgruppen. Eine Darstellungstheorie.* Math. Ann. **179** (1968), 1 - 14.

[17] Bosbach, B.: *Zur Theorie der Teilbarkeitshalbgruppen.* Semig. For. **3** (1971), 1 - 30.

[18] Bosbach, B.:*Schwache Teilbarkeitshalbgruppen.* Semig. For. **12** (1976), 119 - 135.

[19] Bosbach, B.: *Zur Struktur der inversen Teilbarkeitshalbgruppen.* Semig. For. **12** (1976), 137 - 143.

[20] Bosbach, B.:*Zur Theorie der stetigen Teilbarkeitshalbgruppen.* Semig. For. **20** (1980), 299 - 317.

[21] Bosbach, B.:*Archimedische Teilbarkeitshalbgruppen und Quaderalgebren.* Semig. For. **20** (1980), 319 - 334.

[22] Bosbach, B.: *Zur Theorie der vollständigen Teilbarkeitshalbgruppen.* Semig. For. **25** (1982), 111 - 124.

[23] Bosbach, B.: *Concerning Bricks.* Acta Math. Ac. Sc. Hung. **38** (1981), 89 - 104.

[24] Bosbach, B.:*Teilbarkeitshalbgruppen mit vollständiger Erweiterung.* J. Alg. **83** (1983), 237 - 255.

[25] Bosbach, B.: *Lattice ordered binary systems.* Acta Sci. Math. **52** (1988), 257 - 289.

[26] Bosbach, B.:*Separative Teilbarkeitshalbgruppen.* Contributions to general algebra **6** (1988), 49 - 65.

[27] Bosbach, B.:*Orthogonalität und Linearität.* Preprint, Kassel 1988.

[28] Bosbach, B.:*HyperarchimedischeTeilbarkeitshalbgruppen.* Czech.Math. J. **39** (1989), 528 - 543.

[29] Bosbach, B.:*Representable divisibility semigroups.* Proc. Edinb. M. Soc. **34** (1991), 45 - 64.

[30] Bosbach, B.:*Ordnungsmodule. 192 S.* Kassel 2008

[31] BOSBACH, B.: *Convex chains in lattice monoids and lattice loops.* Acta Sci. Math. **67**, No 1-2 (2001), 57 - 75.

[32] BOSBACH, B.: *Ideal Divisibility Monoids.* Result. Math. **41** (2002), 40 - 67.

[33] BOSBACH, B.: *Inverse lattice ordered Semigroups.* Preprint, Kassel 1999.

[34] BOSBACH, B.: *Divisibility Groupoids – Again.* Result. Math. **57** (2010), 257 - 285.

[35] BOSBACH, B.: *Ideal Semigroups.* KOBRA, Kassel, 2012. (First version 1994)

[36] BOSBACH, B.: *Residuationsstrukturen.* KOBRA, Kassel, 2012. (Erste Version 1996)

[37] BOURBAKI, N.: *Topologie Générale.* Hermann, Paris, 1958.

[38] BURMISTROVIČ, I. E.: *Commutative bands of cancellative semigroups.* Sib. Mat. Z. **6** (1965), 284 - 299.

[39] CARRUTH, J.H., J.A. HILDEBRANDT and R.J. KOCH: *The theory of topological semigroups.* Monographs and textbooks in pure and applied mathematics, Marcel Dekker Inc., 1983.

[40] CARRUTH, J.H., J.A. HILDEBRANDT and R.J. KOCH: *The theory of topological semigroups.* Vol 2, Monographs and textbooks in pure and applied mathematics, Marcel Dekker Inc., 1986.

[41] CLIFFORD, A. H.: Arithmetic and idealtheory in commutative semigroups. Ann. Math. **39** (1938), 594 - 610.

[42] CLIFFORD, A. H.: *Naturally totally ordered commutative semigroups.* Amer. J. Math. **76** (1954), 631 - 646.

[43] CLIFFORD, A. H. and G. B. PRESTON: *The algebraic theory of semigroups.* Amer. Math. Soc. Math. Surveys 1961.

[44] CONRAD, P. F.: *The structure of a lattice-ordered group with a finite number of disjoint elements.* Mich. Math. J. **7** (1960), 171 - 180.

[45] CONRAD, P. F.: *Some structure theorems for lattice - ordered groups.* Trans. Amer. Math. Soc. **99** (1961), 212 - 240.

[46] CONRAD, P. F.: *The lattice of all convex ℓ-subgroups of a lattice-ordered group.* Czech. Math. J. **15** (1965), 101 - 123.

[47] CONRAD, P. F.: *Introduction á la théorie des groupes réticulés.* Paris, Sécrétariat mathématique 1967.

[48] Conrad, P. F.: *Lex-subgroups of lattice-ordered groups.* Czech. Math. J. **18** (1968), 86 - 103.

[49] Conrad, P. F.: *Lattice-ordered groups.* Tulane University 1970.

[50] Conrad, P. F.:*Epi-archimedean groups.* Czech. Math. J. **24** (1974), 1 - 27.

[51] Doerge, K.:*Elementare Megenlehre.* Vorlesungsskriptum, 3. Auflage, Köln 1959.

[52] Euclides: *Elemente.* ≈ -400

[53] Faucett, W. M.:*Compact semigroups irreducibly connected between two idempotents.* Proc. Amer. Math. Soc. **6**, 1955, 741 - 747.

[54] Faucett, W. M.: *Topological semigroups and continua with cut points.* Proc. Amer. Math. Soc. **6**, 1955, 748 - 756.

[55] Fuchs, L.:*Teilweise geordnete algebraische Strukturen.* Studia Mathematica, Vandenhoek & Ruprecht, Göttingen 1966.

[56] Fuchs, L.:*A remark on lattice ordered semigroups.* Semig. For.**7** (1974), 372 - 374.

[57] Fuchs, L.: *Note on fully ordered semigroups.* Acta Math. Acad. Sci. Hung. **12** (1961), 255 - 259.

[58] Glass, A. M.:*Ordered permutation groups.* Cambridge University Press, London Mathematical Society lecture note series **55**, 1981.

[59] Harzheim, E.: *Beiträge zur Theorie der Ordnungstypen insbesondere der η_α-Typen.* Math. Ann **154** (1964), 116 - 134.

[60] Hausdorff, F.:*Grundzüge der Theorie der geordneten Mengen.* Math. Ann. **65**, 1908.

[61] Hausdorff, F.:*Grundzüge der Mengenlehre.* Leipzig, 1914.

[62] Hölder, O.:*Die Axiome der Quantität und die Lehre vom Maß.* Ber. d. Sächs. Ges. d. Wiss. Leipzig, Math. Phys. Cl. (1901), 1 - 64.

[63] Hofmann, K. H, & P. S. Mostert*Elements of compact semigroups.* Charles Merrill, Columbus, 1966.

[64] Hofmann, K. H. & J. D. Lawson:*Linearily Ordered Semigroups: Historical Origins and A. H. Clifford's Influence.* Semigroup Theory and its Applications, ed. by Karl. H. Hofmann & Michael W. Mislove. London Mathematical Society Lcture Note Series 231. Cambridge University Press, 1996.

[65] Holland, W. C.: *The lattice-ordered group of automorphisms of an ordered set.* Mich. Math. J. **10** (1963), 399 - 408.

[66] Iwasawa, K.: *On the structure of conditionally complete lattice-groups.* Jap. J. Math. **18** (1943), 777 - 789.

[67] Jaffard, P.: *Théorie des filets dans les groupes réticulés.* C. R. Acad. Sc. Paris **230** (1950), 1024 - 1025.

[68] Jaffard, P.: *Applications de la théorie des filets.* C. R. Acad. Sc. Paris **230** (1950), 1125 - 1126.

[69] Jaffard, P.: *Nouvelle applications de la théorie des filets.* C. R. Acad. Sc. Paris **230** (1950), 1631 - 1632.

[70] Jaffard, P.: *Contribution á l'étude des groupes ordonnés.* J. Math. Pure Appl. **32** (1953), 203 - 280.

[71] Jaffard, P.: *Les systémes d'idéaux.* Dunod, Paris 1960.

[72] Jakubik, J.: *Konvexe Ketten in ℓ-Gruppen.* Časopis pěst. Mat. **84** (1959), 53 - 63.

[73] Jakubik, J.: *Lattice-ordered groups with a basis.* Math. Nachr. **53** (1972), 217 - 236.

[74] Jakubik, J.: *Lattice-ordered groups of finite breadth.* Coll. Math. **27** (1973), 13 - 20.

[75] Jakubik, J.: *Strongly projectable lattice-ordered groups.* Czech. M. Journ. **26** (1976), 642 - 652.

[76] Klein-Barmen, F.: *Über gewisse Halbvrbände und Semigruppen II.* Math. Z. **48** (1942-43), 715 - 734.

[77] Lloyd, J. T.: *Representations of lattice-ordered groups having a basis.* Pac. J. Math. **15** (1965), 1313 - 1317.

[78] McAlister, D. B.: *Amenably ordered inverse semigroups.* J. Alg. **65** (1980), 118 - 146.

[79] Merlier, Th.: *Sur les demi-groups réticulés et les o-demigroupes.* Semig. For. **2** (1971), 64 - 70.

[80] Mostert, P. & A. L. Shields: *On a class of semigroups on* $\mathbf{E}^n$. Proc. Amer. Math. Soc. **7** (1956), 729 - 734.

[81] Mostert, P. & A. L. Shields: *On the structure of Semigroups on a compact manifold with boundary.* Ann. Math. **65** (1957), 117 - 143.

[82] Mostert, P. & A. L. Shields: *One-parameter semigroups in a semigroup.* Trans. Amer. Math. Soc. **96** (1960), 510 - 517.

[83] Paalman-de-Miranda, A. B.: *Topological Semigroups.* Mathematical Centre Tracts 11, 2^{nd} Edition. Mathematisch Centrum Amsterdam 1970.

[84] Repnitzkii, V. B.: *On subdirectly irreducible lattice-ordered semigroups.* Semig. For. **29** (1984), 277 - 318.

[85] Repnitzkii, V. B.: *Varieties of lattice-ordered semigroups.* Diss. Cand. Acad. of Sc. of Moldavia, Kichinew, 1984.

[86] Ribenboim, P.: *Une théorème de réalisation des groupes réticulés.* Pac. J. Math. **10** (1960), 305 - 308.

[87] Riesz, F.: *Sur la theorie générale des operations linéaires.* Ann. Math. **41** (1940), 174 - 206.

[88] Šik, F.: *Über subdirekte Summen geordneter Gruppen.* Czech. Math. J. **10** (1960), 400 - 424.

[89] Šik, F.: *Über die Beziehungen zwischen eigenen Spitzen und minimalen Komponenten einer ℓ-Gruppe.* Acta Math. Acad. Sci. Hungar. **13** (1962), 171 - 178.

[90] Šik, F.: *Estrutura y realisaziones de grupos reticulados. I. Topologia inducida por la realizacion de un grupo reticulado.* Mem. Fac. Ci. Univ. La Habana, Ser. Mat. **1** N° 3 (1964), 1 - 11.

[91] Šik, F.: *Struktur und Realisierung von Verbandsgruppen, III. Einfache Untergruppen und einfache Ideale.* Mem. Fac. Ci. Univ. La Habana, Ser. Mat. **1** N° 4 (1966), 1 - 20.

[92] Šik, F.: *Struktur und Realisierung von Verbandsgruppen V, Schwache Einheiten in Verbandsgruppen.* Math. Nachr. **33** (1967), 221 - 229.

[93] Šik, F.: *Struktur und Realisierung von Verbandsgruppen, IV. Spezielle Typen von Realisierungen.* Mem. Fac. Ci. Univ. La Habana, Ser. Mat. **1** N° **7** (1968), 19 - 44.

[94] Smith, F. A.: *A subdirect decomposition of additively idempotent semirings.* J. Nat. Sc. & Math. **7** (1967), 253 - 257.

[95] Tarski, A.: Fund. Math. **16** (1929), 195 - 197.

[96] van der Waerden, B. L.: *Zur Produktzerlegung der Ideale in ganzabgeschlossenen Ringen.* Math. Ann. **101** (1929), 293 - 308.

Index

Algebra
  Quader -, 40
algebraic
  infimum, 226
annihilator, 146
archimedean, 15, 108
  hyper -, 16, 155
  strictly, 15
  super -, 155
associative, 52
atom
  co -, 81
  hyper -, 13, 81, 82
atomic, 206
automorphism, 48

base, 206
bisection, 144
bordered, 133
  left, 133
  un -, 133
bound
  upper, 132
bounded, 222
  upper, 14
brick, 40
  complete, 40, 41

Calabi, 146
cancellable, 34, 47
  conditionally, 84
  left, 34
  right, 34
cancellative
  0 -, 38
  with 0, 38
carrier, 215
central, 263
chain, 6, 18, 86, 105, 132
  ascending, 168
  continuous, 134, 146
class
  closed
    cancellative, 267
Clifford, Alfred. H., 251
closed, 22, 23
  inf -, 22, 23
  integrally
    completely, 44
  multiple -, 92
  operatively, 213
  sup -, 22, 23
  under multiplication, 12
complement
  left, 39
  right, 39
complete
  conditionally, 14
completion, 11
component, 52
composition, 5, 7, 47

condition
  factor, 6
  left factor, 6
  left/right factor, 6
cone, 26
  positive, 9, 26, 131
congruence, 12, 71
  archimedean, 78
  cancellative, 13
  filet -, 190
  filet-respecting, 191
  finest, 77
    cancellative, 77
    idempotent, 77
  ideal oriented, 75
  idempotent
    finest, 13
  left, 12, 71, 74
  linear, 86
  separative
    finest, 250, 261
converge, 134
convex, 62
coprime, 35, 117
cube
  semigroup, 17
cut, 17, 96, 133
  left, 133
  right, 133

decomposition
  cone, 35
  direct
    inner, 251
  induced, 251
  inner, 194
  orthogonal, 54
  prime, 33
  subdirect, 12, 263
degree
  archimedean, 61
denominator, 49
dense
  in a set, 132
  in itself, 132
disjoint, 35
distributive
  $\bigvee$ -, 15
  $\bigwedge$ -, 14
  completely, 59, 233
  lattice, 24
    absolutely, 15
distributivity
  infinite, 59
divisible, 100
divisor, 168
  left, 50, 263
  normal
    convex, 75, 104
  right, 263
d-monoid
  ortho-finite, 208
d-semigroup
domain
  Bézout, 5
  GCD -, 5
  archimedean
    strictly, 139
  continuous, 108
  inf-continuous, 108
  interval, 135
  sup-continuous, 108

element

  cancellable, 10
  central, 77, 266
  idempotent, 10
  identity, 9, 16, 24
  invertible, 107
  positive, 9
  prime, 32
  semiprime, 16
  zero, 40, 68
end
  of a sequence, 134
endomorphism, 47
  lattice, 87
equivalent
  archimedean, 13, 78
extension
  $\wedge$-normal, 178
  $\bigvee$-complete, 17, 67, 171
  $\bigwedge$-complete, 67, 171
  cancellative stable, 70
  complete, 16, 44, 171
  cube
    lattice, 229
  cut, 174
  identity, 47, 51
  infimum, 221
  lattice point, 18
  lexicographic, 199
  monoid, 10
  quotient, 10, 36, 47, 52

factor, 8
  direct, 18
family, 61, 208
  1-disjoint, 208
  sub -
    finite, 61

Faucett, 146
filet, 190
filter, 7, 58
  p-filter, 58
  lattice, 11, 58, 59
  order, 13
  primary, 61
    real, 217
  prime, 58
  regular, 13, 62
  ultra -, 65
finite
  ortho -, 211, 240
fixpoint, 101
formula
  binomial, 28
  decomposition, 26
  product, 253
function
  continuous, 134
  measure, 30
  minimum
    pointwise, 5
  minimum -
    pointwise, 7

gap, 14, 133, 145
  order, 40
generated
  finitely, 6
group, 5, 8, 19, 21, 249
  ℓ-group, 5
  po-
    semi, 9
  dual, 5
  lattice, 5, 8, 21
    with 0, 22

linearly ordered, 199
module, 5
sub -
convex, 62

height
of an element, 209
Hofmann, Karl H., 147
homomorphism, 249
hull, 60
c-ideal -, 187
convex, 97, 99, 101
identity, 10
polar, 187
quotient, 11, 52, 54, 102

ideal, 57
$\bigcap$-prime, 66
c-ideal, 11, 62, 88
$\bigcap$-prime, 66
invariant, 208
irreducible, 65
minimal prime, 192
prime, 65
d-ideal, 11, 59
p-ideal, 11, 58
u-ideal, 11, 17, 69
v-ideal, 17, 68
z-ideal, 190
finitely generated, 22
archimedean, 61
co-regular, 62
Dedekind, 11
divisor, 69
finitely generated, 5
invariant, 243
irreducible, 12, 57, 86
lattice, 11, 57
left quotient, 70
minimal
prime, 65
of finite character, 61
order, 13
prime, 57, 58
proper, 193
principal, 5
principal v -, 68
regular, 67
right quotient, 70
semiring, 11
ideals
v -, 11
idempotent, 9, 12, 34, 263
identity, 47
infimum, 55, 132, 177
complex, 59
intersection, 66
interval, 132
closed, 132, 135, 146
left open, 133
min, 146
nil, 146
open, 132, 134
real unit, 134
right closed, 133
unit, 146, 147
invariant, 102
inverse, 30, 35
local, 31
invertible, 36, 47
irreducible
$\bigwedge$-irreducible, 62
subdirectly, 13

isomorphic
  anti, 53
isomorphism
  ideal/filter, 13
  order, 13
  order preserving, 143
isotone, 5

jump, 133, 226

kernel, 189
  cancellative, 10, 19, 35, 269
  idempotent, 10, 19, 34, 269
  induced, 251
  of a congruence, 189
  of an ideal, 62
  separative, 19

lattice, 5
  $\bigvee$-distributive, 105
  $\vee$-distributive, 105
  algebraic, 62
  boolean, 22
  complete, 41
    conditionally, 105
  distributive, 21
  distributive, 6–8
  infinitely distributive, 105
  semi -, 6, 8, 19, 21, 249
law
  cancellation, 6
Lawson, Jimmy, D., 147
length
  of a chain, 209
limes, 97
limited
  lower, 132
  upper, 14, 105, 132, 135
linearity, 11, 62, 139
lying
  between, 132

mapping
  inverse, 50
maximum, 132
meet
  pointwise, 47
minimum, 132
  function
    pointwise, 14
modularity, 209
monoid, 21
  c-monoid, 183
  d-monoid
    lex, 21
  convex
    sub -, 201
  direct factor, 194
  divisibility, 5
    basic, 206
    direct factor, 202
    directly indecomposable, 196
    laterally complete, 214
    lex simple, 200
    lex-extension of a, 199
    lex-kernel of a, 200
    maximal chain, 205
    ortho-finite, 211
    projectable, 212
    semi-projectable, 212
  lattice, 41
  lex -, 200
  prime c -, 199
  zero -, 176

normal, 9, 21
  hyper -, 22
    right, 22
  hypern, 242
  right, 9, 21
number
  irrational, 134
  ordinal, 97

operation
  complex, 59, 61
  function, 17
  stable, 68
order
  - complete, 16, 146
  - continuous, 132, 147
  - dense, 16, 146
  isomorphism, 134
  maximum, 16
  minimum, 16
  partial, 54
  total, 16
  type, 96
  well, 97
order-similar, 132
ordered
  fully, 139
  linearly, 21, 132, 139
  partially, 132
  totally, 132, 139
ordinal
  initial, 97
orthogonal, 35
orthogonality, 11, 62

pair
  critical, 81
permutation
  chain, 5
point
  cluster, 134
polar, 18, 184
  C-polar of A, 184
  bi -, 184, 211
  invariant, 208
  maximal, 204
  minimal, 204
  principal, 189
positive, 10, 25
  right, 265
prime, 33, 166
  co -, 117, 156
  completely, 33, 166
  minimal, 204
  semi -, 32, 166
product, 194
  complex, 59
  direct, 194, 268
  ideal, 68
  lexicographic, 199
  prime
    irredundant, 166
  relation, 14
  subdirect, 80, 250, 268
projectable
  semi -, 240
proof
  elementary, 264

quotient
  ideal
    left, 68
    right, 68

radical, 62
regular, 62
relation
  reflexive, 72
  symmetric, 72
  transitive, 72
representable, 233
representation, 208
  binary, 144
  irreducible, 208
residuation, 10
  arithmetic, 52
ring, 22
  arithmetical, 6, 19, 22, 183
  Bézout, 7, 19, 22, 247
  residue class, 183
  semi -, 11
    inverse, 269
root
  square, 144

semigroup, 6
  I -, 146
  d -, 6
  dld -, 24
  r -, 14
  algebraic lattice, 61
  cdl -, 148
  Clifford, 251
  complementary, 39
  complete, 15
  divisibility, 6, 8, 21
    $\bigvee$-complete, 106
    $\bigwedge$-complete, 106
    archimedean, 108
    complete, 106
    continuous, 106
    cube -, 221
    discrete archimedean, 164
    divisible, 101
    factorial, 16, 166
    hyper-archimedean, 80, 155
    inf-continuous, 106
    linear, 131
    locally finite, 103, 159
    real, 84, 155
    representable, 61, 80, 212
    separative, 249
    subdirectly irreducible, 71, 80
    sup-continuous, 106
    super-archimedean, 158
    with 0, 60
  factorial d -, 33
  ideal, 7, 19, 41, 61
    principal, 183
  ideal/filter, 7, 14
  interval, 16, 146
  inverse, 19, 249, 263
    right d -, 263
  one parameter, 131
  ordered
    totally, 8
  principal ideal, 22
  real d -, 143
  representable d -, 86
  semilattice, 269
  separative, 19
  strictly archimedean d -, 143
  sub
    convex, 11
  topological, 8, 16
  totally ordered d -, 21
separative, 255

sequence
  of elements, 134
series
  $0, 1$, 104
set, 13
  directed, 251
  ordered
    linearly, 13
  orthogonal, 206
  power, 97
singleton, 60
space
  Euclidean, 105
splitted, 265
sum
  ideal, 68
support, 101
supremum
  complex, 59

Theorem
  Intermediate Value, 135
  Intersection, 60
  Mapping, 135
  Maximum, 135
  of Bolzano Weierstraß, 135
  of Cantor, 135
  of Hölder and Clifford, 143
  of Heine Borel, 135
  Projection -, 185
theory
  ℓ-group, 5
  congruence, 11
  divisibility, 5
  ideal, 5, 11
    ring, 7
  lattice
    algebraic, 67

union
  disjoint, 250
unit
  private, 9, 24
  right, 88

value, 185
  absolute, 10, 30, 31
  positive, 10
valued
  finitely, 240

In advance

In the following we are concerned with ideal monoids, that is abstractions of ideal structures like those of semigroups, rings, or lattices. The first to initiate and to stimulate such an element free ideal theory was Wolfgang Krull in 1924. It is a great pleasure for the author to present this lecture note in honour of that great pioneer.

It will be offered both, a historical development of abstract ideal theory on the one hand, and an investigation of ideal monoids satisfying

TO CONTAIN IS TO DIVIDE

on the other hand.

The historical part reviews abstract ideal theory until about 1994, and is partially antiquated in general, but nevertheless it should still be interesting for all fans of abstract ideal theory.

That is the reason why we decided to present the 1994-draft, in spite of the fantastic results on Fermat's last theorem achieved by Andrew Wiles, the more as our historical introduction and its citations doesn't take anything from whomsoever.

Ideal Semigroups

to the memory of

Wolfgang Krull
1899 -1971

the great pioneer
of ideal theory

presented by

Bruno Bosbach

1994 - 1998 - 2004 - 2014

Contents

1 History and Development **5**

1.1 Historical Remarks 5

1.2 Towards an Abstract Ideal Theory 12

1.3 The Contents 23

1.4 Some final Remarks 27

2 Factorial Rings **29**

2.1 Preface 29

2.2 Prime Element Factorizations 32

2.3 A direct Ring Decomposition 39

2.4 Ideal theoretical Aspects 44

2.5 Towards abstract considerations 48

3 Lattices **53**

3.1 Some Remarks on Posets 53

3.2 Lattices 57

3.3 Modular and distributive Lattices 59

3.4 Representation 66

3.5 Complete Lattices 69

4 Ideal Systems **71**

4.1 Ideal Operators 71

4.2 A finest Ideal System in general 78

4.3 v- and t-Ideals 80

5 Algebraic m-Lattices 85
5.1 The Notion 85
5.2 Examples 88
5.3 Arithmetics 89
5.4 Prime Elements and primary Elements 96
5.5 Residues 99
5.6 Localization 101

6 Krull's Classics 105
6.1 The Localization Theorem 105
6.2 The Kernel of an Element 106
6.3 The Principal Ideal Theorem 108

7 Prüfer Structures 115
7.1 Left Prüfer Structures 115
7.2 Normal Prüfer monoids 122
7.3 Prüfer Implications 128

8 Mori Structures 133
8.1 The Prime Criterion 133
8.2 Mori Implications 138
8.3 M-Equivalents 142
8.4 The left Divisor Case 144
8.5 The Divisor Case 147
8.6 Further Criteria 148
8.7 Left Prüfer Cases 151
8.8 The commutative Case 154

9 Classical Ideal Structures 157
9.1 Preface 157
9.2 Modular Divisor Ideal Monoids 158
9.3 Classical Divisor Ideal Monoids 161

10 Ringlike Ideal Structures **165**
10.1 Starting ab ovo 166
10.2 Nearer to Dilworth 169
10.3 The Kernel 173
10.4 Idempotency 174
10.5 Decomposition Theorems 177
10.6 M-characterizations 180

11 Archimedean Prüfer Ideal Monoids **185**
11.1 Preliminaries 185
11.2 Arithmetics 186
11.3 Localizations of $AP-$ideal-monoids 187
11.4 P-cancellative AP-ideal-monoids 192
11.5 Ringlike AP-ideal monoids 194

12 Factorial Structures **199**
12.1 UF-Structures 199
12.2 Special cases 202
12.3 Mori Criterions in the integral Case 204
12.4 Factorial Duo structures 208

13 v- and t-Ideals **211**
13.1 Preliminaries 211
13.2 The general Case 212
13.3 Cancellative Monoids 214
13.4 Cancellative Mori v-Monoids 216
13.5 Krull Monoids 222
13.6 Sorrowing looking back 233

Chapter 1

History and Development

1.1 Historical Remarks

According to a speech, [188], of Kurt Hensel (1861-1941), for a long period it has been a common opinion, that *ideal theory* originated, when and because Ernst Eduard Kummer (1810-1893) was faced with a gap in his "proof of Fermat's last theorem", caused by the incorrect assumption of *unique factorization* in *number domains* of type $\mathbf{Z}[\zeta]$, where ζ is a *p-th primitive identity-root*.

Nowadays, however, this view seems to be no longer tenable, as Edwards explains in [112], [113]. All we know seems to be that Kummer treated certain problems on higher residues, assuming unique factorization in $\mathbf{Z}[\zeta]$, and that he contributed to Fermat's problem, which led to an award of the Parisian Academy, although Kummer himself informed Liouville and Cauchy that his expositions were still suffering from some gaps which he was endeavoured to fill.

Ernst Eduard Kummer 1815 -1864

Whether this endeavour or his endeavour on higher residues led to the creation of *ideal complex numbers* seems to be open until now, whereas on the other hand it is certified that Kummer successfully made use of "his ideal numbers" in treating problems of algebraic number theory.

Nevertheless, if merely a demonstration is wanted how decomposition theory may be applied in treating number theoretical problems, Fermat's problem turns out to be most suitable.

The central idea here is to factorize sums in order to apply the rules of divisibility. This will be demonstrated, briefly, along the lines of the monograph of Borewicz/Šafarevič, [55].

As well known, Pierre Fermat, (jurist, 1601-1665), believed to have a proof of the theorem – meanwhile proven by Andrew Whiles – that there are no nontrivial integral solutions of

$$x^n + y^n = z^n \quad (n \in \mathbf{N}) \tag{1.1}$$

except for $n \in \{1, 2\}$. However, given $n = m\ell$, (1.1) leads to

$$(x^m)^\ell + (y^m)^\ell = (z^m)^\ell, \tag{1.2}$$

whence Fermat's theorem is proven once it is proven for all odd prime numbers and the number 4. So, since already Fermat himself gave an elementary proof for $n = 4$ the problem diminishes to treating all odd prime numbers.

Pierre de Fermat
1607 - 1665

Furthermore it is easily seen that a solution with pairwise *relatively prime* numbers x, y, z must exist if a solution, whatever, exists in $\mathbf{Z} \setminus \{0\}$, since each t, dividing two of the three numbers x, y, z, is a divisor of the third one, too, because $t^p \mid a^p \Longrightarrow t \mid a$.

Therefore two principal cases remain to be studied, namely:

(1) $x^p + y^p = z^p$ with: p divides exactly one $u \in \{x, y, z\}$
and
(2) $x^p + y^p = z^p$ with: p divides not even one $u \in \{x, y, z\}$.

We discuss only the first case, since we are merely interested in a historical feedback, and refer the reader to Borewicz/ Šafarevič [55], where classical ideal theory is presented along the lines of Hensel's *p-adic valuations.*

First of all: if ζ is a non-real *p-th primitive identity-root*, then the set $\{\zeta^0, \zeta^1, \ldots, \zeta^{p-1}\}$ exhausts the set of all roots of $x^p - 1$, and this means

$$z^p = \prod{}_0^{p-1}(x + \zeta^k y) \tag{1.3}$$

since the coefficients of the polynomial on the right side have, respectively, the same absolute values as the coefficients of $x^p - 1$.

Furthermore: under the assumption above, one can show that any pair of factors of $x + \zeta^k y$ is relatively prime in $\mathbf{Z}[\zeta]$. Assuming now *unique prime factorization,* this leads to

$$x + \zeta^k y \;=\; \varepsilon_k \alpha_k^p \tag{1.4}$$

where ε_k is a unit and α_k belongs to $\mathbf{Z}[\zeta]$. In particular this implies

$$x + \zeta y \;=\; \varepsilon_1 \alpha^p \;\; (\text{with } \; \alpha = \alpha_1).$$

Hence by symmetry it follows:

$$x - \zeta z \;=\; \varepsilon_2 \, \beta^p \,.$$

However – according to [55] – by relatively simple methods this leads to a contradiction.

That unique prime factorization in $\mathbf{Z}[\zeta]$ is by no means satisfied in any case, was discovered by KUMMER himself *via* studying the case $p = 23$, consult [254].

What now? KUMMER found out, that in many cases much less than unique prime factorization suffices to verify number theoretical interrelations. In particular he observed that already *multiplicative extensions* may turn out as powerful tools. This brought him to considering *congruence classes* as *ideal complex numbers*, and he achieved this way that in the corresponding multiplicative extension all elements of the original structure became uniquely prime decomposable. But, his method failed in providing unique prime factorizations also for all elements, added by the extension process.

Nevertheless, by KUMMER's construction number theoretical problems became solvable, which had successfully withdrawn any solution, so far. One most essential idea in this context was to select certain elements of $\mathbf{Q}[\zeta]$, ζ a *p-th primitive identity-root*, as *integral numbers.*

This was the starting point of RICHARD DEDEKIND (1831-1916), who cleared divisibility in arbitrary *number domains* by taking up KUMMER's crucial idea and completing ideal theory in such a way – compare the X. supplement of the 2. and the XI. supplement of the 3. and 4. edition of DIRICHLET's lectures on number theory, [104]

Richard Dedekind
1831 - 1916

– that nowadays ideal theory is DEDEKINDian IDEAL THEORY.

DEDEKIND asked, how in general by including also ideal objects a divisibility theory for number domains of type $\mathbf{Q}[\vartheta]$, ϑ an *arbitrary algebraic number*, could be established.

In accordance to the theory of integral complex numbers due to CARL FRIEDRICH GAUSS (1777-1855) – DEDEKIND had been his last student – he investigated, which elements of $\mathbf{Q}[\vartheta]$ could act as *integral elements* in such a way that integral rationals *remained* integral and no other rationals *became* integral.

That such a requirement makes sense is an easy consequence of the fact that divisibility in $\mathbf{Z}$ can, of course, not be studied by considering extensions violating *divisibility relations* in the initial domain.

Furthermore, distinguishing integral elements has to take into account, that together with α also all *conjugates* of α become integral, since otherwise there would exist an integral element α and a *non-integral* element β satisfying the same rational relations with respect to $\mathbf{Z}$.

So, at least the coefficients of a *normed irreducible* polynomial f_α with $f_\alpha(\alpha) = 0$ are to be taken as rational numbers, since these coefficients are values of *elementary symmetrical* functions of the conjugated elements α_i $(1 \le i \le n)$ of α and since $a_i = \dfrac{u_i}{v_i}$ leads to $v_i \,|_z\, u_i$. Therefore, integral have to be all algebraic numbers satisfying some relation

$$\alpha^n = a_{n-1}\alpha^{n-1} + \ldots\ldots + a_1\alpha^1 + a_0 \tag{1.5}$$

since $g(\alpha) = 0 \Longrightarrow f_\alpha \,|\, g$ (in $\mathbf{Z}[x]$), and moreover one should be in the position to calculate integral algebraic numbers without leaving the set of algebraic integers.

DEDEKIND showed – by *determinants* and *modules* – that together with α and β also $\alpha+\beta$ and $\alpha \cdot \beta$ satisfy some equation of type (1.5), i. e. that the integers in the sense of (1.5) form a *ring.* Moreover: he showed that α is already integral in the sense of (1.5) if α is root of some *normed polynomial* with *integral algebraic coefficients.* Summarizing he discovered:

The algebraic integers form an integrally closed ring $\mathfrak{G}$.

Furthermore it is easily seen :

If α *is an algebraic number then some quotient* $\dfrac{\alpha}{m}$ *is even an algebraic integer.*

Recall : By definition every algebraic number is a root of some polynomial

$$f(x) \;=\; a_0 + a_1 x + ... + a_n x^n$$

with $a_n =: m \in \mathbf{Z}$. Therefore, multiplication with m^{n-1} provides a polynomial

$$g(x) = a_0 m^{n-1} + a_1 m^{n-2}(mx) + ... + (mx)^n\,,$$

i. e. a polynomial g with $g(\frac{\alpha}{m}) = 0$. So – given an algebraic ϑ –

The ring of all algebraic integers of $\mathbf{Q}\,[\vartheta]$ *is integrally closed in its quotient field.*

Dedekind dropped the requirement that the *extension* should be a *number domain* and looked for an extension of $(\mathbf{N}, \cdot, \,|\,)$, such that $a, b \in \mathbf{N}$ satisfy $a\,|\,b$ in this extension iff $a\,|\,b$ is satisfied already in $\mathbf{N}$. Such an extension should have – above all – an optimal *divisibility arithmetic* and, of course, this depends highly on the elementary property that for all a, b there exist elements u, v satisfying

(L) $$ua + vb \;=\; c \text{ with } c\,|\,a \;\&\; c\,|\,b \quad (\exists\, u, v)\,.$$

So it doesn't seem unlike that Dedekind was led by this phenomenon to his solution, most satisfactory not only for the particular case $\mathbf{Q}\,[\zeta]$, ζ *a primitive p-th identity-root,* but even clearing divisibility interrelations of $\mathbf{Z}$ in the framework of fields of type $\mathbf{Q}\,[\vartheta]$.

Dedekind created the notion of an *ideal* by considering number sets $\mathfrak{a}$, closed under + and containing together with each $x \in \mathfrak{a}$ all multiples of this x – and constructed thus an extension $(\mathfrak{A}, \cdot, \supseteq)$ of $(\mathbf{N}, \cdot, \,|\,)$ satisfying

$$\begin{aligned} \langle a\rangle \cdot \langle b\rangle \quad &= \quad \langle ab\rangle \\ \& \qquad \langle a\rangle \supseteq \langle b\rangle \;&\Longleftrightarrow\; a\,|\,b\,, \end{aligned}$$

and having the *unique prime decomposition property.* By this structure DEDEKIND then could contribute efficiently to a deepening and extension of KUMMER's results on FERMAT's problem, cf. BOREWICZ/ŠAFAREVIČ.

DEDEKIND gave three different outlines of his theory in the supplements, cited above. In particular, in the fourth edition he presented the *Gruppensatz*, telling that the group property of the semigroup of modules $\mathfrak{m}$ which can be multiplied by some c into some ideal $\mathfrak{a} = \mathfrak{m} \cdot c$ leads to the implication

$$\text{(M)} \qquad \mathfrak{a} \supseteq \mathfrak{b} \implies \mathfrak{a} \mid \mathfrak{b}$$

which turned out to guarantee an *ideal* (*unique*) *prime factorization.*

It is easily seen that DEDEKIND's outline up to the *Hauptsatz der Idealtheorie* is of purely algebraic nature. Hence it seems to be most natural that in a fundamental joint paper on *function fields,* [102], RICHARD DEDEKIND and HEINRICH WEBER in 1882 obtain similar results for $\mathbf{Q}(x)$ as DEDEKIND before did w. r. t. algebraic extensions $\mathbf{Q}(\vartheta)$, thus pushing forward even to the theorem of RIEMANN/ROCH . DEDEKIND's success gave rise to intensive endeavours on alternative approaches to some ideal arithmetic. We notice here the contributions of ZOLOTAREV, [435], ENGSTRÖM, [120], and GRAV, [168], [169], on the one hand – and the outlines of HURWITZ, [204], PRÜFER, [351], TSCHEBOTAREV, [404], VON NEUMANN, [335], and ZYGLINSKI, [437], on the other hand.

Leopold Kronecker 1823 - 1891

But, of course, first and formost there is to mention the concept of LEOPOLD KRONECKER (1823 -1891).

Readers, interested in KRONECKER's theory and its significance are referred to the genetic-analytic presentation [118] of EDWARDS where not only the number theoretical aspects discussed but also its algebraic-geometrical relevance up to RIEMANN/ROCH from a new point of view, partially even exceeding KRONECKER .

As to this introduction, we will restrict our considerations to a brief sketch of KRONECKER's principal idea, just as done above w.r.t. to DEDEKIND's theory.

KRONECKER's concept is quite different from DEDEKIND's one. His principal interest is **not** *ideal unique factoring* **but** *ideal linear combining the GCD.* So he restores property (L) whereby he obtains all advantages of an ideal arithmetic.

Starting from function rings over "natural" rings KRONECKER shows – in a modern view – that

> *Any integrally closed integral domain $\mathfrak{I}$ admits a ring extension I_x within the transcendental extension $\mathfrak{K}(x)$ of its quotient field $\mathfrak{K}$ satisfying $\mathfrak{I}_x \cap \mathfrak{K} = \mathfrak{I}$, such that every finitely generated ideal is a principal ideal.*

That is, from the modern point of view, DEDEKIND-extensions lead to some *abelian lattice ordered group satisfying* DCC whereas KRONECKER-extensions may lead merely to some *abelian lattice ordered group* admitting infinite chains.

The advantage of KRONECKER's construction, however, is that it provides even a *Bézout-domain,* whence KRONECKER is in the position to calculate along classical lines, whereas DEDEKIND has to work in merely multiplicative structures. Moreover, from the modern point of view, KRONECKER's approach is more constructive than DEDEKIND's approach is.

However, KRONECKER's theory withdraws any attempt of abstract generalization – because of the central and fundamental role of $\mathfrak{K}(x)$.

This is quite different with the "post DEDEKINDian" approach [186], due to KURT HENSEL:

Like DEDEKIND's fundamental idea HENSEL's principal idea is as elementary as fundamental as efficient :

Let $\mathfrak{I}$ be an integral domain with "a good ideal prime factorization arithmetic". Then each *principal ideal* $\langle a \rangle$ is a unique product of finitely many *ideal prime factors* $\mathfrak{p}_i$ $(1 \leq i \leq n)$, such that we are in the position to *associate* with each $a \in I$ a uniquely determined *exponent* $\mathfrak{p}\,(a)$, called the exponent of $\mathfrak{p}$ in the ideal *prime factorization* of $\langle a \rangle$. Thus each $\langle a \rangle$ and thereby also each a is *coded* by a *sequence,* vanishing at all places but finitely many ones, such that any two different elements a, b have the same code, briefly the same *exponent,* iff $a \,|\, b$ and $b \,|\, a$.

Obviously such an exponent admits an extension to the quotient field $\mathfrak{K}$ of $\mathfrak{I}$, and it is easily seen that the function $\mathfrak{p}$ satisfies $\mathfrak{p}\,(a \cdot b) = \mathfrak{p}\,(a) + \mathfrak{p}\,(b)\,.$

Next: If $\mathfrak{p}$ satisfies the implication $\mathfrak{p} \mid \langle a \rangle, \langle a+b \rangle \Longrightarrow \mathfrak{p} \mid \langle b \rangle$, then one gets nearly immediately $\mathfrak{p}\,(a+b) \geq \min(\,\mathfrak{p}\,(a), \mathfrak{p}\,(b)\,)$.

Finally: If $\mathfrak{I}$ is not a field then there exists at least one $a^* \in K$ satisfying $\mathfrak{p}\,(a^*) = 1$.

Therefore: Ideal arithmetic in the sense of DEDEKIND provides necessarily *a system of valuations* w in the preceding sense, but, the opposite is false! For instance, such a system may provide infinitely many relevant non vanishing values, since ACC need not be satisfied in general, even though it is satisfied in the classical number theoretical situation.

Nevertheless, also in this case we have an *ideal system,* called the system of v-ideals, introduced by VAN DER WAERDEN in [416] and ARNOLD in [25], respectively. This will be elabourated below.

For more detailed information about ideal theory, see above all the report [245] of WOLFGANG KRULL, most historical, genetical and analytical as well, a brilliant presentation of ideal theory, *ab ovo*!

1.2 Towards an Abstract Ideal Theory

Emmy Noether
1882-1935

Approximately 45 years after the fundamental contribution of DEDEKIND and WEBER the question of *unique ideal decomposition* is taken up again in [337] by EMMY NOETHER, who studies abstract integral domains exhibiting the principal result:

Genau dann zerfallen die Ideale eines Integritätsbereiches $\mathfrak{I}$ *eindeutig in Primideale, wenn* $\mathfrak{I}$ *in seinem Quotientenkörper* $\mathfrak{K}$ *ganzabgeschlossen ist und zudem* $\mathfrak{I}$ *die aufsteigende Kettenbedingung* (N) *sowie jeder echte Restklassenring von* $\mathfrak{I}$ *die absteigende Kettenbedingung* (A) *erfüllt.*

Already in 1917, 1918 M. SONO had discussed abstract ideal theory in [400], [401], requiring a JORDAN *composition sequence* and the implication $\mathfrak{p} \supseteq \mathfrak{x} \supseteq \mathfrak{p}^2 \Longrightarrow \mathfrak{p} = \mathfrak{x} \vee \mathfrak{x} = \mathfrak{p}^2$, a certain "substitute" of integral completeness.

Nevertheless it is Emmy Noether's contribution, which is considered and celebrated as the

very beginning of that, what nowadays is called the theory of *Dedekind domains.*

Most interesting in addition it seems, that this paper does not appear until 1927, although her *Idealtheorie in Ringbereichen*, [337], appeared already in 1921 and although the notion of *integral completeness* had played an essential role in her early paper [336], even though in a different context.

The importance of these two Noether papers has nowadays to be seen in their methodical aspects rather than in their results. This view is confirmed also by Emmy Noether herself, who liked to emphasize:

Es steht alles schon bei Dedekind !

But her axiomatical approach may be regarded as some change in doing algebra, sometimes considered even as a milestone in algebra.

Next to Emmy Noether there are to mention Heinz Prüfer and above all Wolfgang Krull who contribute fundamentally to ideal theory already in the twenties.

Prüfer studies divisibility under the assumption that all *finitely generated* ideals $\langle a_1, \dots, a_n \rangle$ be *divisors,* i. e. under the condition

$$\text{(P)} \qquad \langle a_1, \dots, a_n \rangle \supseteq \langle b \rangle \implies \langle a_1, \dots, a_n \rangle \Big| \langle b \rangle \,,$$

[351] and [352], whereas Krull introduces the notion of an AM-*Ring* [1)], i. e. a ring satisfying $\mathfrak{a} \supset \mathfrak{b} \Longrightarrow \mathfrak{a} \mid \mathfrak{b}$, however with ACC, which leads even to the implication $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \mid \mathfrak{b}$.

Non-Noetherian AM-*rings* are considered first by Akizuki in [2].

But not until the early thirties it is Shinziro Mori, who turns systematically to a general theory of *multiplication rings*, briefly *M-rings,* $(\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \mid \mathfrak{b})$. His papers scatter over a period of about 25 years from 1932 by 1957, such that Gilmer/Mott remark in [163] : "Mori developed most of the structure theory." Nevertheless one has to say that Mori gives

1) Allgemeiner Multiplikations-Ring

a characterization of arbitrary multiplication rings merely modulo the requirement that each ideal be an irredundant intersection of *primary* ideals.

However, applying a crucial result of Krull, ([244], Satz 10), Mori verifies

$$(\mathfrak{a} = \ker \mathfrak{a} \;\; (\forall\, \mathfrak{a})) \Longleftrightarrow (\mathfrak{p} \textit{ prime} \Rightarrow \mathfrak{p} \textit{ idemp.} \vee \mathfrak{p} \textit{ irred.}).$$

Here $\ker \mathfrak{a}$ means the intersection of all primary ideals $\mathfrak{q} \supseteq \mathfrak{a}$ where $\mathrm{Rad}\, \mathfrak{q} =: \mathfrak{p}$ be *minimal prime* above $\mathfrak{a}$.

In 1964 Mott takes up the problem of describing M-rings, again, consult [304]. He finds out that $\mathfrak{R}$ is an M-ring iff

(*i*) $\ker \mathfrak{a} = \mathfrak{a}$.

(*ii*) $\mathfrak{q}$ *primary* $\Longrightarrow \mathfrak{q} = (\mathrm{Rad}\ \mathfrak{q})^n$.

(*iii*) *If $\mathfrak{p}$ is a minimal prime divisor of $\mathfrak{a}$ and if in addition n is the first exponent such that $\mathfrak{p}^n$ is an isolated primary component of $\mathfrak{a}$ with $\mathfrak{p}^n \neq \mathfrak{p}^{n+1}$, then $\mathfrak{p}$ does not contain the intersection of the remaining primary divisors $\mathfrak{p}_i^{n_i}$ of $\mathfrak{a}$ with minimal $\mathfrak{p}_i$ above $\mathfrak{a}$.*

These investigations are completed in 1965 by Gilmer/Mott in [163], with respect to arbitrary commutative rings. One central result of that paper tells:

$$(\mathfrak{a} = \ker \mathfrak{a} \;\; (\forall\, \mathfrak{a})) \Longleftrightarrow (\mathrm{Rad}\, \mathfrak{a} \text{ prime} \Rightarrow \mathfrak{a} \textit{ primary}),$$

another one is the equivalence:

$$\mathfrak{R} \textit{ is an M-ring} \Longleftrightarrow \mathfrak{R} \textit{ is a weak M-ring,}$$

i. e., in order that $\mathfrak{R}$ be an M-ring it suffices that each prime ideal $\mathfrak{p}$ of $\mathfrak{R}$ satisfies the implication $\mathfrak{p} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{p} \mid \mathfrak{b}$.

But in both papers, in [163] and in [304] as well, and again in [268] this fact is proven ring theoretically. Finally Gilmer/Mott characterize commutative M-rings as rings satisfying

(*i*) $\mathrm{Rad}\, \mathfrak{a}$ *prime* $\Longrightarrow \mathfrak{a}$ *primary*.

(*ii*) $\mathfrak{q}$ *primary* $\Longrightarrow \mathfrak{q} = \mathfrak{p}^n$, ($\mathfrak{p}$ *prime*).

(*iii*) *If $\mathfrak{p}$ is a proper prime ideal of $\mathfrak{R}$ and if in addition $\mathfrak{p}^n \supseteq \mathfrak{a} \not\subseteq \mathfrak{p}^{n+1}$ then there exists an element $y \notin \mathfrak{p}$ with $\mathfrak{p}^n = \mathfrak{a} : \langle y \rangle$,* and additionally – based on ring theoretical aspects – they point out that the combined condition (*i*) & (*ii*) is equivalent to the implication

$$\text{Rad } \mathfrak{a} \textit{ prime} \implies \mathfrak{a} = (\text{Rad } \mathfrak{a})^n \quad (\exists\, n \in \mathbf{N})\,.$$

M-rings with a view to their total quotient rings are investigated by GRIFFIN in [175]. Here it is shown, in particular, that in M-rings satisfying

$$\forall a \in R \;\exists\; e_a = e_a^2 \;:\;\; ae_a = a$$

finitely generated ideals are 2-*generated.*

As soon as a good commutative theory is exhibited, the question arises whether there is an adequate non-commutative generalization. This question is attacked partly by UKEGAWA, lateron in co-operation with UMAYA and SMITH, respectively, in [405],..., [411], and [394], culminating finally in SMITH, [278], where it is shown that also in the non-commutative case weak AM-rings are even AM-rings.

Merely for the sake of completeness we mention the non-commutative contributions of MURATA, [311],...,[315], which, however, don't have any meaning for this paper.

A first Summary : Already Dedekind emphasizes the importance of the Gruppensatz and shows in principal that this property is equivalent to condition (M) above.

This condition (M) is taken up in the twenties and leads to the notion of a multiplication ring which since then has been an object of intensive and extensive investigations.

Integral domains satisfying (P) were studied first by PRÜFER, [352] , in honor of whom these rings are called nowadays *Prüfer domains.* But the most important characterization of Prüfer domains is due to KRULL, who pointed out that a domain is a Prüfer domain iff each of its localizations R_P is a valuation ring, say has comparable ideals.

Since the method of *localization,* coming from p-adic considerations, and generalized to arbitrary commutative rings by KRULL, is a powerful tool in ring theory, in particular most suitable when studying Prüfer domains, this method may be assumed to be of high importance also w. r. t. lattice theoretical approaches of abstract ideal theory.

Nevertheless, apart from KRULL's condition, there is a most interesting lattice condition, characterizing Prüfer rings. More precisely: the Prüfer condition is equivalent to *distributivity* of the ideal lattice, that is satisfies

$$\text{(D)} \qquad \mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \ = \ (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c})\,.$$

This condition was introduced by FUCHS in [131], and is taken up by JENSEN who proves (D)$\Longleftrightarrow$(P) and gives a new push to the theory of *Prüfer rings* in such a way that LARSEN/MCCARTHY in [268] pay much attention to *Prüfer structures* and *Dedekind structures* as well. Simultaneously once again there arises much discussion of Prüfer structures, culminating in HUCKABA's book [203], where Prüfer rings are defined as rings in which every finitely generated ideal $\mathfrak{a}$, containing at least one cancellable element, is *invertible* or equivalently satisfies the implication $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \mid \mathfrak{b}$.

The most significant aspect of condition (D) is, of course, that it tells exclusively about order relations in the set of *congruences.* Hence it is even of general algebraic nature.

Next, we have to cite a paper of D. D. ANDERSON, [3], where the interaction of $\mathfrak{R}$, $\mathfrak{R}\,[x]$ and $\mathfrak{R}\,(x)$ is investigated, based, of course, on preceding papers. Here it is proved, apart from other results:

(*i*) $\mathfrak{R}\,[x]$ *is an M-ring iff* $\mathfrak{R}$ *is a finite direct product of fields.*

(*ii*) $\mathfrak{R}\,(x)$ *is an M-ring iff* $\mathfrak{R}$ *is an M-ring*.

(*iii*) $\mathfrak{R}\,(x)$ *satisfies* (D) *iff* $\mathfrak{R}$ *satisfies* (D)*, and in this case* $\mathfrak{R}\,(x)$ *is even a Bézout ring.*

Recall KRONECKER's approach. The analogy between condition (*iii*) and KRONECKER's theorem is obvious.

We return to the conditions (M), (P), (N) and (D). Obviously these conditions do not depend on any typical ring theoretical property. Objects under consideration are *sets* and *inclusions*, *products* and *congruences.* Consequently the conditions above are easily redefined for *arbitrary groupoids* and thereby in particular for *semigroups of complexes.* Moreover the Prüfer, and the Mori problem as well, admit more abstract versions w.r.t. the structure of a (*complete*) *algebraic m-lattice* (*multiplicative lattice*), i. e. a complete lattice on which a multiplication is defined, satisfying:

$$\text{(AML)} \qquad A \cdot (\textstyle\sum_{i\in I} B_i) \cdot C \ = \ \textstyle\sum_{i\in I}(AB_iC)\,.$$

That this is not exhibited explicitly until the late thirties should have a simple reason. Only gradually algebraists turn to thinking in lattice structures, even though already DEDEKIND had made first steps "in lattices", which he called *dual groups,* [100], [101].

However, KRULL presented some contributions to an *element free* ideal theory already in the early twenties. The proposal to do ideal theory in an axiomatical way, based on ideal properties only, is due to him, [240], compare his article

Axiomatische Begründung der Idealtheorie

and he is the first, as well, who contributes – implicitly – already in 1929 to theory of algebraic m-lattices by his article :

Idealtheorie in Ringen ohne Endlichkeitsbedingung.

Cum grano salis, in this paper the structure of a ring is taken merely as means of discussion.[2)]

Among the rings with a *good ideal arithmetic,* so far, there are missing two most classical structures, which obviously have an extraordinary ideal theory although not being *Dedekindian*, namely : The ring $\mathfrak{G}$ of all algebraic integers and the ring $\mathbf{Q}\,[x,y]$. This gives rise to the question, whether another type of ideal might succeed where Dedekindian ideals fail. And, moreover, since addition participates merely from a secondary point of view, whereas multiplicative aspects are highly dominating, an attempt is motivated, to settle ideal theory from a purely algebraic point of view , i. e. to start from a *monoid* or some *monoid with zero.* First attempts in this direction go back to 1929.

We recall HENSEL's *valuations* or equivalently *exponents,* and start from a *cancellative monoid.* Building w.r.t. a set A in a first step the set $[A]$ of all elements, whose *exponent* remains below every exponent coding some $a \in A$, and after this building the v*-ideal* $\mathfrak{a} := ([A])$ of all elements, with *exponents* majorizing each exponent, coding an element of $[A]$, we arrive at some set of "ideals", called v-ideals (in German: V̲ielfachen-Ideale) ,

2) At this place the author would like to mention ISIDORE FLEISCHER's analysis [126] of KRULLS early influence in abstract ideal theory. That paper offers a short cut introduction to abstract ideal theory including logical and topological aspects, and in a certain sense might be considered as an " homage" to WOLFGANG KRULL.

behaving like d-ideals and satisfying:

$$\mathfrak{a} \text{ is a } v\text{−ideal} \quad \text{iff} \quad \left(\frac{s}{t}\,\Big|_S\, \mathfrak{a} \Longrightarrow \frac{s}{t}\,\Big|_S\, c \right) \Longrightarrow c \in \mathfrak{a}$$

or, equivalently, according to CLIFFORD, [93],

$$\mathfrak{a} \text{ is a } v\text{−ideal} \quad \text{iff} \quad (\, s \,|\, \mathfrak{a} \cdot t \Longrightarrow s \,|\, c \cdot t \,) \Longrightarrow c \in \mathfrak{a}\,.$$

Thus a semigroup theoretical approach to a general ideal theory of semigroup theoretical relevance is obtained.

First[3)] contributions to v-ideal theory in cancellative monoids appear in 1929, due to ARNOLD and VAN DER WAERDEN, respectively, independent one from each other, but influenced by EMMY NOETHER – two papers, not onely methodically, but even definitely operating *semigroup theoretically* and presenting the result:

> *A cancellative monoid* $(S, \cdot, 1)$ *owns an S-division respecting extension with the unique prime factorization property iff its v-ideal semigroup has this property.*

This approach is taken up in the thirties w.r.t. arbitrary commutative monoids by A. H. CLIFFORD in [93]. CLIFFORD modifies the notion of a v-ideal in the above sense and studies the question of unique ideal prime factorization under the condition, that the ideal primes are irreducible. Finally the author takes up CLIFFORD's ideas in the late fifties/early sixties, settling the general case in [59], [60], [61].

For integral domains the result of ARNOLD/VAN DER WAERDEN means nothing else but that exponents in the above sense do exist if and only if the ZPI-*theorem* for v-ideals is valid, i. e. iff *every v-ideal has a unique v-prime ideal decomposition.*

Let α be integral w.r.t. the integral domain $\mathfrak{I}$. Then the module $\{\alpha^n\}$ is finitely generated in the quotient field $\mathfrak{K}$ of $\mathfrak{I}$. Consequently there exists an element $c \in I$ with $c \cdot \{\alpha^n\} \subseteq I$. This motivates to call β *almost integral* over the ring $\mathfrak{R}$ if β satisfies $c \cdot \{\beta^n\} \subseteq I$. Thus we are led to a v-ideal criterion for condition (M) *via* the implication

(v) $$s^n \,|\, c \cdot t^n \ \ (\forall\, n \in \mathbf{N}) \implies s \mid t\,,$$

---

3) Clearly, a v-ideal in general is what upper classes of DEDEKIND-cuts are in the particular case of the rationals. From this point of view, DEDEKIND is again the forerunner.

meaning nothing else but that in the quotient field of $\mathfrak{J}$ does't exist any almost integral element α outside of S, satisfying $c \cdot \{\alpha^n\} \subseteq S$ $(c \in S)$, whence in this case $\mathfrak{J}$ is called *completely integrally closed.*

Completely integrally closed are for instance the domain $\mathfrak{G}$ of all algebraic integers, and the domain $\mathbf{Q}\,[x_1, \dots, x_n]$. This is easily seen, since condition (v) is satisfied in every *UF-domain* (unique factorization domain).

But: $\mathfrak{G}$ does not satisfy ACC for d-ideals and $\mathbf{Q}\,[x, y]$ does not satisfy DCC for d-ideals w.r.t. proper *residue class rings.*

So, these domains do not satisfy the *d-group theorem*, but by (v) these structures satisfy the *v-group theorem* and thereby condition (M) for v-ideals, thus proving to be a strong alternative ideal arithmetic.

Furthermore it has to be stressed that in field extensions *exponent extensions* are easier to handle than the *d-ideal extensions* are.

Finally we emphasize that the *v-ideal semigroup* is a *homomorphic image* of any other *ideal semigroup,* already in the semigroup case.

This means for commutative rings $\mathfrak{R}$ with identity, that the v-ideal semigroup is a homomorphic image of all other ideal semigroups whose ideals are also d-ideals. In this sense, the d-ideal semigroup is the finest, the v-ideal semigroup the coarsest semigroup of d-ideals with the property that all 1-*generated ideals* are of type $R \cdot a$.

However, v-ideals suffer from two essential lacks. On the one hand, from the number theoretical point of view, v-ideals in rings $\mathfrak{R}$ need not satisfy $\mathfrak{a} + \mathfrak{b} = R \Longrightarrow a + b = 1$ $(\exists\, a \in \mathfrak{a}, b \in \mathfrak{b})$. On the other hand, from the algebraical point of view, they need not have the crucial property of *finite character* which requires that an element a is contained in the ideal hull of a family A_i $(i \in I)$ of ideals, if it is contained already in the hull of a finite subfamily of A_i $(i \in I)$.

But, in spite of these lacks, the v-ideal offers a possibility to transfer the d-ideal to monoids. To this end we consider $\mathfrak{G}$, the domain of algebraic integers.

Here finitely generated d-ideals are finitely generated v-ideals and *vice versa,* whence arbitrary d-ideals may be considered as subsets $\mathfrak{a}$, containing together with each finite subset also the v-ideal, generated by this subset. Subsets of this type were introduced as t-ideals by LORENZEN in [275] and prove to be a most suitable substitute of d-ideals in arbitrary commutative monoids (with zero).

Altogether: As far as a sketch may achieve this, it should have become clear, at least a bit, which way the d-ideal system on the one hand and the v-ideal system on the other hand contribute to classical ideal theory. But again, the reader should not hesitate to consult Krull [245].

So, maybe apart from others, there are two possibilities, above all, of transferring classical ideal theory to abstract structures, namely one along the lines of v-ideal theory, and another one along the lines of t-ideal theory.

As to the first, recall Arnold, van der Waerden, Clifford and the author's contributions to v-ideal theory.

As to the second, there is to mention first of all Paul Lorenzen, who presents in [275] a general abstract ideal theory for cancellative monoids, introducing, apart from other aspects, the system of t-ideals. Lorenzen's ideas are then taken up by Paul Jaffard and Karl Egil Aubert, compare for instance Jaffard's contribution to the ideal theory of cancellative monoids, [213], and Aubert's fundamental paper on *x-ideals*, [38], aside from others, look at [29],..., [41].

But a strong theory of cancellative monoids á la Arnold/van der Waerden is not given until the eighties, based on [55], and an article of Skula [392], improving the results of Borewicz/Šafarevič. Most interesting: this is done by number theoretists rather than algebraists, like Narkiewicz, cf. [333], [334], and Halter-Koch, Geroldinger, Lettl w.r.t. questions of algebraic number theory, ring theory, and convex geometry, cf. [140], [141], [177],..., [179], [272]. And even a paper of analytical character is published, cf. Krause, [237].

Cancellative monoids á la Arnold/van der Waerden are nowadays called cancellative monoids with *divisor theory.* They have a good *analytical characterization* due to Krause, and a most important *algebraic characterization* due to Halter-Koch, who proved in [178]:

$$\begin{gathered}\mathfrak{S}\ \textbf{has a divisor theory}\\ \textbf{iff}\\ \mathfrak{S}\ \textbf{is the divisibility monoid of some Krull domain}\end{gathered}$$

i. e. a domain whose *monoid of principal ideals* has a divisor theory. So – according to a verbal proposal of FRANZ HALTER-KOCH – cancellative monoids with divisor theory in this note are also called *Krull-monoids.*

Given an arbitrary semigroup, the very first question arises, which subsets should be defined as ideals. From the semigroup theoretical point of view the *Rees ideal* ($SI \subseteq I \supseteq IS$) seems to be some suitable candidate, but looking at rings, these sets are obviously too narrow, in what sense ever. As a lattice distributive system, however, *Rees ideal* semigroups have most interesting aspects from the general point of view, and may contribute to characterizing classes of special semigroups in a nice way.

To get an insight, the reader should study D. D. ANDERSON and E. W. JOHNSON, [14]. Here the particularities of Rees ideals are referred, however the articles [103] and [219], concerning *order ideals*, remain unconsidered.

As to the Mori property and related problems on Rees ideals, the reader is referred to DOROFEEVA, MANEPALLI and SATYANARAYANA, [107],. . . , [109] and [285],. . . , [288], respectively. Here the authors uncover, in a certain sense, the semigroup theoretical component of certain ring theoretical contributions.

We come back to lattice theoretical aspects, i. e. to ideal theory in m-lattices. Grown up from the pioneer papers of MORGAN WARD and ROBERT P. DILWORTH in the late thirties, [419], . . . , [422], and the fundamental paper of DILWORTH, [103], m-lattice theory provides a most natural generalization of classical ideal theory, as is pointed out for instance in FUCHS [135].

And, last but by no means least, there is an article of FLEISCHER, [109], analyzing and referring relations between m-lattices and x-ideals.

Finally, we take up again t-ideals, this time w.r.t. rings.

That v-ideal and t-ideal investigations are recently booming is indicated by contributions to the theory of *Krull* and *Mori domains* for instance by VALENTINA BARUCCI and STEPHANIA GABELLI, respectively, [48], [49], [18], [379], [137], and above all by MOSHE ROITMAN et al., [377], [378], [379], [97], [106], by ZAFRULLAH et al., [281], [198], by DOBBS et al., [11], [105], [106], where [11] is even a six-men-paper, and by GRIFFIN, [170], Ira Papik, [345], and Kang, [225], [226], on *v-multiplication rings,* and by Griffin, [172], Kennedy, [231], and Mott, [305],[307], on *Krull rings.*

Altogether, v-ideals and t-ideals have attracted much interest in cancellative monoids and integral domains, and there is no lack in interesting results. But, as far as arbitrary monoids are considered, acceptable answers to the questions

Which properties characterize the Prüfer condition (P) ?

Which properties characterize the Mori condition (M) ?

have remained open, so far.

This is by no means different w.r.t. the investigations of the author towards a general theory of *divisibility semigroups,* abbreviated *d-semigroups.*

Starting from the system $(\mathfrak{A}, +, \cdot)$ of the finitely generated ideals $\mathfrak{a}$ of an *arithmetical* commutative ring with identity, i. e. a ring with distributive ideal lattice, we get:

(A1) $(\mathfrak{S}, \cdot)$ is a semigroup.

(A2) $(\mathfrak{S}, +)$ is a semi-lattice.

(A3) $\mathfrak{x}(\mathfrak{a} + \mathfrak{b})\mathfrak{y} = \mathfrak{x}\mathfrak{a}\mathfrak{y} + \mathfrak{x}\mathfrak{b}\mathfrak{y}$.

(A4) $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \,|\, \mathfrak{b}$.

And choosing these conditions as defining axioms we are led to the structure of *d-semigroups*, whose theory is studied by the author in [63],. . . ,[75], and presented also in the lecture note [77], whose final version is part I of the present folder on TOPICS OF DIVISIBILITY.

But, while the *lattice semigroups* of the *lattice ideals* and the *multiplicative ideals* w.r.t. their formative influence are studied in a satisfactory manner in [74] and [75], respectively, this is quite different with the system of *m-filters,* i. e. subsets, satisfying the implications ($a, b \in F \Longrightarrow a \wedge b \in F$ and $a \in F \Longrightarrow sat \in F$) .

And open as well remained up till now the question, which properties do provide a good description of *lattice semigroups,* satisfying condition (A4).

Hence, studying the Prüfer and the Mori problem in arbitrary situations, really imposes itself to people working on *po*-structures. And this the more, since references from d-semigroups to Prüfer rings and *vice versa* are missing, in spite of respectable developments in both of these fields within the last 25 years. In this sense we may announce:

This paper is both:

A contribution to abstract ideal theory

and

A contribution to the theory of lattice semigroups.

1.3 The Contents

Central and fundamental structure of the main chapters will always be a *complete m-lattice* $\mathfrak{V} = (\mathcal{A}, +, \cap, \cdot)$ whose elements are in general denoted by capital Roman letters – with a *fixed basis* $\mathcal{A}_0$ whose elements will be denoted by lower case Roman letters, whenever we want to emphasize that we are dealing with generators. Provided $\mathfrak{A}$ is even algebraic, we will tacitly suppose that $\mathcal{A}_0$ is even a system of *compact generators.*

If each $a \in \mathcal{A}_0$ is even a *divisor* $(a \supseteq b \Longrightarrow aX = b = Ya \ (\exists\, X, Y))$, $\mathfrak{A}$ will be called an *ideal structure*, and if moreover $\mathcal{A}_0$ is even *closed under multiplication* with compact identity 1, $\mathfrak{A}$ will be called an *ideal semigroup.*

Generators, of course, are considered as something like *principal ideals of rings, semirings* or *semigroups*, but, as is well known, an abstract characterization of principal ideals of rings is impossible. Nevertheless, in many cases the *principal elements* t introduced by DILWORTH in [103] *via*

$$\begin{array}{rrcl} & (a \cap b : t) \cdot t & = & a \cdot t \cap b \quad (\forall\, a, b) \\ \text{and} & (a + b \cdot t) : t & = & a : t + b \quad (\forall\, a, b) \end{array}$$

are a reasonable substitute. They are always divisors, forming always a semigroup. However, there are ideal systems, such that even each ideal is a principal element in the sense above, for example this is the case in Dedekind domains.

In this note principal elements remain outside, except for some remarks at the end of chapter 7. Our way is to start from an AML with a fixed basis.

Let us note $A\,|_\ell\, B$ iff A is a *left divisor,* i. e. if A satisfies some equation $AX = B\ (\exists\, X)$ and let us note $A\,|\,B$ if A is a *divisor,* i. e. if A satisfies even $AX = B = YA\ \ (\exists\, X, Y)$.

Hereby the meaning of the *left Prüfer condition* and the *Mori condition* should be clear.

In order to give a most classical model of the central structures settled later on, we start with a chapter on *factorial rings.*

After this we offer an approach to the theory of ideals in semigroups, starting from a *closure operator.*

This idea goes back to Prüfer [351] and is explicitly cultivated by Krull in [245], where the notions of the v-ideal and the a-ideal are exhibited in a most intensive consideration, by Fuchs in [135], by Kirby in [233], and by Gilmer in [156]. Beyond that one has to mention within this context L. J. Ratliff's article on the Δ-Operator, [354]. Here the ideal structure of a commutative ring with identity seems to serve merely as specialized algebraic multiplication lattice, whence this paper contributes indirectly to an element free ideal theory, exactly in the sense of Krull.

From this point of view our approach is by no means new, but nevertheless there are some insights, seeming new, as far as the author was able to check.

The next chapter provides the arithmetic of m-lattices, as far as this will be necessary for later developments. In particular we will define *residue systems* and *localizations.* Parts could have been cited w.r.t. other papers, however not without disturbing continuity. And moreover one has to take into account that the underlying structure is formally weaker than that of a semigroup of ideals, since abstract ideal theory here is done in an *element free manner,* whence it has to be verified in any case that the classical methods ar still working under (our) weaker assumptions.

We then start discussing *Prüfer problems*, beginning with the left side case. The structure under consideration will be the Algebraic Multiplication Lattice, generated by *left divisors.* This means that the results of this chapter do not remain true in general for semigroups of v-ideals, but large parts will turn out to be independent from the finite character property and consequently most suitable to contribute to a particular study of v-ideals, which is left to a final chapter.

Fundamental will be the theorem that left Prüfer structures are characterized by $\mathfrak{a} \cap (\mathfrak{b} \cup \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) \cup (\mathfrak{a} \cap \mathfrak{c})$ & $(a+b)(a*b+b*a) = a+b$.

Most central and fundamental is the chapter on *prime divisors* and *Mori structures.* Here the *Mori problem* is discussed w.r.t. to an arbitrary AML, which is not assumed to be commutative, but which will turn out to be commutative. Some special AML, for instance, is the lattice of ideals of a semiring.

In accordance to arbitrary rings it is shown next that condition (M) is satisfied iff (M) is satisfied for all *prime supelements* P of B.

Furthermore, as a most surprising result we obtain that an AML, generated by some $\mathcal{A}_0$ of left divisors, is a Mori structure if and only if it satisfies simultaneously the subsequent equations:

$$\text{(A)} \qquad A^n \supseteq B \ \ (\forall n \in \mathbf{N}) \implies AB = B = BA\,,$$

$$\text{(J}^*\text{)} \qquad (A*B+B*A)^2 \ = \ A*B+B*A\,,$$

$$\text{(J}^{\cdot}\text{)} \qquad (A:B+B:A)^2 \ = \ A:B+B:A\,.$$

Here the reader may think of $A*B$ as of the *right ideal quotient* and of $B:A$ as of the *left ideal quotient* in rings.

Therefore, a commutative ring $\mathfrak{R}$ with identity 1 is a multiplication ring, iff its *ideal system* has the *archimedean property* and satisfies in addition $(\mathfrak{a}:\mathfrak{b}+\mathfrak{b}:\mathfrak{a})^2 = \mathfrak{a}:\mathfrak{b}+\mathfrak{b}:\mathfrak{a}$.

Finally the particular case of a divisor generated AML is considered.

Next we turn to *hyper-normal* ideal structures. Hyper-normality deals with the ring theoretical particularity that $\langle a\rangle\langle u\rangle = \langle a\rangle$ implies the existence of some $\langle u\rangle^* \perp \langle u\rangle$ with $\langle a\rangle\langle u\rangle^* = \langle 0\rangle$, for instance $\langle 1-u\rangle$.

This chapter is closely related to classical ideal theory. But since we are working "without elements" new ways of proofs are required. Furthermore one has to take into account, that the class of AMLs considered here is larger than that of ideal systems of commutative rings with identity. But, nevertheless, the progress is rather based on the methods than on the results. It's lattice theory, not ring theory!

One result among others, which may show the power of such endeavour in the sense of KRULL, is the proposition telling, that in hyper-normal ideal structures idempotent elements are sums of idempotent generators, a result for commutative rings with identity going back to MORI [300] and for more general cases proven in GILMER/MOTT [163] and in GRIFFIN [175] as well.

The chapter on hyper-normal ideal structures is followed by a chapter on factorial AMLs on the one hand, and on *classical* ideal semigroups, i. e. *lattice modular ideal semigroups* satisfying that prime elements produce *residue systems* without *zero divisors,* that is elements satisfying $A*0 \neq 0$.

Next we investigate *archimedean Prüfer ideal semigroups.* Main result will be that these ideal semigroups in the classical and also in the hyper-normal case are exactly those whose *localizations* $\mathfrak{A}_M$ are even Mori-ideal semigroups. This property serves in commutative ring theory as definition of the *almost multiplication ring.*

Thus – according to our results – a commutative ring $\mathfrak{R}$ with identity is an almost multiplication ring iff its ideal system forms an archimedean Prüfer structure.

But also in the general case this chapter provides an interesting result, as far as an answer is given to an open question on d-semigroups, telling that the semigroup of the positive *filters* of a d-semigroup $\mathfrak{S}$ is archimedean iff $\mathfrak{S}$ admits an embedding in a *cube lattice.*

In a final chapter we then investigate v- and t*-ideal semigroups* of *monoids.* This will point out again, indirectly, the big power of the algebraic property, which in general is missing, of course, in v-ideal semigroups. But in spite of this we will succeed in characterizing v-ideal semigroups with Prüfer or Mori property by combining the archimedean property with the requirement that each $\langle a\rangle * \langle b\rangle$ be a divisor.

In addition this result clears the interrelation of the archimedean property and the classical *being completely integrally closed* since in cancellative monoids (v) is equivalent to the combination above.

Furthermore, amazingly it turns out that a cancellative monoid is a Mori monoid with respect to some semigroup of ideals iff its v-ideal semigroup satisfies the implication

$$\mathfrak{a} \cdot \mathfrak{x} = \mathfrak{a} \cdot \mathfrak{y} \Longrightarrow (\mathfrak{a} \cap \mathfrak{b}) \cdot \mathfrak{x} = (\mathfrak{a} \cap \mathfrak{b}) \cdot \mathfrak{y}\,,$$

which in particular is satisfied, of course, if v-ideals are cancelable.

Worth mentioning seem to be also the characterizations of *Krull monoids.*

In particular the characterization of Krull monoids *via* by the property to be completely integrally closed combined with the condition that each maximal $\mathfrak{m}$ be some $\langle a \rangle * \langle b \rangle$, leads near to a description of Dedekind domains, given by KRULL, cf. [418].

1.4 Some final Remarks

This lecture note concerns above all the *distributive part* of classical ideal theory, originating from number theory. Questions concerning *modular ideal theory,* originating from geometry, will be considered elsewhere.

The text is written in a self contained manner, except for some elementary *lattice theory* and *universal algebra.* For further information the reader is referred to the monographs of FUCHS [135], GILMER [156] and LARSEN/MCCARTHY [268].

The references at the end of the paper are a rich source for those, interested in the subject and, of course, much more than the papers cited. Nevertheless the reader is referred also to the references of the references. Many of these papers – by a critical view – turn out to concern algebraic multiplication lattices rather than rings.

Aknowledgement : The author is very indebted to a real fan of ideal theory, Frau Christel Schnaase, Albertus Magnus Gymnasium Bensberg, for proof reading and critical remarks in *"statu nascendi"* of the German 1994-version *via* **lots(!) of letters** – over a long lasting period, when things changed again and again.

Chapter 2

Factorial Rings

2.1 Preface

Classical ideal theory originated from decomposition problems in certain *number domains.* Therefore first of all we are faced with the fundamental question

What are the factorial rings characterized by ?

It will be pointed out in this section that factorial rings, i. e. rings whose elements are products of *primes* ($p \mid ab \Longrightarrow p \mid a \vee p \mid b$), coincide with *principal t-ideal rings.*

On the basis of semigroup theoretical insights this result was implicitly exhibited in papers [56] through [61], focussed on a prolongation and a deepening of the Fraenkel, [128], Arnold,[1], and Clifford, [93], papers.

However, in a classic paper, [241], Krull had cleared already the question which types of principal ideal rings do exist, clearly a special case w.r.t. the above theorem. Observe that any principal ideal ring is also a principal t-ideal ring. Krull's answer:

> **Es gibt im wesentlichen keine anderen Hauptidealringe als die endlichen direkten Produkte von Komponenten des Typs $\mathbf{Z}$ oder $\mathbf{Z}_p$.**

Since Krull avoided *ring arithmetic* as far as possible and relied on ideal arithmetic aside from the formula $(a + b)(a + b) = a^2 - b^2$ one could say that by this paper *abstract ideal theory* was borne, and recalling KRULL's 1929 paper on kernels one would like to declare

Abstract ideal theory goes back to Wolfgang Krull ! [1)]

The relation between this chapter and KRULLs pioneer paper [241], is easily described: we are concerned with the wider class of principal t-ideal rings, whereas KRULL studied the classical class of principal d-ideal rings. However, one most important difference has to be mentioned: Whereas KRULL studied the behaviour of ideals from the purely ideal theoretical point of view [2)] the author started from element decompositions.

Again, factorial rings carry a strong *t-ideal semigroup* which is, however, by no means in any case identic with their *d-ideal semigroup,* recall the examples given in the introduction. On the other hand this means – in some sense – that factorial rings offer a most interesting starting point for abstract ideal theory. More precisely:

The t-ideal monoid of factorial rings satisfies all conditions studied in this lecture note and so may serve as a universal model !

To write as self-contained as possible, we develop the notions of a *v-ideal* and that of a *t-ideal* and in addition their calculation rules as far as necessary for understanding this chapter, although this will be done *ab ovo* in the subsequent chapter, starting with a development of some abstract ideal theory.

It will turn out that factorial rings have a *direct decomposition* into *factorial domains* and *special primary rings,* i. e. rings whose *ideal semigroup* is exhausted by the powers of some prime element generated ideal $\langle p \rangle$. Thus structure theory of factorial rings basically is structure theory of factorial domains, a theory to which many authors have contributed, we cite P. SAMUEL, [384], and the contribution of LARSEN/MCCARTHY in [177], p. 190 - 200.

[1)] This the more, according to his paper[240], titled "Axiomatische Begründung der Idealtheorie".

[2)] The author would like to regret that – concentrated in the semigroup situation and very busy outside of any University – he failed to discover KRULLs pioneer paper, and so missed the chance of bringing together KRULLs result and his own one.

But in 1961, when *Studienreferendar* of the Ernst Moritz Arndt Gymnasium Bonn he had – invited by Krull – the chance to meet KRULL for discussing his result walking together with that famous mathematician from the Mathematical Institute of the University of Bonn (on the other side of the street) to KRULL's flat. Unforgettable, very impressed, deeply impressed.

Commutative decomposition theory seems to have at least one origin in the paper [128] of A. Fraenkel. All results of this chapter are taken from [56] through [61], except for a result due to D. D. Anderson [3] proven in an alternative manner.

Unique factorization problems play a crucial role in algebraic number theory. But as was pointed out by Mott in [308] unique factorization is also of important relevance in algebraic geometry. So, for the sake of completeness – we copy a most concentrated remark of Mott:

> "...... Unique factorization has its place in algebraic geometry, too.
>
> Zariski [1947] discovered that there are two distinct concepts of a *simple* (or *non-singular*) point on an r-dimensional algebraic variety V in affine n-space. Traditionally, a point P of V had been defined to be simple if and only if rank $J_P = n - r$, where J_P is the Jacobian matrix $[\delta f_i/\delta x_j]$ at P, where
>
> $$\{f_1(x_1, \dots, x_n)\,,\, f_2(x_1, \dots, x_n), \dots, f_t(x_1, \dots, x_n)\}$$
>
> is a basis of the defining prime ideal of V. Zariski defined P to be simple if and only if the corresponding local ring (R, M), where M is the unique maximal ideal of R, is a regular local ring. Then he observed that the two definitions are equivalent if the ground field k has characteristic 0 or is a perfect field of characteristic $p \neq 0$. Now it is common practice to call P a *regular* point if P has a corresponding regular local ring, and to call P a *smooth* point if the Jacobian criterion is satisfied at P.
> But the regular local rings (R, M) that occur in algebraic geometry as local rings corresponding to regular points are special in that they contain the ground field k. Moreover, R^* (the completion of R with respect to the topology determined by the powers of the maximal ideal M) is isomorphic to the ring of formal power series in r determinants over the residue field R/M. Thus R^* is a UFD and Zariski observed that R is a unique factorization domain as well. For several years it was unknown whether this observation could be extended, but Auslander and Buchsbaum [1959] proved that an arbitrary regular local ring is a UFD.

The line of investigation started by ZARISKI reached its zenith in HIRONAKA's [1964] spectacular proof of the resolution of singularities theorem for algebraic varieties over algebraically closed fields of characteristic 0."

2.2 Prime Element Factorizations

Throughout this chapter ring will mean a commutative ring with identity element 1.

Divisibility, whatever this might be, begins with $\mathbf{N}$ and thereby in $(\mathbf{Z}, +, \cdot)$. Drop now all properties apart from those of rings. Then the classical divisibility theory gets lost, but nevertheless there remain good substitutes. So, let henceforth $\mathfrak{R}$ be a ring.

$a \in R$ is called a *divisor* of $b \in R$ (b a *multiple* of a), by symbols $a \mid b$, if there exists some x with $ax = b$.

Let a, b be elements of R and $d \mid c$ for all *common divisors* c of a and b, that is for all $c \mid a, b$. Then d is called *a greatest common divisor,* briefly a GCD of a and b. If in particular 1 is a GCD of a, b then the elements a, b are called *relatively prime.* $c \in R$ is called a *lowest common multiple,* briefly an LCM of a and b if $a, b \mid c$ & $a, b \mid d \Longrightarrow c \mid d$.

Let $a \mid b$ but let b not divide a, denoted by $b \nmid a$. Then a is called a *proper divisor* of b (b a *proper multiple* of a), in symbols $a \parallel b$. Let $a \mid b$ & $b \mid a$. Then a *is called equivalent* to b, by symbols $a \sim b$. Obviously $\mid$ is *transitive* and, according to $R \ni 1$, the relation $\mid$ is in addition *reflexive.*

$a \in R$ is called a *unit,* if $a \mid 1$. $a \in R$ is called a *zero divisor,* if $0 = a \cdot y$ with $y \neq 0$.

The following is well known, of course: If a is a non zero divisor then a is *cancellable* since we get in this case

$$a \cdot x = a \cdot y \Longrightarrow a \cdot (x - y) = 0 \Longrightarrow x - y = 0 \Longrightarrow x = y,$$

and if a is cancellable then a is no zero divisor since in this case

$$a \cdot y = a \cdot 0 \Longrightarrow y = 0.$$

Finally, we call a and b *associated,* symbolized by $a \equiv b$, if $a = b\varepsilon$ with $\varepsilon \mid 1$.

"There seems to be no book showing that the *relations* $\equiv$ and $\sim$ may be different". This is a remark in Irvin Kaplansky [227], where *the ring of real continuous functions* is presented as an example with $\equiv\, \neq\, \sim$. To see this, consider suitable functions f, g with $f(x) = -g(x)$ if $x \le a < b$, $f(x) = g(x) = 0$ if $a \le x \le b$ and $f(x) = g(x)$ if $b \le x$.

2. 2. 1 Lemma. *$\sim$ and $\equiv$ are congruence relatons w. r. t. multiplication.*

PROOF. Straightforwardly. $\square$

2. 2. 2 Lemma. *The units of $\mathfrak{R}$ form a group.*

PROOF. Straightforwardly. $\square$

2. 2. 3 Definition. Let $\mathfrak{S}$ be a commutative monoid. We call

$$\begin{array}{lrlcl} p \in S & \textit{semiprime}, \text{ if:} & p \sim ab & \Longrightarrow & p \mid a \vee p \mid b\,, \\ p \in S & \textit{prime}, \text{ if:} & p \mid ab & \Longrightarrow & p \mid a \vee p \mid b\,, \\ p \in S & \textit{completely prime}, \text{ if:} & p^n \mid ab & \Longrightarrow & p^n \mid a \vee p \mid b\,, \\ p \in S & \textit{irreducible}, \text{ if:} & a \parallel p & \Longrightarrow & a \mid 1\,. \end{array}$$

Let p be semiprime and let $a \parallel p$. Then $ax = p$ $(\exists x \in R)$ and consequently it follows $p = apy = p \cdot ay$ $(\exists y \in R)$ by $p \nmid a$

2. 2. 4 Lemma. *$p \in R$ is semiprime if and only if*

$$ap \;\&\; b \parallel p \;\Longrightarrow\; ab \parallel p$$

i. e. if the set of proper divisors of p forms a monoid.

PROOF.
$$\begin{aligned} a \parallel p \;\&\; b \parallel p \;&\Longrightarrow\; p = asp = btp \;\; (\exists s, t \in R) \\ &\Longrightarrow\; p = asbtp \\ &\Longrightarrow\; p = ab \cdot stp \;\&\; p \nmid ab\,, \end{aligned}$$

and $a \parallel p \;\&\; b \parallel p \Longrightarrow ab \parallel p$ implies

$$p \sim uv \;\Longrightarrow\; p \mid u \vee p \mid v\,,$$

because $p \not\sim uv$. $\square$

Henceforth the $\sim$-class of a will be denoted by $\overline{a}$ and the corresponding homomorphic image of $(R, \cdot)$ by $(\overline{R}, \cdot)$ or $\overline{\mathfrak{R}}$, respectively.

Obviously $(\overline{R}, \cdot)$ is isomorphic with the monoid of *principal ideals* $\langle a\rangle$ w. r. t. multiplication, and moreover it holds

$$a \,|\, b \Longleftrightarrow \overline{a} \,|\, \overline{b} \quad \text{and} \quad a \,\|\, b \Longleftrightarrow \overline{a} \,\|\, \overline{b}\,.$$

Thus $\,|\,$ defines a *partial order* in $(\overline{R}, \cdot\,)$. Hence we may write

$$\begin{aligned} \overline{a} \le \overline{b} &\ \text{ instead of }\ \overline{a} \,|\, \overline{b} \\ \overline{a} < \overline{b} &\ \text{ instead of }\ \overline{a} \,\|\, \overline{b}\,, \\ \text{and } \overline{a} \wedge \overline{b} = \overline{c} &\ \text{ instead of }\ \overline{c} \text{ is GCD of } \overline{a}, \overline{b}\,. \end{aligned}$$

Furthermore it is clear that properties like to be reducible, semiprime, prime, or completely prime are transferred from $\mathfrak{R}$ to $\overline{\mathfrak{R}}$ and from $\overline{\mathfrak{R}}$ to $\mathfrak{R}$.

The main goal of this section is a characterization of rings whose elements are products of primes.

2. 2. 5 Definition. $\mathfrak{R}$ is called *factorial* if each $a \in R$ is a product of prime elements.

We continue by a series of lemmata.

$$a^2 \,|\, a \ \&\ a \sim b \implies a \equiv b\,. \tag{2.1}$$

PROOF. $a^2x = a \ \&\ au = b \Longrightarrow a(ax{-}1{+}axu) = b \Longrightarrow (\ ) \,|\, b \,|\, a \Longrightarrow (\ ) \,|\, 1.$ □

2.1 leads straightforwardly to

$$m > n \ \&\ a^m \,|\, a^n \implies a^m \equiv a^n\,. \tag{2.2}$$

PROOF. $m > n \ \&\ a^m \,|\, a^n \Longrightarrow (a^n)^2 \,|\, a^n \sim a^m.$ □

2. 2. 6 Lemma. *If $\mathfrak{R}$ is finite then $a \sim b \Longrightarrow a \equiv b$.*

PROOF. Suppose $ax = b \ \&\ by = a$. Then it follows $a(xy)^n x = b$ and there exists some $r \in R$ with $x^{r+1} = x^r \cdot \varepsilon$. Hence $b = ax = a(xy)^r \varepsilon = a\varepsilon$. □

2. 2. 7 Lemma. *If a is not semiprime then a is decomposable, meaning that a is equal to some product bc with $b \,|\, a$ & $c \,|\, a$.*

PROOF. By assumption there exists a product bc satisfying the equivalence $a \sim bc \ \&\ b \,|\, a \ \&\ c \,|\, a$.

Suppose now $a = bcd$. If in addition $bd \,\|\, a$ or $cd \,|\, a$, the proof is complete. Otherwise we have $a \sim cd$ and $a \sim bd$, say

$$au = cd \quad \text{and} \quad av = bd\,.$$

But this implies
$$\begin{array}{rcl} a = bcd & = & bau = cav \\ & \rightsquigarrow & \\ a & = & cbauv \\ & = & bc \cdot a \cdot uv \\ & \sim & a^2\,. \end{array}$$

So, it follows $a \equiv bc$, say $a = b \cdot c\varepsilon$, with $b \,\|\, a,\ c\varepsilon \,\|\, a$. □

(2.3) $$p \ \textit{semiprime} \iff p = ab \Rightarrow p \,|\, a \vee p \,|\, b\,.$$

PROOF. According to the preceding lemma *p is not semiprime* iff *p does not satisfy $p = ab \Longrightarrow p \,|\, a \vee p \,|\, b$.* □

2. 2. 8 Lemma. *Every reducible semiprime element is a zero divisor.*

PROOF. $1 \,\|\, a \,\|\, p \Longrightarrow p \sim ay \Longrightarrow p = pax \Longrightarrow p(1 - ax) = 0$ with $ax - 1 \neq 0$, since otherwise it would result $a \,|\, 1$. □

2. 2. 9 Lemma. *If p is semiprime and $a \,\|\, p$ then a is cancellable.*

PROOF. $a \,\|\, p \Longrightarrow p = pax$. Suppose now $ad = 0$. It follows $p \sim ap = a(p + d) \rightsquigarrow p \,\Big|\, p + d \rightsquigarrow p \,|\, d$, say $d = py$. Hence it results $d = py = axpy = axd = 0$. □

In other words: p is semiprime iff the proper divisors of p form a cancellative monoid, p is irreducible iff the proper divisors of p form even a group.

2. 2. 10 Corollary. *In a finite $\mathfrak{R}$ each semiprime p is irreducible.*

2. 2. 11 Lemma. *If p and q are prime then*

$$p \,|\, q \vee q \,|\, p \vee \left(d \,\Big|\, p, q \Longrightarrow d \,|\, 1\right)\,.$$

PROOF. Suppose $p \nmid q$ & $q \nmid p$ and $d \,\Big|\, p, q$. Then $d \parallel p, q$ which leads to

$$\begin{aligned} p = pdx &\implies p(1-dx) = 0 \;\; (\exists x \in R) \\ &\implies q \mid 1 - dx \\ &\implies qy + dx = 1 \\ &\implies d \mid 1\,. \end{aligned}$$

□

(2.4) $$1 \parallel a \parallel p \;\&\; p \textit{ completely prime} \implies p^2 \,\Big|\, p\,.$$

PROOF.
$$\begin{aligned} p^2 \nmid p \;\&\; a \mid p &\implies p = pax \;\; (\exists x) \\ &\implies p \mid p(1-ax) = 0 \\ &\implies p \mid 1 - ax \\ &\implies py + ax = 1 \;\; (\exists y \in R) \\ &\implies a \mid 1\,. \end{aligned}$$

Thus the assertion follows by contraposition. □

2. 2. 12 Definition. Let $\mathfrak{M}$ be a commutative monoid. We call t^* *a complement* of t (in a) if t^* satisfies $\overline{t} \cdot \overline{t^*} = \overline{a}$ and $\overline{t} \cdot \overline{t^*} = \overline{t} \cdot \overline{x} \Longrightarrow \overline{t^*} \mid \overline{x}$ $(\Longleftrightarrow t^* \mid x)$.

2. 2. 13 Lemma. *If t^* is a complement of t it follows*

$$t \cdot t^* \mid t \cdot x \implies t^* \mid x\,.$$

PROOF.
$$\begin{aligned} t \cdot t^* \mid t \cdot x &\implies t \cdot t^* y = t \cdot x \\ &\implies t \cdot (t^* y - x + t^*) = t \cdot t^* \\ &\implies t^* \mid (t^* y - x + t^*) \\ &\implies t^* \mid x\,. \end{aligned}$$

□

2. 2. 14 Definition. We call $\mathfrak{R}$ *semi-factorial,* if each $\overline{a}$ is a product of semiprimes in such a way that *irredundant* decompositions of the same element have the same set of factors.

2. 2. 15 Lemma. *In a semi-factorial $\mathfrak{R}$ semiprime elements p are prime.*

PROOF. Put $\overline{p} \preceq \overline{a}$ iff $\overline{p}$ *is factor of at least one and thereby of each irredundant semiprime decomposition of* $\overline{a}$.

It is to prove $p \mid ab \Longrightarrow p \mid a \vee p \mid b$ or equivalently $\overline{p} \mid \overline{a}\overline{b} \Longrightarrow \overline{p} \mid \overline{a} \vee \overline{p} \mid \overline{b}$.

(i) In case of $\overline{p} \preceq \overline{ab}$ the proof is clear.

(ii) Otherwise we get $\overline{p} \not\preceq \overline{ab} \rightsquigarrow \overline{p} \cdot \overline{ab} = \overline{ab} \rightsquigarrow \overline{a} \cdot \overline{p} \leq \overline{a} \cdot \overline{b}$ and (w. l. o. g.) $\overline{p} \not\leq \overline{a}$.

But this means $\overline{a} < \overline{ap}$ and thereby $\overline{p} \preceq \overline{x}$ for all $\overline{x}$ with $\overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{p}$. Hence $\overline{p}$ is the (uniquely determined) complement of $\overline{a}$ and consequently a divisor of $\overline{b}$. □

2.2.15 provides as a first main result

2. 2. 16 Corollary. *A ring $\mathfrak{R}$ is semi-factorial iff each $\overline{a}$ is a product of primes.*

2. 2. 17 Lemma. *Let $\mathfrak{R}$ be a ring in which any $\overline{a}$ is a product of primes. Then each prime element is even completely prime.*

PROOF. First assume $p^{m+1} \nmid p^m$. Then $\overline{p}$ is the complement of $\overline{p}^{\,m}$, because with a suitable a it holds:

$$\begin{aligned} p^m p \,|\, p^m x &\implies p^m(pa - x + p) = p^m p \\ &\implies (\ )\,|\,p \vee p\,|\,(\ ) \\ &\implies p\,|\,(pa - x + p) \\ &\implies p\,|\,x\,. \end{aligned}$$

Suppose now $\qquad \overline{p}^{\,n} \leq \overline{a}\overline{b} \quad \& \quad \overline{p}^{\,n} \not\leq \overline{a}\,.$

Then it follows $\overline{p}^{\,m} \cdot \overline{x} = \overline{a}$ with $\overline{p} \not\leq \overline{x}$ and $0 \leq m < n$, and this provides

$$\begin{array}{rcl} \overline{p}^{\,m} \cdot \overline{p} & \leq & \overline{p}^{\,m} \cdot \overline{x} \cdot \overline{b} \\ & \rightsquigarrow & \\ \overline{p} & \leq & \overline{x} \cdot \overline{b} \\ & \rightsquigarrow & \\ \overline{p} & \leq & \overline{b} \qquad (\text{recall } \overline{p} \not\leq \overline{x})\,. \end{array}$$ □

Summarizing we get:

2. 2. 18 Proposition. *For a (commutative) ring (with identity) the following are pairwise equivalent:*

(i) *$\overline{\mathfrak{R}}$ is semi-factorial.*

(ii) *Each $\overline{a}$ of $\overline{\mathfrak{R}}$ is a product of primes.*

(*iii*) *Each* $\overline{a}$ *of* $\overline{\mathfrak{R}}$ *is a product of completely primes.*

We investigate factorial rings w. r. t. their arithmetics.

2. 2. 19 Lemma. *In a factorial ring any prime element p satisfies:*

$$\overline{a} \leq \overline{b} \iff \overline{p}^{\,e} \leq \overline{a} \Rightarrow \overline{p}^{\,e} \leq \overline{b}.$$

PROOF. ($\Longleftarrow$) : Let $\overline{a} = \prod\limits_{1}^{s} \overline{p}^{\,n_\sigma}$ be an irredundant prime-factor-decomposition satisfying $\sigma' \neq \sigma'' \Longrightarrow \overline{p}_{\sigma'} \not\leq \overline{p}_{\sigma''}$. Then the right side provides elements x_σ $(1 \leq \sigma \leq s)$ with

$$\begin{aligned} \overline{b} = \overline{p}_1^{\,n_1} \cdot \overline{x}_1 &= \overline{p}_1^{\,n_1} \cdot \overline{p}^{\,n_2} \cdot \overline{x}_2 \ldots \qquad (2.2.17) \\ &\leadsto \\ \overline{b} &= \overline{a} \cdot \overline{x}_\sigma \,. \end{aligned}$$

The other direction is obvious. □

2. 2. 20 Lemma. *Factorial rings satisfy the ascending chain condition, briefly ACC, for principal ideals.*

PROOF. We prove the descending chain condition w.r.t. $\|$. To this end we start from a chain $\overline{a} > \overline{a}_1 > \ldots > \overline{a}_n > \ldots$ and the uniquely determined irredundant decomposition $\overline{a} = \prod_1^s \overline{p}^{\,n_\sigma}$ with incomparable factors $\overline{p}_\sigma$ in $\overline{\mathfrak{R}}$. There may be reducible factors in this product, but these are idempotent and their proper divisors are cancellable and hence irreducible. Therefore after finitely many steps we arrive at an element $\overline{a}_m$ whose irredundant prime-factor-decomposition contains no longer any reducible factor. □

2.2.20 and 2.2.7 provide as a further main result

2. 2. 21 Lemma. *Any semi-factorial ring* $\mathfrak{R}$ *is even factorial.*

2. 2. 22 Lemma. *Factorial rings satisfy* $a \sim b \Longrightarrow a \equiv b$.

PROOF. There is nothing to show for prime elements p, q with $p \sim q$ since in the case of $p^2 \mathrel{+} p$ all proper divisors of p and q, respectively, are units.

Let now p^e and q^f be prime factor powers satisfying $p^e \sim q^f$. Then it follows $q = p\varepsilon$ with $\varepsilon \,|\, 1$ and we get immediately $p^e \equiv p^f$, if $e = f$, and w. l. o. g. $p^e \equiv p^f$ if $e < f$, since in this case we have $(p^e)^2 \,|\, p^e$.

Thus, since primes are completely prime, the proof is complete by lemma 2.2.21 □

We finish this section by a result that sheds some further light on the structure of factorial rings. It is easily seen that in factorial rings for each pair of principal ideal $\langle a\rangle, \langle b\rangle$ there exists a uniquely determined $\langle c\rangle$ with $\langle c\rangle = \{x \,\big|\, b \mid ax\} := \langle b\rangle : \langle a\rangle$. We show w.r.t. rings of this type:

2. 2. 23 Proposition. *Let $\mathfrak{R}$ be a commutative ring whose ideal quotients $\langle b\rangle : \langle a\rangle$ are principal. Then $\mathfrak{R}$ satisfies in addition:*

$$\text{(N)} \qquad \langle b\rangle : \langle a\rangle + \langle b\rangle : \langle a\rangle \;=\; \langle 1\rangle$$

PROOF. It holds the special implication:

$$\begin{aligned} \langle b\rangle : \langle a\rangle = \langle c\rangle \quad \& \quad & aef = a \;\&\; cef = c \\ \Longrightarrow\;& b \mid a(ef - 1 + c) \\ \Longrightarrow\;& e \mid c \,\Big|\, (ef - 1 + c) \Longrightarrow e \mid 1\,, \end{aligned}$$

which in particular leads to (N). □

Property (N) plays an important role in commutative ring theory, since it is characteristic for rings satisfying.

$$\text{(FD)} \qquad \langle a_1, a_2, ..., a_n\rangle \supseteq b \Longrightarrow \langle a_1, a_2, ..., a_n\rangle \,\Big|\, b\,.$$

More precisely it holds: A commutative ring with identity is called arithmetical iff its ideal lattice is distributive, and this is the case iff it satisfies (N) iff it satisfies (FD).

2.3 A direct Ring Decomposition

The goal of this section is a direct decomposition of factorial rings. Essential for this decomposition will be the divisibility arithmetic, in particular the existence of GCDs and LCMs.

It has already been shown that each pair of primes has a GCD. Next we show that $\overline{R}$ forms a lattice under $\wedge$ and $\vee$.

2. 3. 1 Proposition. *In factorial rings any pair a, b has both, a* LCM *and a* GCD .

PROOF. Choose $a, b \in R$, decompose $\overline{a}, \overline{b}$ in $\overline{R}$ and form prime factor powers. If then

$$\overline{a} = \prod \overline{p}\,_\sigma^{m_\sigma} \quad \text{and} \quad \overline{b} = \prod \overline{q}\,_\tau^{n_\tau}$$

are the uniquely determined irredundant decompositions of $\overline{a}$ and of $\overline{b}$, respectively, then the product of the maximal elements of

$$\{\overline{p}\,_1^{m_1}, \ldots, \overline{p}\,_s^{m_s}, \overline{q}\,_1^{n_1}, \ldots, \overline{q}\,_t^{n_t}\}$$

is the LCM of $\overline{a}, \overline{b}$ in $\overline{R}$ and each preimage of this LCM is a LCM of a, b in the ring $\mathfrak{R}$.

Now we construct the GCD of $\overline{a}, \overline{b}$ in $\overline{\mathfrak{R}}$ as follows: According to 2.2.11 for each pair of primes $\overline{p}, \overline{q}$ there exists the GCD $\overline{p} \wedge \overline{q}$. Hence in the case of $\overline{p} \not\leq \overline{q}$ & $\overline{q} \not\leq \overline{p}$ we get

$$\overline{p}\,^m \wedge \overline{q}\,^n = \overline{p} \wedge \overline{q} \qquad (\text{observe } \overline{a} < \overline{p} \Longrightarrow \overline{ap} = \overline{p})$$

and thereby

$$\text{LCM}\ (\overline{p}\,_\sigma^{m_\sigma} \wedge \overline{q}\,_\tau^{n_\tau})\ \binom{1 \leq \sigma \leq s}{1 \leq \tau \leq t} \ = \ \text{GCD}\,(\overline{a}, \overline{b}) =: \overline{a} \wedge \overline{b}\,.$$

Hence each *preimage* of $\overline{a} \wedge \overline{b}$ is a GCD of a and b in $\mathfrak{R}$. □

2. 3. 2 Definition. A ring $\mathfrak{R}$ is called a *special primary ring* if it contains a prime element $p \in R$ such that the set of all ideals of $\mathfrak{R}$ is exhausted by the set of all $\langle p^k \rangle$.

Now we are ready to prove:

2. 3. 3 The Decomposition Theorem. *A ring $\mathfrak{R}$ is factorial iff it is a finite inner direct sum whose summands are factorial domains or special primary rings.*

PROOF. Let $\overline{0} = \prod \overline{p}\,_\sigma^{n_\sigma}$ be the irredundant prime decomposition of $\overline{0}$. We may assume that $0 = \prod p_{\,\sigma} n_\sigma \quad (1 \leq \sigma \leq s)$ with $p\,_\sigma^{n_\sigma} \cdot p_\sigma = p\,_\sigma^{n_\sigma}$ $(1 \leq \sigma \leq s)$, since it holds

$$p\,_\sigma^{n_\sigma} \cdot p_\sigma \,\Big|\, p\,_\sigma^{n_\sigma} \ \rightsquigarrow \ p\,_\sigma^{n_\sigma}(p_{\,\sigma}\varepsilon) = p\,_\sigma^{n_\sigma}$$
$$\rightsquigarrow \ (p_\sigma\varepsilon)^{\,n_\sigma} \cdot (p_\sigma\varepsilon) = (p_\sigma\varepsilon)^{n_\sigma}\,,$$

whence all we have to do, is to replace p_σ by $p_\sigma\varepsilon$, if necessary. We define

$$e'_\sigma \ := \ \prod p\,_\sigma^{n_\sigma} \quad (\sigma \neq \sigma')\,.$$

Then $e_1 + \ldots + e_n$ is an *orthogonal sum,* that is $e_i^2 = e_i$, $e_i \cdot e_j = 0 \;\; (i \neq j)$, and
$$1 \;=\; e_1 + \ldots + e_n\,.$$
To see this, observe, that $e_1 + \ldots + e_s$ is idempotent and that in addition each prime divisor p of $e_1 + \ldots + e_s$ divides some p_σ and thereby each $e_{\sigma'}$ and consequently e_σ as well. But this means that p divides at least two different and thereby *relatively prime* elements $p_\sigma, p_{\sigma'}$, that is elements whose common divisors are units. Hence p itself must be a unit, too. Consequently $\mathfrak{R}$ is a finite inner direct sum of the ideals Re_σ , i. e.:

$$\mathfrak{R} \;=\; \mathfrak{R}e_1 \oplus \ldots \oplus \mathfrak{R}e_s\,.$$

It remains to show that each $\mathfrak{R}e_\sigma$ is a domain or a special primary ring. To this end we consider the cases $p_\sigma = p_\sigma^{\,2}$ and $p_\sigma \neq p_\sigma^{\,2}$.

(i) Suppose $p_\sigma = p_\sigma^{\,2}$ and $ae_\sigma \cdot be_\sigma = 0$. Then $p_\sigma \mid ab$ whence $p_\sigma \mid a \vee p_\sigma \mid b$ and thereby $ae_\sigma = 0 \vee be_\sigma = 0$.

(ii) Suppose $p_\sigma \neq p_\sigma^{\,2}$. Then each proper divisor of p_σ is a unit, and all elements of Re_σ are of type be_σ with $b \sim p_\sigma^t \;\; (\exists\, t \in \mathbf{N})$.

OBSERVE: From $p := p_\sigma,\;\; n := n_\sigma,\;\; e := e_\sigma$ in the case of $p \nmid a$ the irreducibility of p implies

$$\begin{array}{rcl}
\overline{a} \leq \overline{0} & = & \overline{p}^{\,n} \cdot \overline{e} \\
& \leadsto & \\
\overline{a} & = & \overline{a} \wedge \overline{p}^{n} \cdot \overline{e} \\
& \leq & (\overline{a} \wedge \overline{p}^{n}) \cdot (\overline{a} \wedge \overline{e}) \\
& = & \overline{a} \wedge \overline{e} \\
& \leadsto & \\
\overline{ae} & \leq & \overline{ee} = \overline{e} \\
& \leadsto & ae \equiv e\,.
\end{array}$$

Thereby in the case of $p^m \mid ae \;\&\; p^{m+1} \nmid ae \;\; (\exists 1 \leq m \in \mathbf{N})$ we get:

$$ae = p^m e \cdot x \;\&\; p \nmid x \leadsto xe \equiv e\,. \qquad \square$$

We now turn to the interaction of $\mathfrak{R}$ and $\mathfrak{R}\,[x]$.

2. 3. 4 Theorem. *$\mathfrak{R}\,[x]$ is factorial iff $\mathfrak{R}$ is a factorial ring satisfying the implication $a^2 = 0 \neq a \Longrightarrow a = 0$.*

PROOF. (a) Let $\mathfrak{R}$ be a factorial ring satisfying the implication above. Then $\mathfrak{R}$ is a direct product of factorial domains and the factorial property is transferred from $\mathfrak{R}$ to $\mathfrak{R}\,[x]$ according the classical result of Gauss.

(b) Let now $\mathfrak{R}\,[x]$ be factorial. Then $\mathfrak{R}\,[x]$ satisfies the ascending chain condition for principal ideals and each $a \in R$ has a decomposition $a = p_i \cdot \ldots \cdot p_\sigma$ into semiprime factors $p_\sigma \;\; (1 \le \sigma \le s) \in \mathfrak{R}\,[x]$. Recall now:

$$\begin{aligned} a \;\;|_{\mathfrak{R}\,[x]}\;\; b &\implies a \;\;|_R\;\; b \\ \text{and} \qquad a \;\;\sim_{\mathfrak{R}\,[x]}\;\; b &\implies a \equiv_R \;\; b\,, \end{aligned}$$

where the second line follows from

$$a_0 + a_1 x + \cdots + a_n x^n \,\Big|\, 1 \implies a_0 \,\Big|\, 1\,.$$

This means that semiprime elements p of $\mathfrak{R}$ with prime decomposition $p = \prod p_i(x)$ in $\mathfrak{R}\,[x]$ satisfy

$$p = \prod p_i(x) \;\leadsto\; p \sim p_{j_0} \quad (\exists j \in I)$$

and thereby

$$\begin{aligned} p \,|\, ab &\implies p_j(x) \,|\, a \vee p_j(x) \,|\, b \\ &\implies p_{j_0} \,|\, a \vee p_{j_0} \,|\, b \\ &\implies p \,|\, a \vee p \,|\, b\,. \end{aligned}$$

Hence each semiprime element of $\mathfrak{R}$ is prime in $\mathfrak{R}$. But semiprimes of $\mathfrak{R}$ are not only prime in $\mathfrak{R}$ but even prime in $\mathfrak{R}\,[x]$.

To this end suppose that there are first coefficients a_k in $f(x)$ and b_ℓ in $g(x)$ satisfying $p \,|\, a_k,\; p \nmid b_\ell$. This would imply $p \,|\, a_k \cdot b_\ell$ in contradiction to $p \,|\, a_i b_j \;\; (1 \le i, j \le n)$.

Hence irredundant prime factorizations of 0 in $\mathfrak{R}$ remain irredundant prime factorizations of 0 in $\mathfrak{R}\,[x]$.

Suppose now $a^2 = 0 \neq a$. Then there would be a triple $p,\, n,\, e := p_\sigma,\, n_\sigma,\, e_\sigma$ satisfying $p^2 \nmid p \leadsto a \,|\, p \Longrightarrow a \,|\, 1$.

Hence each prime factor of ex in $\mathfrak{R}e\,[x]$ must be cancellable since ex is cancellable in $\mathfrak{R}e\,[x]$, and in addition it must be a divisor of pe, and even a proper divisor of pe, according to $(pe)^n = 0$.

But this would yield $xe \,|\, e \;\rightsquigarrow\; x|_R\, e$, a contradiction! □

2. 3. 5 Corollary. *A finite ring is factorial iff it is a principal d-ideal ring.*

PROOF. In the finite case each integral component of the decomposition theorem is a field. Hence the decomposition theorem provides a direct product of principal ideal rings. □

There are two natural questions, which now will be considered.

First we ask: when is a factorial ring is a direct product even of fields. The answer is trivial, of course. This is the case iff any $a \in R$ satisfies $a^2 \,|\, a$, i. e. if R is *von Neumann regular.*

In this case $\mathfrak{R}\,[x]$ is a direct product of the principal ideal rings $\mathfrak{R}{\cdot}e_{\sigma_i}\,[x]$ components and hence a multiplication ring, that is a ring satisfying condition (M) of the introduction.

So, it should be mentioned that D. D. Anderson in [3] has shown, that condition (M) for $\mathfrak{R}\,[x]$ is not only necessary, in order that $\mathfrak{R}$ be a direct product of fields, but also sufficient. This will now be proven alternatively to [3]

2. 3. 6 Proposition. *Let* $\mathfrak{R}$ *be a commutative ring with identity* 1. *Then* $\mathfrak{R}\,[x]$ *is a multiplication ring if and only if* $\mathfrak{R}$ *is a direct product of fields.*

PROOF. One direction is clear.

Let now $\mathfrak{R}\,[x]$ be a multiplication ring. Then the lattice of ideals of $\mathfrak{R}\,[x]$ satisfies:

$$\begin{aligned} \mathfrak{a} \cap (\mathfrak{b}+\mathfrak{c}) &= (\mathfrak{a} : (\mathfrak{b}+\mathfrak{c})\,) \cdot (\mathfrak{b}+\mathfrak{c}) \\ &= (\mathfrak{a} : (\mathfrak{b}+\mathfrak{c})\,) \cdot \mathfrak{b} + (\mathfrak{a} : (\mathfrak{b}+\mathfrak{c})\,) \cdot \mathfrak{c} \\ &\subseteq (\mathfrak{a} : \mathfrak{b})\,) \cdot \mathfrak{b} + (\mathfrak{a} : \mathfrak{b})\,) \cdot \mathfrak{c} \\ &= (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c}) \\ &\subseteq \mathfrak{a} \cap (\mathfrak{b}+\mathfrak{c}). \end{aligned}$$

This implies that $\mathfrak{R}$ is (von Neumann) regular, since every $a \in R$ satisfies

$$\langle a \rangle \supseteq \langle x-a \rangle + \langle x \rangle \implies (\langle a \rangle \cap \langle x-a \rangle) + (\langle a \rangle \cap \langle x \rangle\,,$$

which implies
$$\begin{aligned} a &= (x-a)\cdot f(x) + x\cdot g(x) \\ &\quad \text{with } a \mid x\cdot g(x) \rightsquigarrow a \mid g(x) \\ &\rightsquigarrow a \mid (x-a)\cdot f(x) \\ &\rightsquigarrow a \mid xf(x) \rightsquigarrow a \mid f(x) \\ &\rightsquigarrow a^2 \mid af(x) = x(\,f(x)+g(x)\,) - a \\ &\rightsquigarrow a^2 \mid a\,. \end{aligned}$$

Thus the principal ideals form a boolean algebra.

We now show that $\mathfrak{R}$ has the Noether property. From this it will follow that $\mathfrak{R}$ is indeed a direct product of fields. To this end let $A = \langle a_i\rangle$ $(a_i^2 = a_i)$ be an ideal of $\mathfrak{R}$ and suppose

$$\langle A, x\rangle \cdot B = \langle x\rangle$$

in $\mathfrak{R}[x]$. Then there exists an element $a = a^2 \in A$ with

$$\begin{aligned} \langle a, x\rangle \cdot B &= \langle x\rangle \\ &= \langle A, x\rangle \cdot B\,, \end{aligned}$$

and by $B \mid \langle x\rangle$, B is cancellable if $\langle x\rangle$ is cancellable. But this means

$$\langle a, x\rangle = \langle A, x\rangle.$$

that is for each $a_i \in A$

$$\begin{aligned} a_i &= a\cdot u(x) + x\cdot v(x) \\ &\qquad\qquad (\exists : u(x), v(x) \in R(x) \\ &= a\cdot s_i \qquad\qquad (\exists s_i \in R)\,. \end{aligned}$$

This completes the proof. □

2.4 Ideal theoretical Aspects

2. 4. 1 Lemma. *Factorial rings satisfy*

(D) $$\overline{a}\cdot(\overline{b}\wedge\overline{c}) = \overline{a}\cdot\overline{b}\wedge\overline{a}\cdot\overline{c}\,.$$

PROOF. Obviously we get

$$\overline{a} \cdot (\overline{b} \wedge \overline{c}) \;\leq\; \overline{a} \cdot \overline{b} \wedge \overline{a} \cdot \overline{c}\,.$$

It remains to show $\quad \overline{a} \cdot \overline{b} \wedge \overline{a} \cdot \overline{c} \;\leq\; \overline{a} \cdot (\overline{b} \wedge \overline{c})\,.$

To this end let p be prime, $\overline{p}^{\,n} \mid \overline{ab}, \overline{ac}$ and $\overline{p}^{\,m} \mid \overline{a}$ & $\overline{p}^{\,m+1} \nmid \overline{a}$. Then it follows $\overline{p}^{\,n-m} \mid \overline{b}, \overline{c}$ and thereby $\overline{p}^{\,n} \mid \overline{a} \cdot (\overline{b} \wedge \overline{c})$, whence $\overline{a} \cdot \overline{b} \wedge \overline{a} \cdot \overline{c} \leq \overline{a} \cdot (\overline{b} \wedge \overline{c})$. □

2. 4. 2 Definition. By a GCD-*ring* we mean a ring with GCDs satisfying condition (D).

In particular every factorial $\mathfrak{R}$ is a GCD-ring.

2. 4. 3 Lemma. *GCD-rings satisfy*

$$\overline{a} \,|\, \overline{b} \cdot \overline{c} \;\&\; \overline{a} \wedge \overline{b} = \overline{1} \;\;\Rightarrow\;\; \overline{a} \leq \overline{c}\,.$$

PROOF. $\quad \overline{a} = \overline{a} \wedge \overline{b} \cdot \overline{c} \;\leq\; (\overline{a} \wedge \overline{b}) \cdot (\overline{a} \wedge \overline{c}) = \overline{a} \wedge \overline{c}\,.$ □

2. 4. 4 Lemma. *In GCD-rings every semiprime p is completely prime.*

PROOF. Let $\overline{p}$ be semiprime and suppose $\overline{p} \leq \overline{a} \cdot \overline{b}$. It follows:

$$\overline{p} = \overline{p} \wedge \overline{a} \cdot \overline{b} \;\leq\; (\overline{p} \wedge \overline{a}) \cdot (\overline{p} \wedge \overline{b})\,.$$

From this we get $\overline{p} = \overline{p} \wedge \overline{a} \vee \overline{p} = \overline{p} \wedge \overline{b}$, since otherwise $\overline{p} \leq (\overline{p} \wedge \overline{a}) \cdot (\overline{p} \wedge \overline{b}) < \overline{p}$ must be satisfied. So we have $\overline{p} \leq \overline{a} \vee \overline{p} \leq \overline{b}$. Consider some $\overline{p}^{\,n}$ satisfying

$$\overline{p}^{\,n} \leq \overline{a} \cdot \overline{b} \quad \& \quad \overline{p} \not\leq \overline{a}\,.$$

Then $\overline{p} \leq \overline{b}$ whence

$$\begin{aligned} \overline{p}^{\,n} &= \overline{p}^{\,n} \wedge \overline{a} \cdot \overline{b} \\ &\leq (\overline{p}^{\,n} \wedge \overline{a}^{\,n}) \cdot (\overline{p}^{\,n} \wedge \overline{b}) \\ &\leq (\overline{p} \wedge \overline{a})^n \cdot (\overline{p}^{\,n} \wedge \overline{b}) \\ &= \overline{p}^{\,n} \wedge \overline{b}\,. \end{aligned}$$

□

Suppose now that $\mathfrak{R}$ is even a *principal ideal ring.* Then g is GCD of a and b iff $\langle b, c\rangle = \langle g\rangle$, and and it holds the equation

$$\langle a\rangle \cdot \langle b, c\rangle \;=\; \langle ab, ac\rangle\,.$$

Hence (D) is satisfied for the classes $\overline{x}$.

In addition $\mathfrak{R}$ satisfies ACC for principal ideals because

$$\begin{array}{rcl} \langle a_1\rangle \subset \langle a_2\rangle \subset \langle a_3\rangle \subset \ldots & \& & \langle\{a_i\}\rangle = \langle c\rangle \\ & \Longrightarrow & \\ c\,\Big|\, a_i\ \ (i \in \mathbf{N}) & \& & c \in \langle a_1, \ldots, a_\ell\rangle = \langle a_\ell\rangle\ \ (\exists\, a_\ell) \\ & \leadsto & \\ \langle a_\ell\rangle & = & \langle a_{\ell+1}\rangle \cdots . \end{array}$$

Hence any principal ideal ring is factorial. But, of course, the opposite is not true. Consider $\mathbf{Z}[x,y]$. By GAUSS $\mathbf{Z}[x,y]$ is factorial but 1 has no linear combination by x, y. So we have to look for a weakened condition.

Apart from the usual *Dedekindian ideal,* for short d-ideal, there exist further most important ideals.

2. 4. 5 Definition. Let $\mathfrak{S}$ be a commutative monoid. A subset $\mathfrak{a}$ of S is called a *v-ideal* if it satisfies – compare the preface –

$$\left(s\,\Big|\,\mathfrak{a}\cdot t \Rightarrow s\,\Big|\,c\cdot t\right) \implies c \in \mathfrak{a}\,.$$

Obviously, in a ring the zero element 0 is contained in every v-ideal. Therefore no intersection of a family of v-ideals is empty. Furthermore it is easily seen that the intersection of a family of v-ideals is always again a v-ideal. Consequently for each $A \subseteq R$ there exists a finest A containing v-ideal A_v, *generated* by A. For these ideal types we get:

$$A_v = B_v \;\&\; C_v = D_v \implies \langle AC\rangle_v = \langle BD\rangle_v\,,$$

because by assumption

$$s\,\Big|\,(AC)t \iff s\,\Big|\,(AD)t \iff s\,\Big|\,(BD)t\,.$$

So v-ideals may be calculated in a similar manner as d-ideals are calculated. Based on v-ideals we now define

2. 4. 6 Definition. A subset $\mathfrak{a}$ of S is called a *t-ideal* if it contains all v-ideals generated by finite subsets of $\mathfrak{a}$.

The calculation laws for t-ideals are the same as those for v-ideals, as is pointed out in the next chapter. In particular each subset A of S generates uniquely a finest t-ideal A_t by taking all $(A_i)_t$ with finite $A_i \subseteq A$. And forming their set theoretical union, we get

$$A_t = B_t \;\&\; C_t = D_t \implies \langle AC\rangle_t = \langle BD\rangle_t \,,$$

which is left to the reader at this point, since t-ideals are not multiplied in this section.

But, different from v-ideals, t-ideals are of *finite character,* meaning that an element contained in A_t is already contained in some E_t where E is a finite subset of A.

Obviously v- and t-ideals satisfy $a_v = a_t = \langle a\rangle = aS$. Hence any *principal v-ideal ring* and similarly any principal t-ideal ring is a GCD -ring. And, like d-ideals, v-ideals and also t-ideals satisfy

$$(\mathrm{D}^t) \qquad \langle a\rangle_t \cdot \langle b, c\rangle_t \;=\; \langle ab, ac\rangle_t \,,$$

that is the classes $\overline{x}$ satisfy condition (D). This leads to

2. 4. 7 The Characterization Theorem. *A ring $\mathfrak{R}$ is factorial iff it is a principal t-ideal ring.*

PROOF. (a) Let $\mathfrak{R}$ be factorial. Then according to ACC for principal ideals each A_t of $\mathfrak{R}$ contains some a having no proper divisor in A_t. But this a satisfies $\langle a, c\rangle_t = \langle d\rangle_t = \langle a\rangle_t \leadsto a \,|\, c \ (c \in A_t)$, observe $\langle d\rangle_t = \langle a, c\rangle_t \Longrightarrow d \in A_t \;\&\; d \,|\, a \Longrightarrow d \sim a$.

(b) Let now $\mathfrak{R}$ be a principal t-ideal ring. Then $\mathfrak{R}$ is a GCD-ring, recall condition (D), and like above we get ACC for principal ideals.

Consequently $\mathfrak{R}$ is factorial. □

Based on the preceding results We finish this section by a new proof of corollary 2.3.5.

2. 4. 8 Proposition. *A finite commutative ring with identity* 1 *is factorial iff it is a principal d-ideal ring.*

PROOF. It suffices to verify necessity. To this end let $\mathfrak{R}$ be finite and factorial. We show

$$\overline{a} \wedge \overline{b} = \overline{c} \Longrightarrow \langle a, b\rangle = \langle c\rangle \,.$$

To this end we start from

$$\overline{a} \wedge \overline{b} = \overline{c} \quad \text{with} \quad \overline{a} = \overline{c} \cdot \overline{a'},\ \overline{b} = \overline{c} \cdot \overline{b'}\,.$$

Here we may assume that a', b' are *orthogonal*, or equivalently relatively prime.

FOR: By 2.2.10 we may start in $\overline{\mathfrak{R}}$ from irredundant decompositions of $\overline{a'}, \overline{b'}$ into irreducible factors, consult 2.2.10. Moreover, since any common $\overline{p}$ implies $\overline{cp} \mid \overline{c} \leadsto \overline{cp} = \overline{c}$ we may delete common factors successively until there remain orthogonal products.

If now $a' \mid 1$ or $b' \mid 1$, there exists *a fortiori* a linear combination

$$a'x + b'y \;=\; 1\,.$$

Otherwise there exists an n, satisfying

$$(a')^{n+1} \,\Big|\, (a')^n \leadsto (a')^n(a'u) = (a')^n \leadsto (a')^n(1 - a'u) = 0\,.$$

But a', b' are orthogonal. Hence $b' \mid (1 - a'u)$, say $b'v = 1 - a'u$, whence

$$b'v + a'u = 1 \leadsto ca'u + cb'v = au + bv = c\,,$$

that is $\langle a, b\rangle = \langle c\rangle$. So, by induction we get:

$$\langle a_1, \ldots, a_n\rangle \;=\; \langle d\rangle \;\; (\exists d \in R)\,. \qquad \square$$

A final Remark. Again, w.r.t. what is developed in the remainder of this paper, this chapter may serve as a *nucleus.* This will be clear in most situations, whence we omit additional comments and remarks. The interested reader is invited to verify step by step the introducing statement:

2.5 Towards abstract considerations

We finish this chapter by considering the concrete results from an abstract point of view.

Again, v- and t-ideals satisfy $a_v = a_t = \langle a\rangle = aS$. Hence any *principal v-ideal monoid with zero* and similarly any principal t-ideal monoid with zero is a GCD-monoid. And, like d-ideals, v-ideals and also t-ideals satisfy

$$(\mathrm{D}^t) \qquad \langle a\rangle_t \cdot \langle b, c\rangle_t \;=\; \langle ab, ac\rangle_t\,.$$

Henceforth ideal will always mean t-ideal. We denote principal ideals by lower case slanted letters, whereas lower case Gothic letters are taken to denote ideals in general.

2. 5. 1 Definition. $\mathfrak{S}$ is said to be ringlike if its ideals satisfy the implication

$$a \cdot \mathfrak{u} = a \Longrightarrow \exists \mathfrak{u}^* \bot \mathfrak{u} : a \cdot \mathfrak{u}^* = \mathfrak{o}\,.$$

Let henceforth $\mathfrak{S}$ be ringlike and $\mathfrak{A}$ be its ideal extension. Observe $\mathfrak{S}$ is isomorphic to the set of principal ideals, but moreover principal ideals admit an addition and constructing quotients within $\mathfrak{A}$. Therefore we will calculate with principal ideals instead of elements.

As a first fundamental result we get:

$$(2.10) \qquad \begin{aligned} b : a = c \quad \& \quad & a\mathfrak{u} = a \;\&\; c\mathfrak{u} = c \\ \Longrightarrow\;\; & b \supseteq a(\mathfrak{u}^* + c) \\ \Longrightarrow\;\; & \mathfrak{u} \supseteq c \supseteq (\mathfrak{u}^* + c) \\ \Longrightarrow\;\; & \mathfrak{u} \supseteq \mathfrak{u}^* \Rightarrow \mathfrak{u} = 1\,. \end{aligned}$$

This implies in any case

$$(2.11) \qquad u = u^2 \;\supseteq\; a^2 : a \neq 0 \Longrightarrow u = 1\,.$$

Assume now that $\mathfrak{S}$ is complementary. Then we get first:

$$(2.12) \qquad c \in \mathfrak{a} \Longleftrightarrow s \,|\, \mathfrak{a} \Longrightarrow s \,|\, c$$

by:
$$s \,|\, Av \Longrightarrow s : v \,|\, A \Longrightarrow (s : v) \,|\, c \Longrightarrow (s : v)v \,|\, cv \Longrightarrow s \,|\, cv$$

Furthermore we get for finite ideals

$$(2.13) \qquad \langle a_1, \ldots, a_n\rangle \supseteq \mathfrak{b} \;\Longleftrightarrow\; \langle a_1, \ldots, a_n\rangle \Big|\, \mathfrak{b}\,.$$

FOR, put $c := \bigvee_1^n (b : a_i)$. Then it follows:

$$\begin{aligned} d \,|\, b \;&\Longrightarrow\; d \,|\, \mathfrak{a} \cdot c \\ &\;\;\& \\ d \,|\, \mathfrak{a} \cdot c \;&\Longrightarrow\; c \leq b \vee d =: g \,|\, \mathfrak{a} \cdot c \\ &\Longrightarrow\; g : c \,|\, \mathfrak{a} \end{aligned}$$

$$\begin{aligned}
&\Longrightarrow\ g : c \,|\, b \\
&\Longrightarrow\ (g : c)x = b \\
&\Longrightarrow\ \mathfrak{a}x \geq b \\
&\Longrightarrow\ x \geq c \\
&\Longrightarrow\ (g : c)c \leq b \\
&\Longrightarrow\ g \,|\, b \\
&\Longrightarrow\ d \,|\, b,
\end{aligned}$$

that is $\mathfrak{a} \cdot c = b$, in other words $\mathfrak{A}$ is a Prüfer DV-IDM, satisfying in particular $(\mathrm{a} + b)(b : \mathrm{a}) = \mathrm{a}$. This leads next to

$$(a : b) : (b : a) = a : b\,, \tag{2.14}$$

$$(a : b + b : a)^2 = a : b + b : a \tag{2.15}$$

PROOF. (2.14) follows by
$$\begin{aligned}
a : b &= a : (a + b)(b : a) \\
&= (a : (a + b)) : (b : a) \\
&= (a : b) : (b : a)
\end{aligned}$$

Put now $\mathfrak{u} := a : b + b : a$. Then it results (2.15) by

$$\begin{aligned}
(a : b + b : a)^2 &= (a : b) \cdot \mathfrak{u} + (b : a) \cdot \mathfrak{u} \\
&= a : b + b : a\,.
\end{aligned}$$

This completes the prof. □

Let now $\mathfrak{S}$ be ringlike and complementary. Then $\mathfrak{S}$ is even normal (complementary), that is, then $\mathfrak{A}$ satisfies:

$$a : b + b : a = 1 \tag{2.16}$$

Let in the sequel $\mathfrak{S}$ be complementary. Then

2. 5. 2 Proposition. *The subsequent conditions are equivalent:*

(a) *Any a admits a decomposition $u \cdot v$ where u is idempotent and v is cancellable.*

(b) *$\mathfrak{S}$ is complementary and semiprime, that is satisfies the implication $\mathrm{a}^2 = 0 \Longrightarrow \mathrm{a} = 0$.*

PROOF. (a)$\Longrightarrow$(b). Assume that $a = uv$ where $u$is idempotent and v is cancellable. Then it follows

$$a^n = 0 \Longrightarrow (uv)^n = 0 \Longrightarrow uv^n = 0 \Longrightarrow slu = 0 \Longrightarrow a = 0\,,$$

whence $\mathfrak{A}$ is semiprime.

(b)$\Longrightarrow$(a) By assumption it results:

$$b \cdot c = 0 \Longrightarrow (bc)^2 = 0 = (c \vee b)^2 \Longrightarrow b \vee c = 0 = cb\,.$$

So, in case of $b \neq 0$ we get $0 : c =: v \neq 0$ and $1 \neq =: v =: u \leq c$ which by $0 : (0 : (0 : u)) = 0 : u = 0 : (0 : v)) = v$ leads to the implication

$$u + v = 0 : v + 0 : u = u \cap 0 : v* = 1$$
$$\textit{implies}$$
$$u \perp v \;\&\; u^2 \mid uv = 0 \Longrightarrow u = u^2 \leq c\,.$$

Consequently in case of $b \neq 0$ the element c must contain some proper idempotent divisor.

In particular $a^2 : a$ would contain some proper idempotent divisor, in case of $x \neq 0 \;\&\; x \cdot (a * a)^2 = 0$, which is impossible, as was shown above.

Hence $a^2 : a$ is cancellable. But

$$(a : (a^2 : a)))(a^2 : a)\cdot(a : (a^2 : a)(a^2 : a) = a^2 = (a^2 : a)(a : (a^2 : a))\cdot(a^2 : a)$$

whence $(a : (a^2 : a))^2 = (a : (a^2 : a))$, that is

$$a = (a : (a^2 : a)))(a^2 : a) =: u \cdot v$$

where u is idempotent and v is cancellable. $\square$

In the next proof we write slanted letters instead of roman letters, when ever we want to stress that we have the corresponding principal ideal in mind. Observe that $+$ always means the ideal addition.

So $a + b$ means $\langle a, b\rangle$ but it may happen that $a + b = \langle a \wedge b\rangle$.

2. 5. 3 Proposition. *For $\mathfrak{S}$, $\mathfrak{A}$ the subsequent conditions are equivalent:*

(a) *$\mathfrak{A}$ has the Noether property and any $\mathrm{a} : \mathrm{b}$ is principal.*

(b) *Any $a \in S$ is a product of completely prime elements of $\mathfrak{S}$.*

(c) *Any $\mathfrak{a}$ is principal.*

PROOF. (a)$\Longrightarrow$(b) By the Noether property any a has a decomposition into semiprime elements.

But $\mathfrak{S}$ is complementary, which entails for any semiprime element p the implication $p \supseteq ab \Longrightarrow (p : b) : a = 1$, whence p is prime, and furthermore

$p^n \supseteq ab \;\&\; p \not\supseteq a \Longrightarrow p^n \supseteq p^n + (a+p)^n b = p^n + b$, whence p is even completely prime.

(b)$\Longrightarrow$(c). First of all $p^k \supseteq a \;\&\; p^{k+1} \not\supseteq a \;\&\; p^{k+\ell} \supseteq b \Longrightarrow p^\ell \,|\, x$. Let now $b = \prod {p_i}^{n_i}$ be the unique irredundant prime factor decomposition of b. Then we take for each i the exponent ℓ_i in the above sense and get $b : a = \prod {p_i}^{\ell_i}$. That is $\mathfrak{S}$ is complementary. Next by (2.16) it holds $a : (a : b) \vee b : (b : a) = a + b$. This follows since

$$a + b \subseteq a : (a : b) \vee b : (b : a)$$

is evident and since $b : (b : (b : a)) = b : a$ entails

$$\begin{aligned}(a+b) : \Big(a : (a : b) \vee b : (b : a)\Big) &\supseteq \Big(a : (a : (a : b))\Big) + \Big(b : (b : (b : a))\Big) \\ &= a : b + b : a = 1\end{aligned}$$

that is $$a + b \supseteq (a : (a : b) \vee b : (b : a)$$

and thereby $a + b = \langle a, b\rangle$. But $(a : (a : b) \vee b : (b : a)$ is principally generated $a \wedge b$. Hence we may write $a + b = a \wedge b$.

Let now $0 = p_1^{n_1} \cdot \ldots \cdot {p_i}^{n_i} \cdot \ldots \cdot {p_k}^{n_k}$ be the decomposition of 0. Then we may assume that no p_i divides any $p_j \neq p_i$, and that $1 \neq a \supset p_i \neq {p_i}^2$ implies $a = 1$, since $p^2 = p \cdot (pa + a^*) \Longrightarrow p \supseteq (pa + a^*) \Longrightarrow a \supseteq p \supseteq pa + a* \Longrightarrow 1 \neq a \supseteq a^*$, a contradiction.

Furthermore it holds $au = a \supset p \Longrightarrow au^* = 0 \Longrightarrow u \supseteq p \supseteq u^* \Longrightarrow u = 1$ and thereby $ax = ay \supset p \Longrightarrow a(x+y)x' = a(x+y) \Longrightarrow x' = 1$ that is the cancellation law for the set of all $a \supset p$.

This finally leads to a direct decomposition of $\mathfrak{S}$ by the idempotent powers $u_i := e^{n_i}$ whose factors are factorial in any case and in addition primary or cancellative with zero 0. This entails the ascending chain condition for principal ideals and thereby the Noether property, recall the implication $\mathfrak{b} \subseteq \mathfrak{a} \;\&\; b \in \mathfrak{b} \;\&\; a \in \mathfrak{a} - \mathfrak{b} \Longrightarrow b \subset b \wedge a \in \mathfrak{a} - \mathfrak{b}$.

Thus it is shown by Noether that any $\mathfrak{a}$ is finitely based and it was shown above that any finitely generated ideal is a principal ideal.

Finitely (c)$\Longrightarrow$(a) follows by definition. □

All conditions of this note will be phrased in the language of algebraic multiplication lattices, that is a generalization of the t-ideal structure of monoids.

Chapter 3

Lattices

3.1 Some Remarks on Posets

3. 1. 1 Definition. $(M, \leq)$ is a *poset* (partially ordered set) if

(R) $$a \leq a \ (\forall a)$$

(S) $$a \leq b \leq a \implies a = b$$

(T) $$a \leq b \leq c \implies a \leq c\,.$$

$(M, \leq)$ is called a *totally ordered set*, equivalently a *chain*, if any two elements a, b are *comparable*, that is satisfy $a \leq b \vee b \leq a$.

Bounds, limits, intervals, maximal etc. are defined as usual.

Some examples:

$[a, b] := \{x \mid a \leq x \leq b\}$, $(a, b) := \{x \mid a < x < b\}$, $(a, b] := \{x \mid a < x \leq b\}$, $(a] := \{x \mid x < a\}$ and $S = \mathrm{Sup}(A) \ :\Longleftrightarrow \ (a \leq S \ (\forall a \in A))\ \&\ (a \leq b \ (\forall a \in A) \Longrightarrow S \leq b)$.

The theory of posets is fundamental and exciting, as well, and there is an abundance of interesting results. Here, however, we are interested merely in the most cited lemma of mathematics.

3. 1. 2 (ZL) Zorn's Lemma. *Let $\mathfrak{P}$ be a non empty poset whose chains are upper limited. Then $\mathfrak{P}$ contains at least one maximal element.*

Later we will verify the equivalence of **(ZL)** with

3. 1. 3 (AC) The Axiom of Choice. *Let* $\{A_i\}$ $(i \in I)$ *be a family of pairwise disjoint sets. Then there exists a set* A*, which contains exactly one element of each* A_i *.*

Precisely one would have to speak of ZORN's principle. In his paper [436] ZORN demonstrated that the maximum principle, telling that any system of sets which contains together with any chain also the union of the members of this chain, does contain at least one maximal set, leads in many situations of abstract mathematics to well known results proven before by the axiom of choice, see below.

As will be shown below **(ZL)** $\Longrightarrow$ **(AC)** is nearly obvious, whereas **(AC)** $\Longrightarrow$ **(ZL)** requires some mathematical power. So, in concrete situations, starting from **(ZL)** this power works implicitly and shortens the proof – sometimes extremely. As examples, left to the reader, we give the theorems that any linear space contains a basis, and that in any *ring with identity,* there exists at least one *maximal ideal* in the set of all ideals, not containing the identity element 1.

In the early days of set theory sometimes the obvious logical equivalent of **(ZL)**, due to HAUSDORFF/KURATOWSKI, is stressed, telling

3. 1. 4 (HK). *Any poset contains a maximal chain.*

But ZORN's lemma is nowadays the standard formulation.

We restrict ourselves to these few results here. In another lecture note the reader will find further equivalents.

The real fan, however, is referred to RUBIN/RUBIN [382]. Here more than two hundred equivalents distributed over nearly all fields of structure theory are presented.

As to the equivalent **(ZL)** $\Longleftrightarrow$ **(AC)** the implication **(ZL)** $\Longrightarrow$ **(AC)** is nearly obvious – consider the family of all sets containing at most one element of each A_i. So it remains to be verified

3. 1. 5 Theorem. **AC** $\Longrightarrow$ **ZL**.

PROOF. This proof is done indirectly along the lines of MARTIN KNESER, [235], as it is given by HERMES in [190].

We start from a *poset* $\mathfrak{H} = (H, \leq)$ without any maximal element, whose non empty chains K are limited, and whose $\mathrm{Sup}K$'s are denoted by $g(K)$.

Next we associate with each $x \in H$ the set $s(x) := \{y \mid y > x\}$, and we denote by M the set of all $S(x)$.

By **AC** the set M admits a function φ with $\varphi(S(x)) := f(x) \in S(x)$. In particular this means

$$x < f(x) .$$

Finally we choose and fix an element $a_0 \in H$.

On the basis of these ingredients we now act as follows:

Call ZORN-*set* any $Z \subseteq H$ that satisfies the subsequent three conditions (i) through (iii)

(i) $a_0 \in Z$

(ii) $x \in Z \Longrightarrow f(x) \in Z$

(iii) $\emptyset \neq K \subseteq H$ & K a chain $\Longrightarrow g(K) \in Z$.

Trivial ZORN-sets are H itself or $[a_0) := \{x \mid a_0 \leq x\}$. Furthermore the intersection Z_0 of all ZORN-sets is obviously again a ZORN-set.

Hence Z_0 is the smallest ZORN-set and each element of Z_0 lies above a_0, since $[a_0)$ contributes to the intersection.

We will show that Z_0 is even a chain. This will complete the proof since (Z_0) by (ii) would contain $f(g(Z_0)) > g(Z_0)$, a contradiction to the sup-property of $g(Z_0)$.

HENCEFORTH elements z will always be supposed to be an element of Z_0. An element $a \in Z_0$ will be called *distinguished* if $z < a \Longrightarrow f(z) \leq a$.

Evidently a_0 is distinguished since there exists no $z < a_0$.

Now we associate with each distinguished element a the set

$$B(a) := \{z \in Z_0 \mid z \leq a \vee f(a) \leq z\} \subseteq Z_0$$

and consider a (fixed) distinguished element a:

(a) By $a_0 \leq a$ we get $a_0 \in B(a)$.

(b) In case of $z \in B(a)$ it holds one of the following three cases:

$$(i) \quad z < a \ , \ (ii) \quad z = a \ , \ (iii) \quad f(a) \leq z .$$

In case (i) we conclude $f(z) \leq a$, since a is distinguished. In each of the other cases we infer immediately $f(a) \leq f(z)$. Hence in each of these cases it results $f(z) \in B(a)$.

(c) Let now K be a not empty chain of elements of $B(a)$.

Case 1. All elements of K lie below a. Then $g(K) \leq a$ lies below a, too, and thereby because $g(K) \in Z_0$ it holds also $g(K) \in B(a)$.

Case 2. There exists some $k \in K$ which does not lie below a. Then it results $f(a) \leq k \leq g(K)$, that is again $g(K) \in B(a)$.

Combining (a), (b), (c), we get that $B(a)$ is a Zorn-set, which leads to $Z_0 \subseteq B(a)$. This means in particular that any distinguished element a is comparable with any element of Z_0.

In a last step we now show that the set A of all distinguished elements forms a Zorn-set, leading to $Z_0 = B(a)$ and thereby to comparability of any pair a, b of distinguished elements.

(a) a_0 is distinguished, as was shown above.

(b) Let a be distinguished. Then $f(a)$ is distinguished again.

To this end we consider some $z < f(a)$. By our development above z belongs to $B(a) = Z_0$, whence $z \leq a$ or $f(a) \leq z$ is fulfilled. In the case under consideration this means $z \leq a$.

Assume first $z = a$. Then there remains nothing to be shown.

Assume next $z < a$. Then we get $f(z) \leq a < f(a)$, since a is distinguished.

(c) Let finally K be a non empty chain of distinguished elements. We have still to verify that $g(K)$ is distinguished, too. Clearly $g(K) \in Z_0$, since all distinguished elements belong to Z_0. We consider some $z < g(K)$.

In case of $k \in K$ ($\exists k \in K$ with $z < k$) it follows $f(z) \leq k$ since k is distinguished, and thereby $f(z) \leq g(K)$.

But the opposite case is impossible,

For: All $k \in K$ are distinguished. Hence each k is comparable with each z. Hence in this case z would be an upper bound of K and thereby $g(K) \leq z$ in spite of $z < g(K)$.

Consequently: The set of all distinguished elements forms a Zorn-set and is thereby equal to Z_0. But this means that each element of Z_0 is distinguished and consequently comparable with each other element of Z_0.

Hence Z_0 is a chain and $g(Z_0)$ is maximal in $(H, \leq)$. $\square$

3.2 Lattices

We now turn to special posets, called *(semi-) lattices.*

3. 2. 1 Definition. A poset $(M, \leq)$ is called a *sup-semi-lattice,* if it satisfies

$$\forall a, b \ \exists\, c =: \sup(a, b) : (a, b \leq c) \ \& \ (a, b \leq x \Longrightarrow c \leq x),$$

Dually the *inf-semi-lattice* is defined.

Let $(M, \leq)$ be a sup-semi-lattice . Then we denote $\sup(a, b)$ by $a \vee b$ and read a *join* b and in case that $(M, \leq)$ is an inf-semi-lattice , we denote $\inf(a, b)$ by $a \wedge b$ and read a *meet* b.

3. 2. 2 Lemma. *Let* $(M, \leq)$ *be a* sup-*semi-lattice . Then*

$$
\begin{array}{llcl}
\text{(I)} & a \vee a & = & a \\
\text{(K)} & a \vee b & = & b \vee a \\
\text{(A)} & a \vee (b \vee c) & = & (a \vee b) \vee c\,.
\end{array}
$$

PROOF. $\sup(a, b) = \sup(x, y)$ means $u \geq a, b \Longleftrightarrow u \geq x, y\,.$ $\square$

3. 2. 3 Lemma. *Let* $(S, \cdot)$ *be a groupoid, satisfying* (I), (K) *and* (A), *that is a commutative idempotent semigroup. Then*

$$a \leq b \ \ :\Longleftrightarrow \ \ a \cdot b = b$$

defines a sup-*closed partial order on* S *with* $\sup(a, b) = ab$.

PROOF. Under the conditions above it holds:

(R) by $a \cdot a = a \rightsquigarrow a \leq a\,,$

(S) by $a \cdot b = b \ \& \ b \cdot a = a \Longrightarrow a = b \cdot a = a \cdot b = b\,,$

(T) by $a \cdot b = b \ \& \ b \cdot c = c \Longrightarrow a \cdot c = a \cdot b \cdot c = b \cdot c = c$

and moreover we get $a \cdot b = \sup(a,b)$ by

$a, b \leq a \cdot b$ & $a \cdot x = x = b \cdot x \Longrightarrow (a \cdot b) \cdot x = x.$ □

According to 3.2.2 and 3.2.3 any sup-semi-lattice $(M, \leq)$ is associated with a commutative, idempotent semigroup $\mathfrak{S}(M)$ and conversely any commutative idempotent semigroup $(S, \cdot)$ is associated with some sup-semi-lattice $\mathfrak{P}(S)$. Moreover it holds:

3. 2. 4 Proposition. *Choose the operators $\mathfrak{S}$ and $\mathfrak{P}$ as above. Then*

$$\begin{aligned} \mathfrak{P}(\mathfrak{S}(M, \leq)) &\cong (M, \leq) \\ \text{and} \qquad \mathfrak{S}(\mathfrak{P}(S, \cdot)) &\cong (S, \cdot)\,, \end{aligned}$$

a result which is left to the reader.

The structure of *lattices* was introduced by Dedekind under the name *dual group*, cf. [101].

3. 2. 5 Definition. Let $\mathfrak{L} := (L, \vee, \wedge)$ be an algebra of type (2,2). Then $\mathfrak{L}$ is called a *lattice* if

(I$\vee$)	$a \vee a = a$	(I$\wedge$)	$a \wedge a = a$
(K$\vee$)	$a \vee b = b \vee a$	(K$\wedge$)	$a \wedge b = b \wedge a$
(A$\vee$)	$a \vee (b \vee c) = (a \vee b) \vee c$	(A$\wedge$)	$a \wedge (b \wedge c) = (a \wedge b) \wedge c$
(V$\vee$)	$a \vee (b \wedge a) = a$	(V$\wedge$)	$a \wedge (b \vee a) = a$.

It is immediately seen that the lattice structure is *self dual* . This means: given an equation in $\mathfrak{L}$ this equation "remains" valid if the operations $\wedge$ and $\vee$ are exchanged. Less evident is, however, that (I$\vee$) and (I$\wedge$) are developable from the remaining equations, which is shown as follows: Suppose that (K$\vee$),...,(V$\wedge$) are valid. Then:

$$\begin{aligned} a \wedge a &= a \wedge (a \vee (b \wedge a)) && (\mathrm{V}\vee) \\ &= a \wedge ((b \wedge a) \vee a) && (\mathrm{K}\vee) \\ &= a && (\mathrm{V}\wedge)\,. \end{aligned}$$

Furthermore, applying (A$\wedge$), we get

$$a \wedge b = a \iff a \vee b = b\,. \tag{3.11}$$

Hence $a \leq b :\Longleftrightarrow a \vee b = b$ implies $a \geq b :\Longleftrightarrow a \wedge b = b$, that is $a \leq b :\Longleftrightarrow a \wedge b = a$. Consequently: if $(L, \vee, \wedge)$ is a lattice then

$$\begin{aligned} a \leq b \;\; &:\Longleftrightarrow \;\; a \wedge b = a \\ (&\Longleftrightarrow \;\; a \vee b = b) \end{aligned}$$

defines a partial order on L satisfying by (3.11) the rule of *isotonicity:*

(ISO)
$$\begin{aligned} b \leq c \;\; &\Longrightarrow \;\; a \wedge b \leq a \wedge c \\ &\;\;\&\;\;\;\; a \vee b \leq a \vee c\,. \end{aligned}$$

3.3 Modular and distributive Lattices

Within the abundance of lattices some classes turn out as most central and fundamental. Roughly speaking these are the lattices closely related to foundations, that is *logics, general algebra, and geometry, and* w.r.t. *applications like the algebra of circuits.*

3. 3. 1 Definition. A lattice is called *distributive*, if it satisfies

(D$\wedge$) $\quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

(D$\vee$) $\quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$,

that is – by isotonicity, since $\geq$ is always given – if it satisfies:

(D$'_\wedge$) $\quad a \wedge (b \vee c) \leq (a \wedge b) \vee (a \wedge c)$

(D$'_\vee$) $\quad a \vee (b \wedge c) \geq (a \vee b) \wedge (a \vee c)$.

Distributivity is required dually. So distributive lattices ar self dual. However, we may drop one of the two requirements.

3. 3. 2 Lemma. $(L, \vee, \wedge)$ *is – already – a distributive lattice if only one of the two equations* (D$'_\wedge$), (D$'_\vee$) *is fulfilled.* .

PROOF. Let (D$'_\wedge$) be satisfied then it follows (D$_\wedge$) and by (V$_\vee$) we get

$$\begin{aligned} (a \vee b) \wedge (a \vee c) &= ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) \\ &= a \vee (a \wedge c) \vee (b \wedge c) \\ &= a \vee (b \wedge c)\,. \end{aligned}$$
□

There are various semi-lattice oriented versions of distributivity. Here we We present:

3. 3. 3 Proposition. *A lattice $\mathfrak{L}$ is distributive, if it has the decomposition property*

(SD) $$x \leq a \vee b \Longrightarrow x = x_a \vee x_b \ (\exists x_a, x_b \,:\, x_a \leq a, x_b \leq b)\,.$$

PROOF. First of all observe that $\mathfrak{L}$ is already distributive, if

$$a \leq b \vee c \Longrightarrow a = (a \wedge b) \vee (a \wedge c)$$

is satisfied since

$$a \wedge (b \vee c) = (a \wedge (b \vee c)) \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)\,.$$

Suppose now that $a \leq b \vee c$. Then $a = a_b \vee a_c$ with $a_b \leq a \wedge b$ and $a_c \leq a \wedge c$, that is $a \leq (a \wedge b) \vee (a \wedge c)$ whereby the equation results $a = (a \wedge b) \vee (a \wedge c)$. Thus the decomposition property implies distributivity.

Conversely let $\mathfrak{L}$ be distributive. Then

$$\begin{aligned} x = x \wedge (a \vee b) &= (x \wedge a) \vee (x \wedge b) \\ &=: x_a \vee x_b \text{ with } x_a \leq a \ \&\ x_b \leq b. \end{aligned}$$ □

3. 3. 4 Definition. A lattice is called *modular*, if it satisfies the self dual implication

(MO) $$a \geq c \ \Longrightarrow \ a \wedge (b \vee c) = (a \wedge b) \vee c\,.$$

Observe: (MO) is readable as equation. Replace a by $a \vee c$. Then (MO) reads

$$(a \vee c) \wedge (b \vee c) = ((a \vee c) \wedge b) \vee c\,.$$

Further one observes that it suffices to require – merely – the inclusion of the left side w.r.t. the right side.

SINCE: it holds always $a \geq a \wedge b$ and furthermore by isotonicity we get $b \vee c \geq (a \wedge b) \vee c$.

In particular by definition all distributive lattices are modular – *a fortiori.*

A classical example of a modular lattice is the lattice of all *subgroups* of an abelian group.

PROOF. Let $\mathfrak{G}$ be an abelian group. Then $x \in G$ belongs to the subgroups $\mathfrak{A}, \mathfrak{B}$ if it equals some $a+b$ $(a \in A, b \in B)$. Suppose now $A \supseteq C$. Then it results

$$\begin{aligned} x \in A \cap (B+C) \implies x &= b+c \in A \ \ (b \in B, c \in C) \\ \implies b &= x-c \in A \cap B \quad (\text{recall } C \subseteq A) \\ \implies x &= b+c \in (A \cap B)+C\,, \end{aligned}$$

that is $A \cap (B+C) \subseteq (A \cap B)+C$. □

3. 3. 5 Corollary. *Let $\mathfrak{A}$ be an algebra, defined by equations implying explicitly or implicitly an abelian group operation. Then the lattice of all closed subsets is modular.*

Hence, in particular the lattice of all *subspaces* of some *linear space* and the lattice of all *ideals* of any *ring* are modular.

3. 3. 6 Definition. A lattice $\mathfrak{L} := (L, \vee, \wedge)$ with *minimum* 0 and *maximum* 1 is called *complemented* if any x is associated with some x' satisfying

(COM) $$x \vee x' = 1 \ \&\ x \wedge x' = 0.$$

$\mathfrak{L}$ is called *relatively complemented* if (COM) is valid – merely – for any closed interval $(\,a\,] := \{x \mid x \le a\}$ of $\mathfrak{L}$.

Finally we remark:

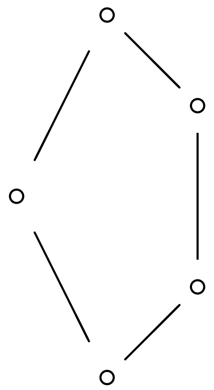
3. 3. 7 Definition. Let $\mathfrak{L}$ be distributive and complemented. Then $\mathfrak{L}$ is called a *boolean lattice*, or synonymously a *boolean algebra.*
The absolutely best possible candidate here is the *power set lattice.* As a most important technical example recall the algebra of circuits.

We are now going to present two classical characterizations of modular and distributive lattices, respectively, due to R. Dedekind and G. Birkhoff, respectively. First of all, a remark:

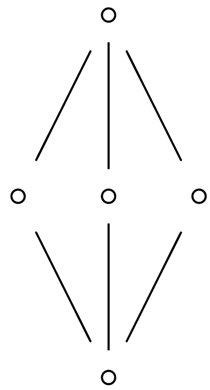
Let $\mathfrak{P} := (P, \le)$ be a finite poset. Then $\mathfrak{P}$ admits a representation by a *Hasse-diagram* . To this end we associate any $a \in M$ with some point of $\mathbf{R} \times \mathbf{R}$ in such a manner that all $x \ge a$ are accessible from below, when starting from a.

One way of characterizing classes of lattices is the method of *forbidden sublattices.* The most trivial example: A lattice is a chain, if it does not contain any $(\{a, b, 0, 1\}, \wedge, \vee)$ with $a \not\leq b \not\leq a$ and $a \wedge b = 0, a \vee b = 1$.

Distributive and modular lattices admit a characterization by forbidding the subsequent lattices, called *pentagon* and *diamond, respectively.*



THE PENTAGON



THE DIAMOND

3. 3. 8 Dedekind. *A lattice is modular iff none of its sublattices is isomorphic to the pentagon.*

PROOF. If $\mathfrak{L}$ is not modular then there exist elements a, b, c with $a \geq c$, satisfying

$$A := a \wedge (b \vee c) > (a \wedge b) \vee c =: C\,,$$

and $b =: B$ cannot be larger than C and cannot be less than A, since otherwise, in the first case, it would follow $b \geq c$ and in the second case $b \leq a$ and thus in any case it would result $a \wedge (b \vee c) = (a \wedge b) \vee c$.

Hence the elements A, B, C are pairwise different, and it holds moreover $B \wedge A = b \wedge a \geq B \wedge C \geq b \wedge a$, that is $B \wedge A = B \wedge C$, and dually $B \vee A = B \vee C$.

Assume now that the underlying lattice contains some pentagon. Then modularity is obviously violated. □

The preceding theorem raises an issue, which gives rise to a special consideration.

Obviously in the pentagon there are two maximal chains of different length between 0 and 1 . In the modular case, however this will not happen, as is pointed out by

3. 3. 9 The Modular Chain Theorem. *Let $\mathfrak{L}$ be a modular lattice and let $a > a_1 \ldots > a_n = b$ be some maximal chain in $[\,a, b\,]$ – of length n. Then $a > a_1 > \ldots > a_n$ is even of maximal length in the set of all chains from a to b.*

PROOF. By induction:

Obviously the assertion is true in the case that a *covers* b, that is the case where the a-chain has length 1.

Let now the assertion already been proved for all maximal chains of a length between 1 and $n-1$. We start from a maximal a-chain and assume that $a > b_1 > b_2 > \ldots > b_n > b_{n+1} = b$ is a formally longer chain.

CASE 1. Suppose $a_k \geq b_m$. Then by induction assumption (IA) we can put in some maximal chain $a_k > c_1 > c_2 > \ldots > c_\ell > c_{\ell+1} = b_m$ and again by (IA) we calculate that from a to b *via* $a_1, \ldots, a_k, c_1, \ldots b_m, \ldots, b_n$ it is not longer than along $a_1, \ldots, a_{n-1}$. This provides nearly immediately that the b-chain from a to b contains at most as much members as the a-chain.

CASE 2. There exists no pair of the case 1 type. Then it holds

$$a_1 \wedge b_1 > a_1 \wedge b_2 > a_1 \wedge b_3 > \ldots > a_1 \wedge b_n > a_1 \wedge b_{n+1}\,.$$

So, by (IA) there are at least two different elements b_i, b_j with $a_1 \wedge b_i = a_1 \wedge b_j$ and by maximality of the a-chain also with $a_1 \vee b_i = a_1 \vee b_j = a$, that is a pentagon in $\mathfrak{V}$, a contradiction. □

Next we present:

3. 3. 10 The Interval Theorem. *Let $\mathfrak{L}$ be modular and let $a, b \in L$. Then the intervals $[\,a \wedge b, b\,]$ and $[\,a, a \vee b\,]$ are order isomorphic.*

PROOF. Put

$$\begin{aligned} f_a(x) &:= a \vee x \qquad (x \in [\,a \wedge b, b\,]) \\ f_b(y) &:= b \wedge y \qquad (y \in [\,a, a \vee b\,])\,. \end{aligned}$$

Then $u \leq v \Longrightarrow f_a(u) \leq f_a(v)$ by isotonicity, and by modularity

$$f_a(f_b(y)) = f_a(b \wedge y) \;=\; a \vee (b \wedge y) = (a \vee b) \wedge y = y$$

and dually

$$f_b(f_a(x)) = f_b(a \vee x) \;=\; b \wedge (a \vee x) = (b \wedge a) \vee x = x\,.$$

Hence f_a is *surjective*, *injective* and *isotone.* $\square$

Suppose $a < b$ and $[\,a, b\,] = \{a, b\}$. Then a and b are called neighboured, or equivalently a is called a lower neighbour of b, respectively, b is called an upper neighbour of a. In this case we write $a \succ b$.

3. 3. 11 The Neighbour Theorem. *Let $\mathfrak{L}$ be a modular lattice and let p be an upper neighbour of $p \wedge q$. Then $p \vee q$ is an upper neighbour*

3. 3. 12 Definition. A lattice is called of *finite length* if any chain $a_1 > a_2 > \ldots > a_n \ldots$ is finite.

Clearly, if $\mathfrak{L}$ is modular and of finite length any a is associated uniquely with the common length of all maximal chains from 0 to a. Recall, by ZORN there exists a maximal chain, which must be finite by assumption. We symbolize this number by $\dim(a)$, it is called the *dimension* of a in $\mathfrak{L}$.

Now we are ready to prove a well known result of linear algebra:

3. 3. 13 The Dimension Formula. *Let $\mathfrak{L}$ be a modular lattice of finite length. Then all pairs a, b satisfy:*

$$\text{(DIM)} \qquad \dim(a) + \dim(b) = \dim(a \wedge b) + \dim(a \vee b)\,.$$

PROOF. Recall that the intervals $[\,a \wedge b, b\,]$ and $[\,a, a \vee b\,]$ are isomorphic and "walk" one time from $a \wedge b$ along a, the other time from $a \wedge b$ along b to $a \vee b$. This leads immediately to (DIM). $\square$

3. 3. 14 Lemma. *Let $\mathfrak{L}$ be modular. Then it is easily checked*

$$(x \wedge (y \vee z)) \vee (y \wedge z) = (x \vee (y \wedge z)) \wedge (y \vee z)\,,$$

and the elements

$$A = (a \wedge (b \vee c)) \vee (b \wedge c), \ldots, C = (c \wedge (a \vee b)) \vee (a \wedge b)$$

satisfy

$$A \vee B = B \vee C = C \vee A = (a \vee c) \wedge (b \vee c) \wedge (a \vee b) =: 1_{A,B,C}$$

and by duality

$$A \wedge B = B \wedge C = C \wedge A = (a \wedge c) \vee (b \wedge c) \vee (a \wedge b) =: 0_{A,B,C}.$$

PROOF.

$$\begin{aligned} A \vee B &= (a \wedge (b \vee c)) \vee (b \wedge c) \vee (b \wedge (c \vee a)) \vee (c \wedge a) \\ &= (a \wedge (b \vee c)) \vee (b \wedge (c \vee a) \\ &= ((a \wedge (b \vee c)) \vee b) \wedge (a \vee c) && \text{(MO)} \\ &= (a \vee b) \wedge (b \vee c) \wedge (a \vee c) && \text{(MO)}\,. \end{aligned}$$

□

3. 3. 15 G. Birkhoff. *A lattice $\mathfrak{L}$ is distributive iff it contains no sublattice isomorphic to the pentagon or to the diamond.*

PROOF. We may start from a lattice, which is modular but not distributive. Define A, B, C as above. In case that two of these elements are equal, we get w. l. o. g. $A \leq B$. This leads further to:

$$\begin{aligned} a \wedge (b \vee c) &= (a \wedge (b \vee c)) \wedge ((b \wedge (a \vee c)) \vee (a \wedge c) \\ &= (a \wedge (b \vee c) \wedge b \wedge (a \vee c)) \vee (a \wedge c) && \text{(MO)} \\ &= (a \wedge b) \vee (a \wedge c)\,. \end{aligned}$$

Hence by symmetry in case of $a \wedge (b \vee c) \not\leq (a \wedge b) \vee (a \vee c)$ we get $A \neq B$ and $A \neq C$.

But, because of 3.3.14 it can neither hold $B \leq C$ (nor $C \leq B$), since in case of $<$ modularity would be violated and in case of $=$ rule 3.3.14 would be violated. Consequently in the case of $a \wedge (b \vee c) \not\leq (a \wedge b) \vee (a \vee c)$ by duality we are led to five different elements $0_{A,B,C}, A, B, C, 1_{A,B,C}$, which form a sublattice of the diamond type.

Conversely, lattices containing the pentagon or diamond as sublattice obviously cannot be distributive. □

By the preceding two propositions we get in addition:

3. 3. 16 Corollary. *A lattice is distributive iff it satisfies the self dual equation:*

(DIS) $\qquad (a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a)\,.$

PROOF. This equation excludes the pentagon and the diamond, as well, as sublattices, that is (DIS) provides distributivity.

On the other hand (DIS) follows straightforwardly by (D$\wedge$). □

(DIS) says obviously that the elements $0_{A,B,C}$ and $1_{A,B,C}$ of the proof above collapse, that is diamonds degenerate to points.

3. 3. 17 Proposition. *A lattice $\mathfrak{L}$ is distributive iff it satisfies*

$$\begin{array}{c} a \wedge x = a \wedge y \\ \& \\ a \vee x = a \vee y \end{array} \implies x = y\,.$$

PROOF. If $(L, \wedge, \vee)$ is not distributive, then $\mathfrak{L}$ contains a pentagon or a diamond, whence $x = y$ cannot follow by the premise. And: if, conversely, $\mathfrak{L}$ is distributive, we get by the premise

$$\begin{aligned} x &= x \wedge (a \vee y) \\ &= (x \wedge a) \vee (x \wedge y) \\ &= (y \wedge a) \vee (y \wedge x) \\ &= y \wedge (a \vee x) \\ &= y \wedge (a \vee y) \\ &= y\,. \end{aligned}$$

□

3.4 Representation

Let $\mathfrak{S}$ be any structure, for instance some *linear space* or a *group* or a *ring* or a *topological space* or some *geometry* or some *poset.* Then the elements of this structure are usually not concretely defined. If, however, we succeed to show that the abstract structure is isomorphic to some concrete structure then – maybe – this leads to advantages w. r. t. further investigations.

This is most impressive shown by the structure of a linear space. Here we start from an abstract linear space, we show that this space contains a *basis* and are thus in the position to consider the *vectors* of this space as *n-tuples* of *scalars,* that is elements of the underlying *field.*

Thus the given linear space turns to a concrete structure, *modulo* the underlying field. This is the point, when students feel most relieved, since they rediscover what they studied at school.

Similarly we could discuss the representation of the linear space of linear operators from $\mathfrak{K}^m$ into some $\mathfrak{K}^n$ by *matrices.*

At this place we are concerned with posets and the trial of their representation.

Clearly, the value of our efforts will be demonstrated by the results. But, didactically considered, their value might be much more important, since the method of proof is extremely elementary but will demonstrate – most impressively – all essentials of a representation procedure in general.

The fundamental idea is simple. We want to *encode* the elements of P by $0,1$-sequences. This will lead to further representation possibilities.

3. 4. 1 Definition. Let $\mathfrak{P}$ be a poset. By an *order filter* of $\mathfrak{P}$ we mean any subset A of P – not necessarily $\neq \emptyset$ – which contains together with any x also all $y \geq x$. Dually, by an *order ideal* we mean any subset B of P, which contains together with any y also all elements $x \leq y$.

In particular in case of $F = [\,x\,) := \{u \,|\, x \leq u\}$ we call F a *principal order filter* and define dually the notion of a *principal order ideal.*

Obviously the set theoretical complement of an order filter is an order ideal and conversely the complement of an order ideal is an order filter.

Also, we see immediately that there are enough ideals and enough filters, meaning that for any pair $a \neq b$ there exist at least one ideal and at least one filter, respectively, containing one of these two elements but avoiding the other one.

Now we consider the family of all *decompositions* $P = A_i + B_i \ (i \in I)$, where A_i is a filter and $B_i = P - A_i$ is an ideal. Then for a fixed element $x \in P$ it holds componentwise $x \in A_i$ *aut* $x \in B_i$. Thus the mapping $f_x : i \longmapsto x_i \in \{0,1\}$ with

$$\begin{aligned} f_x(i) &= x_i = 1 \Longleftrightarrow x \in A_i \\ f_x(i) &= x_i = 0 \Longleftrightarrow x \notin A_i \end{aligned}$$

provides a unique encoding for x such that:

$$x \leq y \Longleftrightarrow x_i \leq y_i \ \ (\forall i \in I)$$

is satisfied. Applying his equivalence we are immediately led to

3. 4. 2 The Representation Theorem for Posets. *Any poset may be considered as a set of* $0,1$*-sequences, w. r. t. component comparing.*

And this implies:

Any poset may be considered as a system of sets w.r.t. inclusion .

PROOF. Part one is clear by the construction described above.

In order to prove part 2 we associate with each sequence $\{x_i\}$ that subset of I, which contains exactly the indices i with $x_i = 1$. □

A Hint: It should be emphasized that the set of filters, including the empty set, and dually the set of ideals, containing the empty set as well, is closed w.r.t. $\bigcap$ and $\bigcup$. Consequently we could have shown that any poset may be considered as a system of sets w.r.t. inclusion. In this case the elements of $\mathfrak{P}$ would be represented by the principal filters and principal ideals of $\mathfrak{P}$, respectively, and we would get a codification of the elements by choosing the set of all filters or ideals, respectively as index set I.

We now turn to semi-lattices.

3. 4. 3 Definition. Let $\mathfrak{S}$ be a $\vee$-semi-lattice . Then a subset I of S, maybe empty, is a *semi-lattice ideal* if

$$a \vee b \in I \iff a, b \in I\,.$$

$I \subseteq S$ is consequently an ideal iff firstly together with any a, b also $a \vee b$ belongs to I and secondly together with any $y \in I$ also all $x \leq y$ are in I.

Observe: Any semi-lattice ideal is also an order ideal of the corresponding poset.

Obviously S itself is a semi-lattice ideal and together with any family of semi-lattice ideals also the intersection of this family is a semi-lattice ideal. Hence any subset A of S generates a smallest ideal $\langle A \rangle$ namely the intersection of all A containing ideals, denoted by $[\,A\,]$. This externally defined *hull* turns out as

$$\{x \,\big|\, x \leq a_1 \vee \ldots \vee a_n \;\; (\exists a_i \in A \;\; (1 \leq i \leq n)\}$$

and is thus also internally definable.

Let now $a \neq b$ be two elements of a semi-lattice $\mathfrak{S}$. Then obviously there exists some a and b separating ideal. This means that the above representation theorem holds similarly also for semi-lattices.

Like posets and semi-lattices also lattices generate representation problems. But if this shall be realized by subsets of a set we have to take into account that this is impossible unless the lattice under consideration is distributive. In the distributive case, however we succeed relatively straightforwardly.

FOR: $u \neq v$ are separated once $u \wedge y$ and $u \vee v$ are separated, whence we may start from some $u < v$. Then there exists a *value* M that is a maximal u containing but v avoiding ideal with $a, b \notin M \Longrightarrow a \wedge b \notin M$, that is $a \wedge b \in M \Longrightarrow a \in M \bigvee b \in M$, whence M is prime.

FOR: $\mathfrak{L}$ is distributive, hence in case of $a, b \notin M$ and $a \wedge b \in M$ on the one hand the set of all x with $a \wedge x \in M$ forms a proper supideal B of M and on the other hand the set of all y with $y \wedge b \in M \ \ (\forall b \in B)$ forms a proper supideal A of M. This would lead to $v \in A \wedge B$ that is $v = v \wedge v \in M$, opposite to the assumption. Consequently the method of proof for posets can be transferred to distributive lattices in a $\wedge$-respecting manner , that is we get:

3. 4. 4 (G. Birkhoff). *Any distributive lattice is a lattice of sets.*

Analogously we obtain

3. 4. 5 M. H. Stone. *Any boolean algebra is a field* $(F, \cap, \cup, ')$ *of sets.*

3.5 Complete Lattices

We symbolize $\operatorname{Sup}(a_i)$ $(i \in I)$ also by $\bigvee A$ and $\operatorname{Inf}(a_i)$ $(i \in I)$ also by $\bigwedge A$.

3. 5. 1 Definition. A lattice is called *conditionally complete* if any *upper bounded supset* is even *upper limited.* A conditionally compete lattice is called *Sup-distributive* if is it satisfies

(DV) $$s = \bigwedge a_i \,(i \in I) \implies x \vee s = \bigwedge (x \vee a_i) \,(i \in I) \,.$$

Dually the notion of *Inf-distributivity* and axiom (DS) are defined.

Finally, a conditionally complete lattice is called *completely distributive* if it satisfies – for all existing limits:

(DV1) $$\bigwedge_C \left[\bigvee_{A_\gamma} a_{\gamma,\alpha}\right] = \bigvee_\Phi \left[\bigwedge_C a_{\gamma,\phi(\gamma)}\right]$$

(DV2) $$\bigvee_C \left[\bigwedge_{A_\gamma} a_{\gamma,\alpha}\right] = \bigwedge_\Phi \left[\bigvee_C a_{\gamma,\phi(\gamma)}\right] \,,$$

where γ runs through the set C and Φ denotes the set of all mappings ϕ from C into the *union* of all A_γ with $\phi(\gamma) \in A_\gamma$.

Obviously any conditionally complete chain is completely distributive, and thereby in particular Sup- and Inf- distributive. On the other hand (DV1) and (DV2) are independent one from each other.

FOR:Consider the system of all *closed subsets* of the plane. Let further C be the circle $x^2 + y^2 = 1$ and denote by C_k the sets of points $x^2 + y^2 \leq 1 - k^{-2}$ $(k \in \mathbf{N})$. Then in the lattice of all closed subsets of the plane it holds

$$C \cap \bigvee C_k = C \neq \emptyset = \bigvee (C \cap C_k) .$$

3. 5. 2 Definition. A lattice $\mathfrak{L}$ is called *complete*, if each $A \subseteq L$ is upper limited – by $\operatorname{Sup}(A)$. This is, of course, equivalent to the property that each $A \subseteq L$ is lower limited – by $\operatorname{Inf}(A)$.

If $\mathfrak{L}$ is complete we denote $\operatorname{Inf}(L)$ by 0 and $\operatorname{Sup}(L)$ by 1.

Observe: By definition the empty set $\Box$ satisfies $\operatorname{Sup}(\Box) = \operatorname{Inf}(L) = 0$ and $\operatorname{Inf}(\Box) = \operatorname{Sup}(V) = 1$.

Chapter 4

Ideal Systems

4.1 Ideal Operators

Let $(S, \cdot) =: \mathfrak{S}$ be a *semigroup.* By the *global* $G(\mathfrak{S}) =: \mathfrak{G}$ of $\mathfrak{S}$ we mean the *powerset* of S considered w. r. t. *the complex product*

$$A \cdot B := \{a \cdot b \,|\, a \in A, b \in B\} =: AB := A \cdot B\,, \quad (A, B \subseteq S)$$

and hence in particular with $A \cdot \square = \square = \square \cdot A$.

By a *monoid* we mean, of course, a *semigroup* with *identity* 1. A monoid is called a 0-*monoid* if it contains a zero 0 satisfying $0 \cdot a = 0 = a \cdot 0$.

Obviously the *global* of a 0-monoid is again a 0-monoid.

Any semigroup admits a 0-*monoid-extension.* If necessary, adjoin an identity 1 or a zero 0.

A semigroup satisfying $xa = xb \Longleftrightarrow a = b \Longleftrightarrow ax = bx$ is called *cancellative.* If $\mathfrak{S}$ is a cancellative monoid without identity, the corresponding monoid is again a cancellative monoid.

A semigroup with 0 is called 0-*cancellative*, if it satisfies $xa = xb \neq 0 \Longrightarrow a = b$ and $ax = bx \neq 0 \Longrightarrow a = b$.

Finally, by a cancellative semigroup with *zero* we mean a cancellative semigroup with adjoined 0.

Let $\mathfrak{G} := G(\mathfrak{S})$ be the global of the semigroup $\mathfrak{S}$. Then $\mathfrak{G}$ is a *poset* w.r.t. $\supseteq$ and $(\,G(\mathfrak{S})\,, \cup, \cap\,)$ is a *boolean algebra* and a *po-semigroup,* as well, since

$$\begin{gathered} A \supseteq B \\ \Longrightarrow \\ AX \supseteq BX \quad \& \quad XA \supseteq XB\,. \end{gathered}$$

Next, defining: $\sum A_i \;:=\; \bigcup A_i \quad (i \in I)\,,$

we get $X \cdot (\sum A_i) \cdot Y \;=\; \sum (X \cdot A_i \cdot Y)\,.$

We are interested in certain *ideal homomorphic images* of $G(\mathfrak{S})$ with multiplication $\circ$ where $\mathfrak{S}$ is a 0-monoid. The reason ?

Let $\mathfrak{R}$ be a *classical number domain.* Then *prime factorization* – even though perhaps possible – by no means need be unique. Hence the question arises whether uniqueness might be restored in some extension. This is the central subject of *ideal theory.*

The method, in general, is the following:

Consider semigroups of ideals, in order to investigate divisibility of $\mathfrak{R}$ *via*

$$\langle t \rangle \;\Big|\; \langle a \rangle\,.$$

To this end we have to certify in general at least

$$\begin{array}{ccc} \text{ideal } \langle a \rangle & \supseteq & \text{ideal } \langle b \rangle \\ & \Rightarrow & \\ & a \,\Big|\, b & \end{array}$$

and in rings one should try to ensure

$$a, b \in I \implies a \pm b \in I$$

in order to save as much addition as possible by

$$\begin{array}{ccc} a = b + c & \& & a, b \in I \\ & \Rightarrow & \\ c & \in & I\,. \end{array}$$

There may exist a large variety of interesting homomorphic images, but in general different images are of different value, of course, w.r.t. our purpose.

In particular we are interested in certain ϕ-images whose elements are subsets of S satisfying

(C0)
$$\begin{array}{ccc} \phi\, X & = & \phi\, Y \\ & \Longrightarrow & \\ \phi\,(AX) = \phi\,(AY) & \& & \phi\,(XA) = \phi\,(YA)\,. \end{array}$$

In other words we are looking for homomorphisms ϕ of $\mathfrak{G}(S)$ on semigroups of subsets of S with multiplication $\circ$ satisfying $\phi\,(A)\,\circ\phi\,(B)\;=\phi\,(AB)$. Observe that in case of (C0) we are in the position to define a product $\phi\,A\circ\phi\,B$ by $\phi\,A\circ\phi\,B:=\phi\,(AB)$.

Most *ideal* are, of course, furthermore images satisfying

$$\begin{array}{llcl} (i) & S\cdot A\cdot S & \subseteq & \phi\,A \\ (ii) & X\circ(\sum A_i)\circ Y & = & \sum(X\cdot A_i\cdot Y) \quad (i\in I)\,, \end{array}$$

where $\cdot$ is taken as symbol of the complex product in $\mathfrak{G}$, $\circ$ as multiplication symbol of the image of $\mathfrak{G}$, and $\sum$ as symbol of the finest $\phi\,(X)$ containing all components.

Let henceforth $\mathfrak{S}$ be a 0-monoid and $\mathfrak{G}$ its global. We call ϕ an *ideal operator* and $\phi\,(A)$ a ϕ*-ideal* if the operator ϕ satisfies (C0) and thereby $\phi\,A\circ\phi\,B:=\phi\,(AB)$ and if in addition the subsequent conditions (C1) through (CI) are satisfied:

$$\begin{array}{lrcl} \text{(C1)} & A & \subseteq & \phi\,A \\ \text{(C2)} & \phi\,(\phi\,A) & = & \phi\,A \\ \text{(C3)} & A\subseteq B & \Rightarrow & \phi\,A\subseteq\phi\,B \\ \text{(CI)} & S\cdot a\cdot S & \subseteq & \phi\,(a)\,. \end{array}$$

Clearly, by an *ideal semigroup* we mean the set of all $\phi\,(A)$ w.r.t. $\circ$ where ϕ is an ideal operator. As usual $\phi\,(A)$ *is called a principal ideal* if $\phi\,(A)$ is equal to some $\phi\,(a)$.

Obviously by (C1) through (C3) ϕ is a *closure operator*, meaning in particular, that the intersection of closed sets is closed, whereas ϕ by (CI) is an *ideal operator* satisfying $S\cdot(\phi\,A)\,\cdot S\subseteq\phi\,A$. Observe:

$$\begin{array}{rcl} x\in\phi\,A & \Longrightarrow & S\cdot x\cdot S\subseteq\phi\,x\subseteq\phi\,A \\ & \Longrightarrow & S\cdot x\cdot S\subseteq\phi\,A \\ & \rightsquigarrow & \\ S\cdot(\phi\,A)\cdot S & \subseteq & \phi\,A\,. \end{array}$$

Furthermore (C1) through (C3) imply:

$$\text{(4.8)} \qquad A_i\;=\phi\,(A_i{}')\;\Longrightarrow\;\sum A_i\;=\phi\,(\sum A_i)\;\;(i\in I)\,.$$

PROOF. Suppose $A_i = \phi(A_i{}')$. It follows $A_i = \phi(A_i)$ and thereby

$$\begin{array}{rcl} \phi(\bigcap A_i) & \subseteq & \phi(A_i) = A_i \ (\forall i \in I) \\ & \leadsto & \\ \phi(\bigcap A_i) & \subseteq & \bigcap A_i \\ & \leadsto & \\ \phi(\bigcap A_i) & = & \bigcap A_i \ , \end{array}$$

the final conclusion by (C1). $\square$

As an example of a homomorphism satisfying (C1) through (C3) but not (CI) we give:

$$\begin{array}{lrcl} & \mathfrak{G}(\mathbf{R},+) & \longrightarrow & (\{[a,b] \,|\, a,b \in \mathbf{R}^\infty\} \cup \square\,,+) \\ \text{with} & \phi(A) & := & \sum [a,b] \ \ ([a,b] \supseteq A) \,. \end{array}$$

As the very first ideal semigroup we present the semigroup of *Rees ideals* of commutative 0-monoids, briefly the semigroup of *r-ideals* $\phi_r A$ satisfying

$$\phi_r A \ := \ \langle A \rangle_r := SA\,.$$

Obviously in commutative semigroups satisfying $a \,|\, b \;\&\; b \,|\, a \Longrightarrow a = b$ r-ideals are *order filters* and *vice versa.*

Another example is given by the classical *c-ideals* (linear (c)ombining-ideals) $\phi_c A$ of commutative rings with identity, defined *via*

$$\phi_c A := \langle A \rangle_c := \{\textstyle\sum_1^n r_i a_i \,|\, r_i \in R, a_i \in A\} =: \langle a_1, \ldots, a_n \rangle\,.$$

Every 0-monoid $\mathfrak{S}$ may be considered in a canonical manner as a *semi-ring* by defining $a + b := 0$. This allows to consider the r-ideals and c-ideals above, as well, as *semiring ideals* of some commutative semiring.

Here a *semiring* is supposed to be an algebra of type $(H, +, \cdot, 0, 1)$ where $(H, +, 0)$ is a commutative (additive) monoid with *identity* 0 and where $(H, \cdot, 1)$ is a monoid, not necessarily commutative, with identity 1, satisfying $x(a + b)\,y = xay + xby$.

Apart from the given semi-ring ideal type there is another one of similar interest.

Consider again the c-ideal $\mathfrak{c}$ of a commutative ring with identity. $\mathfrak{c}$ owns the properties that together with a and $a + b$ also b belongs to $\mathfrak{c}$ and that together with each a also all elements ar belong to $\mathfrak{c}$. The same is true if we define semi-ring ideals in this sense, in particular for the semi-rings $(H, \wedge, \cdot, 1, 0)$ with $x(a \wedge b)y = xay \wedge xby$. This includes the semigroup of m-filters, that is filters F satisfying $(a, b \in F \iff a \wedge b \in F)$ of *lattice ordered semigroups*, in particular of the *distributive lattice* and of the *lattice group cone with zero*.

Thus most classical situations are included if we define d-ideals for commutative semi-rings with 0 and 1 by

$$a \in \mathfrak{d} \Longrightarrow ar \in \mathfrak{d}(\forall\, r \in H)\,\&\, a, b \in \mathfrak{d} \Longrightarrow (a, a+b \in \mathfrak{d} \Rightarrow b \in \mathfrak{d}).$$

It is easily seen that this definition provides in fact a system of ideals, and it is moreover easily seen that commutativity is unessential for this definition.

Let now ϕ be an ideal operator, i. e. let ϕ satisfy $\phi\,(AB) = (\phi\, A) \circ (\phi\, B)$. For the sake of convenience we will formulate the subsequent rules of this section merely one sided. But, again, recall that by right-left symmetry the right-left dual versions are valid, too.

4. 1. 1 Definition. Let $\phi\ (A_i)\ \ (i \in I)$ be a family of ϕ-images. We define

$$\sum \phi\ (A_i)\ := \ \bigcap \phi\ (B_j)\ \ (\phi\ (B_j)\ \supseteq A_i\ \ (\forall i \in I)).$$

Clearly we could have required equivalently $\phi\ (B_j)\ \supseteq \phi \bigcup (A_i)$. Hence we get immediately:

$$\sum \phi\ (A_i)\ = \ \phi\ \left(\bigcup A_i\right)\quad (i \in I)\,. \tag{4.9}$$

Furthermore it holds:

$$\phi \sum \phi\ (A_i)\ = \ \sum \phi\ (A_i)\quad (i \in I)\,. \tag{4.10}$$

PROOF. Recall 4.8 and observe that $\phi \sum A_i$ is the intersection of closed sets. $\square$

In particular the preceding lemma certifies

$$\phi\, A\ = \ \sum \phi\,(a)\ \ (a \in A)\,. \tag{4.11}$$

Moreover (4.10) implies

$$(\phi\, X\,) \circ \sum \phi\, A_i\ = \ \sum\, (\,\phi\, X) \circ (\,\phi\, A_i\,)\ \ (i \in I)\,. \tag{4.12}$$

PROOF.
$$\begin{aligned}(\phi X)\circ\sum\phi A_i &= (\phi X)\circ\phi\left(\bigcup A_i\right)\ \ (i\in I)\\ &= \phi\left(X\cdot\bigcup A_i\right)\\ &= \phi(\bigcup(X\cdot A_i)\ )\\ &= \sum\phi(X\cdot A_i) \qquad\qquad (4.10)\\ &= \sum(\,(\phi X)\circ(\phi A_i)\,)\,.\end{aligned}$$ □

Next we obtain

(4.13) $$\phi A \;=\; \sum\phi(B_i)\ \ (\,\phi(\,B_i\,)\supseteq A\,)\ \ (i\in I)$$

PROOF. By (4.11) we get

$$\phi A \;=\; \sum\phi(a)\ \ (a\in A)\ .$$

Hence, by (4.10), it results

$$\begin{aligned}\phi A &= \bigcap\phi(B_i)\quad(\,\phi(B_i)\supseteq\phi(a)\,,\ a\in A\,)\\ &\leadsto\\ \phi A &= \sum\phi(B_i)\quad(\,\phi(\,B_i\,)\supseteq A\,)\ .\end{aligned}$$ □

Put now

(4.14) $$\begin{aligned}A*\phi B &:= \{x\,|\,A\cdot x\subseteq\phi B\}\quad(x\in S)\,.\\ \phi B : A &:= \{y\,|\,y\cdot A\subseteq\phi B\}\quad(y\in S)\,.\end{aligned}$$

This provides the crucial rule:

(4.15) $$\begin{aligned}A*\phi B &= (\phi A)*(\phi B)\\ &= \sum\phi(x)\ \ (A\cdot x\subseteq\phi B)\,.\end{aligned}$$

PROOF.
$$\begin{aligned}A\cdot x\subseteq\phi B &\Longrightarrow \phi(\,(\phi A)\cdot x\,)\subseteq\phi B\quad(\mathrm{C1},\mathrm{C2})\\ &\Longrightarrow (\phi A)\cdot x\subseteq\phi B\,, \qquad\qquad (\mathrm{C1})\end{aligned}$$
$$\leadsto\qquad A*\phi B\ \subseteq\ (\phi A)*(\phi B)\subseteq A*\phi(B)$$

and – putting $X := (\phi A)*(\phi B) = A*\phi B$ – we get

$$\begin{aligned}A\cdot X &\subseteq \phi B\\ &\leadsto\\ A\cdot(\phi X) &\subseteq (\phi A)\circ(\phi X)\\ &\subseteq \phi B\\ &\leadsto\\ \sum\phi(x) &= \phi X = X\,.\end{aligned}$$

we are through. □

In particular, together with ϕA, ϕB by (4.15) also $(\phi A) * (\phi B)$ is a ϕX.

Finally : Given a family of subsets of S it may be useful to verify first (C1) through (CI), in order to define a multiplication by

$$(\phi A) \circ (\phi X) \;:=\; \phi (AX).$$

But, of course, one succeeds only if and if

$$\begin{aligned} \phi X = \phi Y \;\Longrightarrow\;& \phi(AX) = \phi(AY) \\ \&\;\;& \phi(XA) = \phi(YA) \end{aligned}$$

This idea will be taken up in the next section.

The rules developed so far follow from (C0) through (CI), and it is easily seen that the subsets ϕX behave most similarly to classical *ideals*.

Nevertheless, with respect to classical problems and with respect to an optimal *ideal arithmetic* the axioms stated above fail to be strong enough. Therefore we now turn to special ideal semigroups.

We consider in $(\mathbf{R}^{\geq 0}, +)$ the operator $\phi A := \operatorname{Inf}(A)$. ϕ is ideal, of course, but ϕ fails to satisfy

(FC)
$$\begin{aligned} c \in \phi A \;\Longrightarrow\;& c \in \phi(a_1, \ldots, a_n) \\ & (\exists\, a_i\, (1 \leq i \leq n) \in A). \end{aligned}$$

However, any ideal operator ϕ is associated in a canonical manner with an ideal operator ϕ_e of *finite character,* i. e. some ϕ_e satisfying (FC). More precisely:

4. 1. 2 Proposition. *Let ϕ be an ideal operator. Then*

$$\phi_e A \;:=\; \bigcup \phi(a_1, \ldots, a_n) \quad (a_i \in A)$$

is an ideal operator, too, satisfying in addition axiom (FC).

PROOF. The conditions (C1) through (CI) and (FC) are satisfied evidently. So it remains to verify that

$$(\phi_e A) \circ (\phi_e B) \;:=\; \phi_e (A \cdot B)$$

makes sense, or – equivalently – that we get

$$\phi_e X = \phi_e Y \implies \phi_e(AX) = \phi_e(AY).$$

But this results from

$$x \in \phi_e X \implies x \in \phi(y_{i_1}, \ldots, y_{i_s}) \ \ (\exists\, y_{i\ldots} \in Y)$$

via:

$$\begin{array}{rcl} \phi_e X = \phi_e Y & \& & u \in \phi_e(AX) \\ & \implies & \\ u & \in & \phi(a_1x_1, \ldots, a_nx_n)(x_i \in X) \\ & \subseteq & \phi(a_1, \ldots, a_n) \circ \phi(x_1, \ldots, x_n) \\ & \subseteq & \phi(a_1, \ldots, a_n) \circ \phi(y_1, \ldots, y_m) \\ & \subseteq & \phi(a_1y_1, \ldots, a_ny_m)\,(y_i \in Y) \\ & \implies & \\ u & \in & \phi_e(AY) \\ & \rightsquigarrow & \\ \phi_e(AX) & \subseteq & \phi_e(AY) \\ & \rightsquigarrow & \\ \phi_e(AX) & = & \phi_e(AY), \end{array}$$

where the final conclusion follows by duality. □

Obviously a subset $\mathfrak{a}$ is some $\phi_e A$ if and only if with each finite subset $E \subseteq \mathfrak{a}$ the set ϕE is again contained in $\mathfrak{a}$.

This view provides immediately that each ϕA is some $\phi_e B$ but, of course, not necessarily equal to $\phi_e A$. Hence in particular each $A * \phi_e B$ is some $\phi_e X$, and together with a family $\phi_e A_i$ $(i \in I)$ its intersection is some $\phi_e A$.

4.2 A finest Ideal System in general

Obviously Dedekind ideals of arbitrary rings satisfy much of ideal theory presented above. But they fail to satisfy (C0). This motivates looking for some substitute for the non commutative case. To begin with, we define:

$$\begin{array}{rrcl} & \phi_{\max}(\square) & := & \square \\ \& & \phi_{\max}(A \neq \square) & := & S. \end{array}$$

Then it follows

4. 2. 1 Proposition. *$\phi := \phi_{\max}$ is an ideal operator, and there exists a finest ideal operator $\phi_{\min} =: \kappa$ defined by the family of all ideal operators ϕ_i via:*

$$\langle A\rangle_\kappa \;:=\; \phi_{\min} A := \bigcap \phi_i\, A\,,$$

and this operator κ satisfies moreover condition (FC).

PROOF. $A \subseteq \langle A\rangle_\kappa$, $A \subseteq B \Longrightarrow \langle A\rangle_\kappa \subseteq \langle B\rangle_\kappa$ and $S\cdot a\cdot S \subseteq \langle a\rangle_\kappa$ are evident. Next $\langle A\rangle_{\kappa\kappa} = \langle A\rangle_\kappa$ follows from

$$\begin{array}{rcl} A \subseteq \langle A\rangle_\kappa & \rightsquigarrow & \langle A\rangle_\kappa \subseteq \langle A\rangle_{\kappa\kappa} \\ & \& & \\ \langle A\rangle_{\kappa\kappa} & = & \langle \bigcap \phi_i\, A,\ \ (i\in I)\,\rangle_{\,\kappa} \\ & = & \bigcap (\phi_j \bigcap \phi_i\, A)\ \ (i,j\in I) \\ & \subseteq & \bigcap \phi_i\,(\phi_i\, A)\ \ (i\in I) \\ & = & \langle A\rangle_\kappa\,. \end{array}$$

Furthermore it holds

(COL) $\qquad \langle X\rangle_\kappa = \langle Y\rangle_\kappa \;\Longrightarrow\; \langle A\cdot X\rangle_\kappa = \langle A\cdot Y\rangle_\kappa$

(COR) $\qquad \langle U\rangle_\kappa = \langle V\rangle_\kappa \;\Longrightarrow\; \langle U\cdot A\rangle\kappa = \langle\, \mathsf{V}\ \cdot A\rangle_\kappa\,,$

since $\langle X\rangle_\kappa = \langle Y\rangle_\kappa$ implies

$$\phi_i\,(A\cdot X) = \phi_i\,(\phi_i\, A\cdot \phi_i\, X) \;\supseteq\; \phi_i\,(\phi_i\, A\cdot Y) = \phi_i\,(A\cdot Y)\,.$$

Finally we consider κ_e. Since κ is an ideal operator, κ_e is again ideal whence κ_e contributes to κ. Hence $\kappa = \kappa_e$. □

We will not return to κ. All we wished to show was the existence of ideal operators also in the non commutative case. But, we will come back to r- and d-ideals $\langle A\rangle$, respectively, in the non commutative case.

As is easily seen these ideals need not satisfy $\langle a\rangle_r\cdot\langle b\rangle_r = \langle ab\rangle_r$ or $\langle a\rangle_d\cdot\langle b\rangle_d = \langle ab\rangle_d$, respectively. Nevertheless they *behave distributively*, and they satisfy

$$\langle A\rangle \;=\; \sum_{a\in A} \langle a\rangle\,.$$

So they are examples of ideals apart from ideal operators – in the sense of this paper.

This shows that an ideal system may be most important though it does not satisfy condition (C0).

4.3 v- and t-Ideals

An efficient ideal theory for monoids requires, of course, an ideal notion as near as possible to the d-ideal notion. Starting from v-ideals this can be realized *cum grano salis* by the *t-ideals,* introduced by PAUL LORENZEN in [275]. Recall the chapter on rings!

Again, let $\mathfrak{S}$ be a commutative 0-monoid. We define

$$s \,|\, A \;\;:\Longleftrightarrow\;\; s \,|\, a \;(\forall\, a \in A)$$

and
$$\phi_v\, A =: \langle A \rangle_v \;\;:=\;\; \{c \,\big|\, s \,|\, A \cdot t \Longrightarrow s \,|\, c \cdot t\}\,.$$

This provides a function of the *power set* $G(S)$ into itself. Furthermore we have

$$\begin{aligned} \langle X \rangle_v = \langle Y \rangle_v \;\;&\Longrightarrow\;\; (\, s \,|\, (A \cdot X)\, t \Longrightarrow s \,|\, (A \cdot Y)\, t\,) \\ &\Longrightarrow\;\; \langle A \cdot X \rangle_v = \langle A \cdot Y \rangle_v \end{aligned}$$

and thereby

$$\langle A \rangle_v \circ \langle B \rangle_v \;\;:=\;\; \langle AB \rangle_v\,.$$

We now verify (C1) through (CI).

Ad (C1): $A \subseteq \langle A \rangle_v$ because $(a \in A) \Longrightarrow (s \,|\, At \Longrightarrow s \,|\, at)$.

Ad (C2): $\langle A \rangle_{vv} = \langle A \rangle_v$ by

$$s \,|\, X \cdot t \Longrightarrow s \,|\, \langle X \rangle_v \cdot t \leadsto \langle A \rangle_{vv} \subseteq \langle A \rangle_v\,.$$

Ad (C3):
$$\begin{array}{ccc} A \supseteq B & \& & c \in \langle B \rangle_v \\ & \Longrightarrow & \\ s \,|\, At \Rightarrow & s \,|\, Bt & \Rightarrow s \,|\, ct \\ & \leadsto & \\ s \,|\, At & \Rightarrow & s \,|\, ct \\ & \leadsto & \\ c & \in & \langle A \rangle_v\,. \end{array}$$

Ad (CI):
$$c \in \langle a \rangle_v \;\;\Longleftrightarrow\;\; a \,|\, c\,.$$

v-ideals work sometimes in rings where d-ideals fail to have a good ideal arithmetic – as has been developed already within our historical remarks, again – consider for instance $\mathbf{Q}[x, y]$, and in addition v-ideals are of great importance in analysis, recall that upper classes of DEDEKINDian cuts of $(\mathbf{R}^{\geq 0}, +)$ are v-ideals. Unfortunately v-ideals fail to be of finite character. But – as shown above – we can change to the operator

$$\phi_t\, A := \langle A\rangle_t := \Big\{c\,\Big|\, s \mid Et \Longrightarrow s \mid ct \ \ (\exists\, E \subseteq A\,, E = \langle e_1, \ldots, e_n\rangle)\Big\}$$

satisfying condition (FC). For cancellative monoids this means that v-ideals admit a description by quotients *via* $A^{-1} := \{x \mid Ax \subseteq S\}$ because

$$\begin{aligned} c \in A_v \iff & s \mid A \cdot t \Rightarrow s \mid c \cdot t \\ \iff & A \cdot ts^{-1} \subseteq S \Rightarrow c \cdot ts^{-1} \subseteq S \\ \iff & c \cdot A^{-1} \subseteq S \\ \iff & c \in (A^{-1})^{-1}\,. \end{aligned}$$

This is essential for our next consideration:

As remarked already in the introduction, in the integral domain $\mathfrak{G}$ of all algebraic integers any v-ideal is a d-ideal.

SKETCH OF A PROOF: [1] Let $\gamma_1, \gamma_2, \ldots, \gamma_n$ be elements of $\mathfrak{G}$ and let $\mathfrak{G}_\gamma$ be the integral part of $\mathbf{Q}[\gamma_1, \gamma_2, \ldots, \gamma_n]$. W.r.t. $\mathfrak{G}_\gamma$ each d-ideal $\langle\beta_1, \beta_2, \ldots, \beta_m\rangle$ of $\mathfrak{G}_\gamma$ is equal to the corresponding t-ideal $\langle\beta_1, \beta_2, \ldots, \beta_m\rangle_t$, since the d-ideals of $\mathfrak{G}_\gamma$ form a divisor theory. Hence d-ideals of $\mathfrak{G}_\gamma$ are also v-ideals of $\mathfrak{G}_\gamma$.

A Hint: According to DEDEKIND, we get $\mathfrak{a} \cdot \mathfrak{a}^{-1} = \langle 1\rangle$ for any ideal $\mathfrak{a}$ of any $\mathfrak{G}_\gamma$. Furthermore $\mathfrak{a} \longmapsto \mathfrak{a}_v$ provides a homomorphism satisfying $\mathfrak{a}_v \supseteq \mathfrak{b}_v \Longrightarrow \mathfrak{a}_v \,\Big|\, \mathfrak{b}_v$. Hence in the semigroup of d-ideals and the semigroup of v-ideals of $\mathfrak{G}_\gamma$, too, may both be considered as a divisor theory, and it remains only to show $\mathfrak{a} = \mathfrak{a}_v$. This is clear in case of an irreducible $\mathfrak{p}$ since $\mathfrak{p}_v = (\mathfrak{p}^{-1})^{-1} = \langle 1\rangle$ would lead to $\mathfrak{p}^{-1} = R$, in contradiction to the Gruppensatz. So, let $\mathfrak{a}$ be an arbitrary ideal with $\mathfrak{a}_v \supset \mathfrak{a}$. Then, since $\mathfrak{a}_v$ is also a d-ideal there exists some irreducible $\mathfrak{p}$ with $\mathfrak{a}_v \cdot \mathfrak{p} \supseteq \mathfrak{a} \rightsquigarrow \mathfrak{a}_v \cdot \mathfrak{p}_v = \mathfrak{a}_v$ for at least one irreducible $\mathfrak{p}$, and thereby furthermore to $\mathfrak{p}_v = \mathfrak{p} = \langle 1\rangle$, a contradiction.

[1] The interested reader is referred to the final chapter

Consequently each finitely generated d-ideal of $\mathfrak{G}_\gamma$ is also a t-Ideal of $\mathfrak{G}_\gamma$.

Let now $\mathfrak{a} := \langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle_{\mathfrak{G}}$ be a finitely generated d-ideal of $\mathfrak{G}$ and suppose

$$\sigma \Big|_{\mathfrak{G}} \mathfrak{a} \cdot \tau \implies \sigma \Big|_{\mathfrak{G}} \gamma \cdot \tau .$$

We consider the integral part $\mathfrak{G}^*$ of $\mathbf{Q}\,[\alpha_1, \alpha_2, \ldots, \alpha_n, \gamma]$, and here in particular the d-ideal $\mathfrak{a}^* := \langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle^*$.

On the one hand, $\mathfrak{a}^*$ is a t-ideal in $\mathfrak{G}^*$ and on the other hand each pair α^*, $\beta^* \in G^*$ satisfies

$$\alpha^* \Big|_{\mathfrak{G}} \beta^* \implies \alpha^* \Big|_{\mathfrak{G}^*} \beta^* ,$$

recall, if the quotient of two elements of $\mathfrak{G}^*$ belongs to G, then this quotient is even contained in G^*.

Consequently γ belongs to $\mathfrak{a}^*$, whence it is representable – even – in $\mathfrak{G}^*$ by a *linear combination* $\sum \alpha_i \ (1 \le i \le n)$.

W. r. t. the great significance of t-ideals we remark that Clifford was the first to work with finitely generated v-ideals in arbitrary commutative monoids in [93], and that Lorenzen was the one who exhibited the notion of a t-ideal when studying ideal theory of commutative cancellative monoids in [275].

But in spite of this, for a long time t-ideals were not respected adequately, as is emphasized by Aubert in his article [41] on ideals of finite character.

That things have changed should be cleared by the series of "t-papers" mentioned in the introduction and in addition by the preceding chapter on factorial rings.

Finally : v-ideals admit a non commutative version by defined by the equivalence $a \,|\, b :\Longleftrightarrow b \in SaS$ and

$$\langle A \rangle_v := \{c \;\Big|\; s \,|\, u\,A\,v \Longrightarrow s \,|\, ucv\} .$$

The concrete relevance of v-ideals was already discussed.

The abstract relevance of v-ideals stems from $\langle a \rangle_v = S \cdot a \cdot S$ and the fact that the v-ideal semigroup is a homomorphic image of each semigroup of ideals satisfying the v-implication.

OBSERVE: If $\star$ is an ideal operator of the described type then $\langle A\rangle_\star \longmapsto \langle A\rangle_v$ provides a function and thereby a homomorphism, since from $\langle A\rangle_\star = \langle B\rangle_\star$ it results:

$$\begin{aligned} s \,\Big|\, uAv \;&\Longrightarrow\; \langle u\rangle_\star \circ \langle A\rangle_\star \circ \langle v\rangle_\star \subseteq \langle s\rangle_\star \\ &\Longrightarrow\; \langle u\rangle_\star \circ \langle B\rangle_\star \circ \langle v\rangle_\star \subseteq \langle s\rangle_\star \Longrightarrow s \,\Big|\, uBv\,. \end{aligned}$$

SUMMARIZING: In any monoid ideal arithmetic strongly depends on its v-ideal arithmetic.

Chapter 5

Algebraic m-Lattices

5.1 The Notion

5. 1. 1 Definition. Let $(L, \leq)$ be a complete lattice. $a \in V$ *is called compact* if

$$a \leq \bigvee b_i \ \ (i \in I) \implies a \leq b_{i_1} \vee \ldots \vee b_{i_n} \\ (i_k \in I, 1 \leq k \leq n).$$

5. 1. 2 Definition. Let $(L, \leq)$ be a complete lattice. Then $(L, \leq)$ is called *algebraic*, if any $b \in L$ is some $\bigvee a_i \ \ (i \in I)$ with compact elements $a_i \in V$.

Most classical models are for instance the lattice of all subspaces of some linear space, the lattice of all filters of some poset or some semi-lattice, and, of course, the lattice of all ideals of some monoid or of some ring. But also, of course any powerset lattice is algebraic, too.

This in mind we denote the elements of algebraic lattices by capitals and reserve lower case letters for special – selected – elements, representing *principal ideals*

Furthermore remembering that concrete ideal theory is the back ground of abstract ideal theory, we denote $\leq$ by $\subseteq$ and

$$\begin{aligned} \sum A_i \ \ (i \in I) &:= \bigvee A_i \ \ (i \in I) \\ \bigcap A_i \ \ (i \in I) &:= \bigwedge A_i \ \ (i \in I). \end{aligned}$$

Symptomatic is the lattice of all ideals of a $\vee$-semi-lattice .

FOR: Let $\mathfrak{L}$ be an algebraic lattice. Obviously, together with any pair a, b also the *sum* of this pair is compact. Associate now with any A the set $\phi\,(A)$ of all compact elements, contained in A. Then it is easily checked that this leads to a $\sum$ and $\bigcap$-respecting *bijection.*

Let $\mathfrak{A}$ be an algebraic lattice. Then again and again the relation

$$A \succeq B :\Longleftrightarrow (A \supseteq X \supseteq B \Rightarrow A = X \vee X = B)$$

does play a technical role. Hence, we introduce this relation explicitly again, although it was defined already in the above chapter on posets and lattices. As usual $A \succ B$ will mean, of course, $A \succeq B$ & $A \neq B$.

5. 1. 3 Definition. Let $\mathfrak{A} = (\mathcal{A}, \Sigma, \cap)$ be an algebraic lattice. Then $\mathfrak{A}$ is called an *algebraic multiplicative lattice* , if on $\mathcal{A}$ in addition some associative multiplication is defined,, satisfying:

$$\begin{aligned} 1 \cdot A &= A = A \cdot 1 \\ \text{and} \qquad X \cdot (\textstyle\sum A_i) \cdot Y &= \textstyle\sum (X A_i Y) \quad (i \in I). \end{aligned}$$

AGAIN: The most classical <u>A</u>lgebraic <u>M</u>ultiplicative <u>L</u>attice, in the sequel abbreviated by AML, is the lattice of all ideals of some commutative ring with identity 1.

5. 1. 4 Definition. $D \in \mathcal{A}$ is called a *left divisor* of C, symbolized by $D \big|_{\ell} C$, if $C = DX \ \ (\exists\, X)$.

D is called a *left divisor* of $\mathfrak{A}$ if D is a left divisor of all elements $C \in \mathcal{A}$ below D .

Finally we call D a *divisor*, if D satisfies the implication:

$$D \supseteq C \implies D \big|_{\ell} C \ \& \ D \big|_{r} C\,.$$

In this case we write $D \big| C$.

5. 1. 5 Definition. Let $\mathfrak{A}$ be an AML. Then $\mathfrak{A}$ is called *left divisor-AML,* abbreviated LD-AML if there exists some *basis* $\mathcal{A}_0$ consisting of compact left divisors such that any A is a sum of elements of $\mathcal{A}_0$.

Consequently $\mathfrak{A}$ is called a *divisor AML,* abbreviated D-AML, if it even contains a basis $\mathcal{A}_0$ consisting of compact *divisors*, that is an $\mathcal{A}_0$ of elements a satisfying the implication $a \supseteq B \Longrightarrow B = aX = Ya \ \ (\exists X, Y)$.

If this is the case we keep some basis of this type fixed and denote its elements by lower case Roman letters.

RECALL that 0 is generated by the empty set of generators.

Let $\mathfrak{A}$ be an AML with $\mathcal{A}_0$ consisting of arbitrary compact generators. If in addition $\mathcal{A}_0$ is multiplicatively closed we call $\mathfrak{A}$ an *ideal structure.*

If moreover all elements of $\mathcal{A}_0$ are even left divisors or divisors, respectively, we call $\mathfrak{A}$ a *left divisor AML,* briefly an LD-AML or a *divisor semigroup,* briefly a D-AML, respectively.

If finally $\mathfrak{A}$ is generated by a monoid of compact divisors we call $\mathfrak{A}$ an ideal divisor monoid, for short an IDM.

Lastly we call $\mathfrak{A}$ *integer,* if all generators $x \neq 0$ satisfy:

$$\begin{aligned} x \cdot A = x \cdot B \ &\Longleftrightarrow \ A = B \\ &\Longleftrightarrow \ A \cdot x = B \cdot x\,. \end{aligned}$$

It is nearly obvious that ideal semigroups may be considered as semigroups of ideals $(\mathcal{A}_0, \cdot)$, define for $A \subseteq \mathcal{A}_0$

$$\langle A \rangle \ := \ \{x \,\big|\, x \geq \textstyle\sum a \ \ (a \in A)\}\,,$$

and by definition these ideals are of finite character.

On the other hand the semigroups of v-ideals, need not have the FC-property. Consequently we have to distinguish between *ideal semigroups* and *semigroups of ideals.*

Prototype of an integral ideal semigroup is, of course, the d-ideal semigroup of the integral domain, but also the t-ideal semigroup of the *ℓ-group cone* extended by 0 or more generally of the cancellative d-semigroup extended by a zero element 0, satisfy the conditions of an integral ideal semigroup.

Finally we emphasize that two elements A, B are called *orthogonal,* also *relatively prime,* if $A + B = 1$.

We finish this short introduction by two central notions:

5. 1. 6 Definition. An AML is called noetherian, equivalently is said to have the Noether property, if

(N) Any element is sum of finitely many generators.

An AML is called *archimedean* if it has the archimedean property

(A) $$A^n \supseteq B \;\; (\forall n \in \mathbf{N}) \Longrightarrow AB = B = BA\,.$$

5.2 Examples

5. 2. 1 Example. *Define on* $\{1, u, a, 0\}$ *a lattice order by putting* $1 \leq u \leq a \leq 0$ *and a multiplication via* $1x = x = x1$, $0x = 0 = x0$, $u^2 = u$, $ua = a$, $au = a^2 = 0$. *Then all elements are left divisors, but u is no right divisor.*

5. 2. 2 Example. *Define on* $\{1, u, a, b, 0\}$ *a lattice order by putting* $1 \leq u \leq a \leq 0$ & $1 \leq u \leq b \leq 0$ *and a multiplication via* $1x = x = x1$, $0x = 0 = x0$, $u^2 = u, ua = aub = b, au = ab = ba = bu = 0$. *Then all elements are left divisors, but u is no right divisor, and it holds:* $(a + b)u = uu = u$, *but* $au \neq a$.

5. 2. 3 Example. *Define on* $\{1, u, v, w, 0\}$ *a multiplication by* $1 \cdot x = x = x \cdot 1, u^2 = u, uv = w, vu = v^2 = vw = 0$ *and consider the set of Rees ideals. This is in particular a distributive lattice, generated by* $\{\langle 1\rangle, \langle u\rangle, \langle v\rangle, \langle 0\rangle\}$. *Here* $\langle u\rangle$ *is a left but no right divisor while* $\langle v\rangle$ *is a right but no left divisor.*

5. 2. 4 Example. *Consider the semigroup* $\mathfrak{S}$ *of pairs* $(a\,|\,b)$ *of non negative numbers* w.r.t. $(a\,|\,b) \circ (c\,|\,d) := (a + c\,|\,2^c b + d)$. *It is not difficult to verify that right divisors are (also) left divisors whereas the converse need not hold.*

This means that $S(a\,|\,b)S$ *is always equal to* $(a\,|\,b)S$. *Consequently all principal ideals are left divisors, but not necessarily also right divisors of this lattice distributive Rees ideal structure.*

5. 2. 5 Example. *Put in* $\mathbf{R}^2$ $(a,b) \subset (c,d)$ *iff* $b < d$. *Then*

$$\begin{aligned} M := \quad & \Big\{(0,0),(0,\frac{1}{2}),(0,\frac{3}{4}),\ldots, \\ & (0,\frac{2^n-1}{2^n}),(0,1),(-1,2),(+1,2),(0,3)\Big\}. \end{aligned}$$

is a complete algebraic lattice, satisfying

$$x \cap \textstyle\sum_{i\in I} a_i \;=\; \textstyle\sum_{i\in I}(x\cap a_i)\,,$$

(that is an AML w.r.t. $\cap$*), and the elements* $a := (-1,2)$ *and* $b := (+1,2)$ *are compact, whereas* $a \cap b = (0{,}1)$ *fails to be compact.*

5.3 Arithmetics

Throughout this chapter $\mathfrak{A}$ will denote at least an arbitrary AML. Elements of $\mathcal{A}$ in general are symbolized by capital Roman letters, elements symbolized by lower case Roman letters are always tacitly supposed to be some compact generator. This means that each $A \in \mathcal{A}$ is of type $\sum_{i\in I} a_i$ and thereby in particular:

$$(A \subseteq B) \iff (x \subseteq A \Rightarrow x \subseteq B)\ . \tag{5.3}$$

First of all we collect some $(\cdot\,,\subseteq)$-rules, however, on the grounds of duality we restrict our considerations to one side only.

$$\begin{aligned} A \subseteq B \implies & B = B + A \\ \implies & X\cdot B = X\cdot(B+A) \\ \implies & X\cdot B = X\cdot B + X\cdot A \\ \implies & X\cdot A \subseteq X\cdot B\,. \end{aligned} \tag{5.4}$$

Because $X \subseteq 1$ this implies

$$X\cdot A \;\subseteq\; A\,. \tag{5.5}$$

$$\begin{aligned} A + BC \;&=\; A + A\cdot C + B\cdot C \\ &=\; A + (A+B)\cdot C\,. \end{aligned} \tag{5.6}$$

So by induction we get:

$$A + B_i \ (1 \le i \le n) \ = \ 1 \Longrightarrow A + \prod_1^n B_i \ = 1\,. \tag{5.7}$$

$$\begin{aligned} A + BC \ &\supseteq \ AA + AC + BA + BC \\ &= \ (A+B)\cdot(A+C)\,. \end{aligned} \tag{5.8}$$

In particular the preceding lemma leads by induction to

$$A + B^n \ \supseteq \ (A+B)^n\,. \tag{5.9}$$

Putting $A \perp B :\Longleftrightarrow A + B = 1$, equation (5.8) provides immediately

$$A \supseteq BC \ \& \ A \perp C \Longrightarrow A \supseteq B\,. \tag{5.10}$$

Furthermore, $AB = BA \Longrightarrow AB \supseteq (A+B)(A \cap B)$. Hence we get

$$AB = BA \ \& \ A \perp B \Longrightarrow AB = A \cap B\,. \tag{5.11}$$

As a divisor criterion we formulate:

$$A \,\Big|\, B \Longleftrightarrow A(A * B) = A \cap B\,. \tag{5.12}$$

Again, we say that A *covers* B, in symbols $A \succ B$, if A is different from B and $A \supset X \supseteq B \Longrightarrow X = B$. We write $A \succeq B$ if no element lies strictly between A and B, that is if $A = B$ or $A \succ B$. By definition, for instance, the maximal elements cover the identity element 1.

Apart from multiplication, taken as fundamental operation, in the following we will be concerned above all with *residuation* which reflects the forming of *quotient ideals*, f. i. in rings.

5. 3. 1 Definition. Let $A, B \in \mathcal{A}$. By the *right quotient*, or synonymously *right residual* of A in B we mean the element

$$A * B \ := \ \textstyle\sum_{i \in I} x_i \quad (A \cdot x_i \subseteq B)\,.$$

Right-left dually the element $B : A$ is defined.

As immediate consequences we get:

$$A \supseteq B \ \Longleftrightarrow \ B * A = 1 \tag{R1}$$

(R2)
$$A * B = (A + B) * B = A * (A \cap B)$$

(R3)
$$A * B \supseteq A * AB \supseteq B$$

(R4)
$$A, B \subseteq A : (B * A),$$

and their right-left dual versions. Furthermore we get :

(5.17)
$$(\textstyle\sum A_i) * B = \bigcap (A_i * B) \quad (i \in I).$$

PROOF.
$$\begin{aligned} & x \subseteq (\textstyle\sum A_i) * B \\ \Longleftrightarrow\ & (\textstyle\sum A_i) \cdot x \subseteq B \\ \Longleftrightarrow\ & \textstyle\sum (A_i \cdot x) \subseteq B \\ \Longleftrightarrow\ & A_i \cdot x \subseteq B \ (\forall i \in I) \\ \Longleftrightarrow\ & x \subseteq A_i * B \\ \Longleftrightarrow\ & x \subseteq \bigcap (A_i * B) \qquad (i \in I). \end{aligned}$$
□

(5.18)
$$A * \bigcap B_i = \bigcap (A * B_i) \qquad (i \in I).$$

PROOF.
$$\begin{aligned} & x \subseteq A * \bigcap B_i \\ \Longleftrightarrow\ & A \cdot x \subseteq \bigcap B_i \\ \Longleftrightarrow\ & A \cdot x \subseteq B_i \qquad \forall i \in I) \\ \Longleftrightarrow\ & x \subseteq A * B_i \\ \Longleftrightarrow\ & x \subseteq \bigcap (A * B_i) \qquad (i \in I). \end{aligned}$$
□

(5.19)
$$A \subseteq B \Longrightarrow C * A \subseteq C * B.$$

PROOF.
$$\begin{aligned} A \subseteq B & \Longrightarrow A = A \cap B \\ & \Longrightarrow C * A = C * A \cap C * B \\ & \Longrightarrow C * A \subseteq C * B \end{aligned}$$

and
$$\begin{aligned} A \subseteq B & \Longrightarrow B = B + A \\ & \Longrightarrow B * C = (B + A) * C \\ & \Longrightarrow B * C = B * C \cap A * C \ \ (5.17) \\ & \Longrightarrow A * C \supseteq B * C. \end{aligned}$$
□

(5.20)
$$(A \cap B) * (A \cap C) \supseteq B * C \subseteq (A + B) * (A + C).$$

PROOF.
$$\begin{aligned}(A\cap B)*(A\cap C) &= (A\cap B)*C \qquad (5.18)\\ &\supseteq B*C\\ &\subseteq B*(A+C)\\ &= (A+B)*(A+C).\end{aligned}$$
□

(5.21)
$$AB*C = B*(A*C)$$

PROOF.
$$\begin{aligned}x\subseteq AB*C &\iff A\cdot(B\cdot x)\subseteq C\\ &\iff (B\cdot x)\subseteq A*C\\ &\iff x\subseteq B*(A*C)\,.\end{aligned}$$
□

(5.22)
$$A*(B:C) = (A*B):C\,.$$

PROOF.
$$\begin{aligned}x\subseteq A*(B:C) &\iff A\cdot x\subseteq B:C\\ &\iff A\cdot x\cdot C\subseteq B\\ &\iff x\cdot C\subseteq A*B\\ &\iff x\subseteq (A*B):C\,.\end{aligned}$$
□

5. 3. 2 Lemma. *Let* $A=\sum_{i\in I}a_i$ *and* $B=\sum_{j\in J}b_j$. *Then*

$$\begin{aligned}A\cdot B &= \sum(a_i\cdot b_j)\ \ ((i,j)\in I\times J)\,,\\ A+B &= \sum(a_i+b_j)\ \ ((i,j)\in I\times J)\\ \textit{and}\quad A\cap B &= \sum((a_{i_1}+\ldots+a_{i_m})\cap(b_{j_1}+\ldots+b_{j_n}))\\ &\qquad (i_1,\ldots,i_m\in I\,,\ j_1,\ldots,j_n\in J)\,.\end{aligned}$$

PROOF. $A\cap B\supseteq\sum\ldots$ is evident and $x\subseteq A\cap B$ implies the existence of some $a_1,\ldots,a_m\subseteq A$, $b_1,\ldots,b_n\subseteq B$ satisfying:

$$\begin{aligned}x\subseteq A\cap B &\implies x\subseteq A\ \&\ x\subseteq B\\ &\implies x\subseteq a_1+\ldots+a_m\\ &\quad\ \&\quad x\subseteq b_1+\ldots+b_n\\ &\implies x\subseteq(a_1+\ldots+a_m)\cap(b_1+\ldots+b_n)\\ &\implies x\subseteq\sum\ldots\,.\end{aligned}$$
□

Recall: An AML is called *lattice distributive,* briefly *distributive,* if its lattice satisfies

(D)
$$A\cap(B+C) = (A\cap B)+(A\cap C).$$

5. 3. 3 Lemma. *If* (D) *is fulfilled for all finitely generated elements* A, B, C, *then it follows even in general*

$$A \cap \sum B_i \;=\; \sum (A \cap B_i) \;\; (i \in I). \tag{5.24}$$

PROOF. The first assertion follows by 5.3.2, the second by :

$$\begin{aligned}
& x \subseteq A \cap (B + C) \\
\Longrightarrow \quad & x \subseteq (a_1 \cap b_1) + (a_1 \cap b_2) + \ldots + (a_\ell \cap b_m) \\
& \quad + \; (a_1 \cap c_1) + (a_1 \cap c_2) + \ldots + (a_\ell \cap c_n) \\
& \quad \subseteq (A \cap B) + (A \cap C).
\end{aligned}$$

Finally we get: $A \cap \sum B_i \supseteq \sum (A \cap B_i)$ is evident and $x \subseteq A \cap \sum B_i$ implies the inclusion $x \subseteq A \;\&\; x \subseteq \sum B_i$ and thereby $x \subseteq A \;\&\; x \subseteq B_{i_1} + \ldots + B_{i_n}$, which leads to $x \subseteq (A \cap B_{i_1}) + \ldots + (A \cap B_{i_n}) \subseteq \sum (A \cap B_i)$ $(i \in I)$. □

As a most important consequence of (D) we next point out:

5. 3. 4 Lemma. *Let* $\mathfrak{A}$ *be an arbitrary AML. Then it holds:*

$$(A + B)U = U \implies BU : A = B : A\,. \tag{5.25}$$

PROOF.

$$\begin{aligned}
(A + B)U &= A + B \\
&\Longrightarrow \\
BU : A &= BU : (A + BU) \\
&\supseteq BU : (A + B) \\
&= BU : (A + B)U \\
&= (BU : U) : (A + B) \\
&\supseteq B : (A + B) \\
&= B : A\,.
\end{aligned}$$

□

5. 3. 5 Lemma. *Let* $\mathfrak{A}$ *be a lattice distributive AML and let* A *be a right divisor. Then*

$$(A + B)U = A + B \implies BU = B\,.$$

PROOF.

$$\begin{array}{rcll}
A + \underline{BU} & = & A + (A+B)U & \\
& = & A + \underline{B} & \\
& \& & & \\
A \cap \underline{BU} & = & (BU : A)A & \\
& = & (B : A)A & \text{(see above)} \\
& = & A \cap \underline{B} & \\
& \rightsquigarrow & & \\
BU & = & B &
\end{array}$$

this implies $BU = B$ by distributivity, cf. 3.3.17. □

5. 3. 6 Corollary. *Under the assumption of the preceding lemma $A = a_1 + \ldots + a_n$ implies $AU = A \supseteq B \Longrightarrow BU = B$ – by induction.*

5. 3. 7 Corollary. *If $\mathfrak{A}$ is lattice distributive and generated by right divisors, then it holds*

$$(a_1 + \ldots + a_n) \cdot U = (a_1 + \ldots + a_n) \supseteq B \Longrightarrow BU = B\,.$$

Observe

$$(a_1 + \ldots + a_n) \supseteq B \Longleftrightarrow (a_1 + \ldots + a_n) = (B + a_1 + \ldots + a_n).$$

The question arises whether this is true in general. To this end we consider the filters $(x \geq y \in F \Longrightarrow x \in F)$ of $(\mathbf{Q}^{\geq 0}, \min, +)$. Here we get $\mathbf{Q}^+ + \mathbf{Q}^+ = \mathbf{Q}^+$ but $\langle 1 \rangle \supset \langle 1 \rangle + \mathbf{Q}^{\vdots} = \{x | x \geq 1\}$. Hence the rule of 5.3.7 does not hold in general.

Next we present

5. 3. 8 The power lemma. *Any AML $\mathfrak{A}$ satisfies*

$$\begin{array}{rcl}
A^m \supseteq B \supseteq A^{m+p} & \& & A^n \succeq A^{n+1} \\
& & (\forall n : \ m \leq n \leq m+p-1) \\
& \Longrightarrow & \\
B & = & A^{m+\ell} \ \ (\exists \ell \leq p)\,.
\end{array} \tag{5.26}$$

PROOF. Let $A^k \supseteq B$ & $A^{k+1} \not\supseteq B$ & $B \supseteq A^{k+\ell}$ be satisfied. Then we obtain $B + A^{k+1} = A^k$ and thereby:

$$\begin{array}{rcll} B & = & B + A^k \cdot A^\ell & \\ & = & B + A^{k+1} \cdot A^{\ell-1} & \\ & \overset{(5.6)}{=} & B + (B + A^{k+1})A^{\ell-1} & \\ & = & B + A^k \cdot A^{\ell-1} & \\ & = & B + A^k & \text{(by induction)} \\ & = & A^k & \text{(by assumption).} \end{array}$$

□

Finally we give

5. 3. 9 The Divisor Lemma. *Let $\mathfrak{A}$ be a complete, commutative, not necessarily algebraic multiplicative lattice.*

Let moreover $A \supseteq B \supset A(A * B)$ and $S \supseteq A(A * B)$ and let $B * S$ be a divisor. Then it follows $(B * S)^n \Big| B$ $(\forall n \in \mathbf{N})$.

PROOF. Put $A * B := X$. Then $S \supseteq AX$ implies

(5.27) $$Y := B * S \supseteq X * S \supseteq X * AX \supseteq A \supseteq B\,,$$

which leads to

(E(1)) $$Y^1 \Big| A \quad \& \quad Y^1 \Big| B\,.$$

Assume now that

(E(n)) $$Y^n \Big| A \text{ and } Y^n \Big| B\,.$$

is already proven. Then putting

$$A_1 := Y^n * A \text{ and } B_1 := Y^n * B$$

we obtain
$$\begin{array}{rcl} A_1 * B_1 & = & (Y^n * A) * (Y^n * B) \\ & = & A * B \\ & = & X \end{array}$$

and thereby
$$B_1 \supseteq A_1 \cdot X.$$

Define now:
$$S_1 := Y^n * S\,.$$

Then it results:
$$\begin{aligned} S_1 &\supseteq Y^n * A \cdot X \\ &\supseteq (Y^n * A) \cdot X \\ &= A_1 \cdot X \\ &= A_1 \cdot (A_1 * B_1) \\ &\& \\ B_1 * S_1 &= (Y^n * B) * (Y^n * S) \\ &= B * S = Y\,. \end{aligned}$$

So, by (5.27) remains valid even if we replace A by A_1 and B by B_1, whence

$$Y \Big| A_1 \ \rightsquigarrow\ Y \Big| B_1$$

that is
$$Y \Big| Y^n * A \ \rightsquigarrow\ Y \Big| Y^n * B$$

meaning

(E($n+1$))
$$Y^{n+1}|A \ \ \&\ \ Y^{n+1}\Big| B\,.$$

This completes the proof. □

5. 3. 10 Corollary. *Assume* $P \supseteq A(A * b)$ & $b * bP = P$. *Then* $P^n \supseteq A\ \ (\forall\, n \in \mathbf{N})$.

After this excursion on general arithmetic we now turn to certain special elements.

5.4 Prime Elements and primary Elements

Recall: $D \in \mathcal{A}$ is called a *left divisor* of C, by symbols $D \,\Big|_\ell\, C$, if $C = DX\ \ (\exists\, X)$. D is called a *left divisor* of $\mathfrak{A}$ if D is a left divisor of all elements contained in D. Dually right divisors are defined.

D is called a *divisor* if D is both, a left- and a right-divisor, symbolized by $D \Big| C$.

5. 4. 1 Lemma. *Left divisors $D \in \mathcal{A}$ satisfy*

$$D(D * C) \;=\; D \cap C\,.$$

PROOF. By assumption $D \cap C = DX \;\; (\exists\, X)$ with $X \subseteq D * C$, and this implies $D(D * C) \subseteq D \cap C = DX \subseteq D(D * C)$. □

Again we emphasize that the basic structure under consideration is an AML, and again we recall that by definition $\mathfrak{A}$ is right-left dual, meaning in particular that $\mathfrak{A}$ is $*\,,\,:$ - dual.

5. 4. 2 Definition. Let $\mathfrak{A}$ be an AML. An element $P \in \mathcal{A}$ different from 1 is called *prime* if

$$ab \subseteq P \;\Longrightarrow\; a \subseteq P \vee b \subseteq P\,,$$

and $Q \in \mathcal{A}$ different from 1 is called *primary* iff

$$\begin{array}{c} ab \;\subseteq\; Q \\ \Longrightarrow \\ a \subseteq Q \vee b^n \subseteq Q \;\; (\exists\, n \in \mathbf{N}) \quad \& \quad b \subseteq Q \vee a^n \subseteq Q \;\; (\exists\, n \in \mathbf{N})\,. \end{array}$$

If moreover Q satisfies $x^n \subseteq Q \Rightarrow x \subseteq P$ then Q is called more precisely *P-primary.*

Finally we call $P \in \mathcal{A}$ *completely prime* if each P^n is primary.

Hence P is completely prime iff P is a prime element satisfying in addition:

$$\begin{array}{c} P^n \;\supseteq\; AB \\ \Longrightarrow \\ P^n \supseteq A \vee P \supseteq B \quad \& \quad P^n \supseteq B \vee P \supseteq A\,. \end{array}$$

5. 4. 3 Lemma. *P is prime iff*

$$P \supseteq AB \;\Longrightarrow\; P \supseteq A \vee P \supseteq B\,.$$

Therefore the prime property is independent from the distinguished basis.

PROOF. $A = \sum_1^m a_i \;\&\; B = \sum_1^n b_j \Longrightarrow AB = \sum_{1,1}^{m,n} a_i\, b_j$ (5.3.2). Suppose now $P \supseteq AB \;\&\; P \not\supseteq A$ with prime element P. Then there exists some

${a_i}' \subseteq A$ with $P \not\supseteq {a_i}'$ & $P \supseteq {a_i}'b_j \quad (\forall\, j \in J)$. This leads to $P \supseteq b_j\,(j \in J)$ and thereby to $P \supseteq B$. – The rest follows *a fortiori.* □

5. 4. 4 Definition. Let $\mathfrak{A}$ be an AML. By the *radical* of $A \in \mathcal{A}$ we mean

$$\begin{aligned}\operatorname{Rad} A \ :=\ & \textstyle\sum_{i\in I} x_i \quad ({x_i}^{n_i} \subseteq A)\\ & (\exists\, x_i \in \mathcal{A}_0\,,\ n_i \in \mathbf{N}).\end{aligned}$$

By definition it evidently results $A \supseteq B \Longrightarrow \operatorname{Rad} A \supseteq \operatorname{Rad} B$.

5. 4. 5 Lemma. *If $X \subseteq \operatorname{Rad} A$ is compact then $X^n \subseteq A$ $(\exists\, n \in \mathbf{N})$.*
Hence the radical property is independent from the distinguished basis.

PROOF. It holds $a^p\,,\ b^q \subseteq A \Longrightarrow (a+b)^{p+q} \subseteq A$. Hence

$$\begin{aligned} x \subseteq \operatorname{Rad} A \ &\Longrightarrow\ x \subseteq \textstyle\sum_1^k a_i \ \text{ with } ({a_i}^{\ell_i} \subseteq A\ \ (\exists\, \ell_i))\\ &\Longrightarrow\ x^n \subseteq A\ \ (\exists\, n \in \mathbf{N})\,.\end{aligned}$$

which completes the proof. □

The preceding lemma provides

5. 4. 6 Lemma. *Q is primary iff Q is different from 1 and satisfies in addition the implication:*

$$\begin{gathered} Q \ \supseteq\ ab \\ \Longrightarrow \\ Q \supseteq a \vee \operatorname{Rad} Q \supseteq b \quad \& \quad Q \supseteq b \vee \operatorname{Rad} Q \supseteq a \end{gathered}$$

or respectively – cf. the proof of 5.4.3 – the implication:

$$\begin{gathered} Q \ \supseteq\ AB \\ \Longrightarrow \\ Q \supseteq A \vee \operatorname{Rad} Q \supseteq B \quad \& \quad Q \supseteq B \vee \operatorname{Rad} Q \supseteq A \end{gathered}$$

Consequently the primary property is independent from the fixed basis.

Furthermore we get:

5. 4. 7 Lemma. *If $\mathfrak{A}$ is even an ideal semigroup and Q is primary with $\operatorname{Rad} Q = P$ then P is prime.*

PROOF. $P \supseteq xy \;\&\; P \not\supseteq x \Longrightarrow Q \supseteq y(xy)^{n-1} \Longrightarrow P \supseteq y \vee Q \supseteq (xy)^{n-1}$. Hence $P \supseteq xy \;\&\; P \not\supseteq x \Longrightarrow P \supseteq y$, since the opposite would lead to a contradiction. □

The subsequent lemma will play a key role in various proofs.

5. 4. 8 Lemma. *Suppose $A \cdot X \subset b$. Then there exists a maximal $P \supseteq X$ satisfying $b \cdot P \subset b$ and this P is prime and satisfies in addition $b * bP = P$.*

PROOF. Let X_i $(i \in I)$ be an ascending $\supseteq$-chain satisfying $X_i \supseteq X$ and $b \cdot X_i \subset b$. Then we get $\sum_{i \in I} b \cdot X_i = b \cdot \sum_{i \in I} X_i \subset b$. Therefore the ascending chain X_i $(i \in I)$ is bounded by $\sum_{i \in I} X_i$. So by ZORN there exists a maximal P with $P \supseteq X$ and $b \cdot P \subset b$.

Assume now $P \supseteq U \cdot V$ but $P \not\supseteq U, V$. Then it follows

$$\begin{aligned} bP &\supseteq b\,(U+P)\cdot(V+P) \\ &= b\,(V+P) = b\,. \end{aligned}$$

Hence P is prime.

It remains to show $b * bP = P$. Here first we get $b * bP =: Y \neq 1$ because $b * bP = 1 \Longrightarrow b = bP$. But this means $1 \neq Y \supseteq P$ and thereby $Y = P$ since P was chosen maximal w. r. t. $C \supseteq X$ and $b \supset b \cdot C$. □

5. 4. 9 Lemma. *Let $\mathfrak{A}$ be an AML with compact identity 1 and $A \neq 1$. Then there exists a maximal prime element $P \supseteq A$ and among all A containing prime elements at least one minimal prime element P over A.*

PROOF. The first assertion results from 5.4.8, the second since the intersection of a chain of prime elements is again prime. □

As usual we will call *maximal* the *successors* of 1. Obviously maximal elements are prime. Furthermore we will call minimal prime those elements which are minimal in the set of prime elements.

5.5 Residues

The classical *residue classes* in rings are reflected as residue elements in the structure of an AML, where they play a similar role like in ring theory.

5. 5. 1 Lemma. *Let A be an element of an AML $\mathfrak{A}$. Then $\phi_A : X \longmapsto A+X =: \overline{X}$ provides a $\sum$-respecting homomorphism with $\overline{X} \circ \overline{Y} := A+XY$ satisfying in addition*

$$A_i \supseteq A \ (\forall\, i \in I) \implies \phi_x(\textstyle\bigcap_{i\in I} A_i\ ) = \textstyle\bigcap_{i\in I} \phi_x A_i \ .$$

PROOF. According to (5.6) the *operator* ϕ_A provides a multiplicative $\sum$-homomorphism respecting the algebraic property. The rest is evident. □

5. 5. 2 Lemma. *Let $\mathfrak{A}$ be an AML. Then in $\mathfrak{A}/A$ exactly the elements of type $\sum_1^n \overline{c}_i$ are compact and if b and c are compact then $A+b$ equals $A+c$ iff there exists a compact $A_e \subseteq A$ with $A_e + b = A_e + c$.*

PROOF. One part follows *straightforwardly*. The other one by

$$\begin{array}{rcl} A_{e1} + b \supseteq c \ \&\ A_{e2} + c \supseteq b & \implies & (A_{e1} + A_{e2}) + b \supseteq c \\ & \& & (A_{e1} + A_{e2}) + c \supseteq b \\ & \implies & \\ (A_{e1} + A_{e2}) + b & = & (A_{e1} + A_{e2}) + c\,. \end{array}$$ □

In an arbitrary $\mathfrak{A}$ the image of a divisor under $X \longmapsto A + X$ need not be again a divisor, put for instance in the pentagon $x^2 = 0$ and adjoin a new identity. However, it holds:

5. 5. 3 Proposition. *If $\mathfrak{A}$ is lattice modular then divisors "remain" divisors in $\overline{\mathfrak{A}}/A$.*

PROOF. Let D be a divisor in $\mathfrak{A}$ and suppose w.l.o.g. $C \supseteq A$. Applying modularity we get

$$\begin{array}{rcl} \overline{D} \supseteq \overline{C} & \implies & \overline{C} = A + (D \cap C) \\ & \implies & \overline{C} = A + D(D * C) \\ & \implies & \overline{C} = A + (A + D)(A + D * C) \\ & \implies & \overline{C} = \overline{D} \cdot \overline{D * C}\,, \end{array}$$

whence $\overline{D}$ is a divisor of $\overline{\mathfrak{A}}$. □

5. 5. 4 Lemma. *Let $\mathfrak{A}$ be lattice modular and as ideal semigroup be generated by a set $\mathcal{A}_0$ of compact divisors.*

Then in case that the elements $a \neq 0$ of $\mathcal{A}_0$ are cancellable in $\mathfrak{A}$ and that P is prime, $\mathfrak{A}_0/P =: \overline{\mathfrak{A}}_0$ is integral (w.r.t. $\overline{\mathcal{A}}_0$).

PROOF. Let $\overline{a} \neq \overline{P} = \overline{0}$. Then $\overline{a} \cdot \overline{x} = \overline{0}$ implies immediately $\overline{x} = \overline{0}$, and in addition we get in case of $\overline{a} \cdot \overline{X} \neq \overline{0}$, that is in particular if $a \not\subseteq P$

$$\begin{array}{rrcl}
 & \overline{a} \cdot \overline{X} & = & \overline{a} \cdot \overline{Y} \\
\Longrightarrow & P + aX & = & P + aY \\
\Longrightarrow & a \cap (P + aX) & = & a \cap (P + aY) \\
\Longrightarrow & (a \cap P) + aX & \overset{\text{(MO)}}{=} & (a \cap P) + aY \\
\Longrightarrow & a(a * P) + aX & = & a(a * P) + aY \\
\Longrightarrow & aP + aX & = & aP + aY \\
\Longrightarrow & a(P + X) & = & a(P + Y) \\
\Longrightarrow & P + X & = & P + Y \\
\Longrightarrow & \overline{X} & = & \overline{Y}\,.
\end{array}$$

□

Finally

5. 5. 5 Lemma. *Let $\mathfrak{A}$ be lattice modular and as ideal semigroup be generated by a set $\mathcal{A}_0$ of compact divisors, and let moreover $\mathfrak{A}$ satisfy*

$$au = a \Longrightarrow \exists u \perp u^* : au^* = 0$$ [1)]

Then $P + au = P + a \Longrightarrow P + u = P + 1$.

PROOF. By assumption we obtain:

$$\begin{array}{rrcl}
 & \overline{a} \cdot \overline{u} & = & \overline{a} \\
\Longrightarrow & P + a & = & P + au \\
\overset{\text{(MD)}}{\Longrightarrow} & a & = & (a \cap P) + au) \\
\Longrightarrow & a & = & a(p + u) = as \ \ (s \notin P) \\
\Longrightarrow & P \supseteq as^* & = & 0 \rightsquigarrow P \supseteq s^* \\
\Longrightarrow & P + s & = & P + s^* + s = P + 1 \\
\Longrightarrow & P + u & = & P + 1\,.
\end{array}$$

□

5.6 Localization

As a second most important tool of finding *ideal homomorphisms,* ring theoretists apply the method of *localization* which will now be developed

[1)] This property will play an important role, when studying classical aspects.

for our purposes. However, for the sake of clearness and convenience we will restrict our considerations to commutative ideal semigroups and hence to commutative ideal monoids.

5. 6. 1 Definition. Let $\mathfrak{A}$ be a commutative IDM, $A \in \mathcal{A}$ and S a multiplicatively closed subset of $\mathcal{A}_0$. We define

$$A_S \ := \ \sum_{i\in I} x_i \quad (s_i \cdot x_i \subseteq A \ (\exists s_i \in S)).$$

As is easily verified, the operator S is a closure operator.

5. 6. 2 Proposition. *Let $\mathfrak{A}$ be a commutative ideal monoid and let S be a multiplicatively closed subset of A. Then we obtain*

(L1) $$(A+B)_S \ = \ (A_S+B_S)_S$$

(L2) $$(A\cdot B)_S \ = \ (A_S\cdot B_S)_S$$

(L3) $$(a*B)_S \ = \ a_S * B_S$$

(L4) $$(A\cap B)_S \ = \ A_S \cap B_S$$

(L5) $$(\sum A_i)_S \ = \ (\sum (A_{i\,S}))_S \ \ (i \in I)\,.$$

PROOF. Ad (L1). *A fortiori* we get

$$(A_S+B_S)_S \ \supseteq \ (A+B)_S\,,$$

and it follows for each $x \in \mathcal{A}_0$:

$$\begin{aligned} x \subseteq (A_S+B_S)_S \ &\Longrightarrow \ xs \subseteq A_S + B_S \ \ (\exists\, s \in S) \\ &\Longrightarrow \ \exists : \overline{a}_i \subseteq A_S \ \& \ \overline{b}_j \subseteq B_S \ : \\ &\qquad xs \subseteq \overline{a}_1 + \ldots + \overline{a}_m + \overline{b}_1 + \ldots + \overline{b}_n \\ &\Longrightarrow \ \exists\, t \in S \ : \ a_i \cdot t \subseteq A \ \& \ b_j \cdot t \subseteq B \\ &\qquad \& \ x(st) \subseteq a_1 \cdot t + \ldots + b_n \cdot t \\ &\Longrightarrow \ x \subseteq (A+B)_S\,. \end{aligned}$$

Ad (L2). We proceed in a similar manner as below (L1).

Ad (L3). First suppose $x \subseteq (a*B)_S$. Then there exists an element $s \in S$ with $xs \subseteq a*B$ and thereby with $as\cdot x \subseteq B \subseteq B_S$. If now $a' \subseteq a_S$ it results next with some $t \in S$ in a first step $a' \cdot t \subseteq a$ and hence in a second step $a' \cdot x \cdot (st) \subseteq B$. Thus we get $a' \cdot x \subseteq B_S$ and thereby finally $x \subseteq a_S * B_S$.

Suppose now $x \in a_S * B_S$. Then we get $a_S \cdot x \subseteq B_S$ whence $ax \subseteq B_S$ is satisfied. But this implies $a \cdot xs \subseteq B$ $(\exists s \in S)$ and thereby $x \subseteq (a * B)_S$.

Ad (L4). $A_S \cap B_S \supseteq (A \cap B)_S$ is evident and $x \cdot s \subseteq A$ & $x \cdot t \subseteq B$ implies $x \cdot st \subseteq A \cap B$.

Ad (L5). This follows *straightforwardly* from (L1). □

The formulas just proven have far reaching consequences.

5. 6. 3 Proposition. *Let $\mathfrak{A}$ be a commutative IDM and S a multiplicatively closed subset of compact divisors. Then by*

$$\begin{aligned} A_S \circ B_S &:= (A \cdot B)_S \\ A_S \oplus B_S &:= (A + B)_S \end{aligned}$$

two operations on the set of all A_S are defined such that this set of all A_S forms a commutative IDM which is a homomorphic image of $\mathfrak{A}$ under $\Phi_S : A \longmapsto A_S$.

PROOF. First of all, by 5.6.2, $\circ$ and $\oplus$ don't depend on the arguments $A, B, ...$ of $A_S, B_S, ...$ Hence $\circ$ and $\oplus$ are *functions.*

Furthermore, again on the grounds of 5.6.2, the mapping $A \longmapsto A_S$ provides a homomorphism of $\mathfrak{A}$ on $\mathfrak{A}_S$ w.r.t. $\cdot \longmapsto \circ$ and $+ \longmapsto \oplus$, and by (L4) the intersection in $\mathfrak{A}_S$ is identic with the intersection in $\mathfrak{A}$.

Finally $\sum_S$ acts as $\sum$-operation in this lattice.

Hence Φ_S provides a $\sum$-respecting homomorphism of $\mathfrak{A}$ on $\mathfrak{A}_S$.

We now show that $\mathfrak{A}_S$ is not merely an AML but even a commutative IDM Since $\mathfrak{A}$ is a commutative IDM , compact generators produce compact products whence we may infer:

$$\begin{aligned} x_S \subseteq \textstyle\sum_S (A_{i\,S}) &\Longrightarrow x_S \subseteq (\textstyle\sum A_i)_S \\ &\Longrightarrow x \subseteq (\textstyle\sum A_i)_S \\ &\Longrightarrow xs \subseteq a_1 + ... + a_n \\ &\qquad (\exists\, s \subseteq S\,, a_k \subseteq A_{i_k}\,,\ 1 \leq k \leq n) \\ &\Longrightarrow \forall\, x' \subseteq x_S\ \exists\, t \in S\ : \\ &\qquad x' \cdot t \cdot s \subseteq a_1 + ... + a_n \\ &\Longrightarrow x_S \subseteq (a_1)_S \oplus \ldots \oplus (a_n)_S. \end{aligned}$$

Consequently the set of all x_S forms a set of compact generators of $\mathfrak{A}_S$ and in particular 1_S is compact. Furthermore each x_S is a divisor since

$$\begin{aligned} a_S \supseteq b_S \Longrightarrow b_S &= a_S \cap b_S \\ &= (a \cap b)_S \\ &= (a(a * b))_S \\ &= a_S \circ (a * b)_S \Longrightarrow a_S \Big| b_S \,. \end{aligned}$$

Therefore, recall $x_S \circ y_S = (xy)_S$, $\mathfrak{S}$ is a commutative IDM, generated by $\{x_S\}$. □

5. 6. 4 Proposition. *Let $\mathfrak{A}$ be a commutative IDM and S a multiplicatively closed system of generators. Then each prime element P of $\mathfrak{A}$ is "extended" to a prime P_S of $\mathfrak{A}_S$ and each primary Q of $\mathfrak{A}$ is "extended" to a primary Q_S of $\mathfrak{A}_S$.*

PROOF. $a_S \cdot b_S \subseteq P_S$ implies $a \cdot bs \subseteq P$ $(\exists s \in S)$ from which follows $a \subseteq P \vee bs \subseteq P$ leading to $a_S \subseteq P_S \vee b_S \subseteq P_S$. In an analogous manner we get that Q_S is primary in $\mathfrak{A}_S$ if Q is primary in $\mathfrak{A}$. □

The great importance of the introduced operator results from the fact that ideal identities may be checked by consulting $\mathfrak{A}_S$.

In particular one may restrict to considering the localizations $\mathfrak{A}_S$ where S consists of all s not contained in a given prime element P. To emphasize this, one writes alternatively A_P instead of $A_{\{x \mid x \not\subseteq P\}}$ and calls $\mathfrak{A}_P$ the *localization* of $\mathfrak{A}$ at the place P.

A final Remark. The reader should take into account that a prime element P with $S := \{s \,|\, s \not\subseteq P\}$ satisfies $P_S = P$ on the one hand and that $a_P = 1_P$ holds for all $a \not\subseteq P$ on the other hand, because

$$\begin{aligned} a \subseteq P_S &\Longrightarrow as \subseteq P \;\; (\exists\, s \in S) \\ &\Longrightarrow a \subseteq P \,, \end{aligned}$$

and since $a \not\subseteq P \Longrightarrow 1 \cdot a \subseteq a \;\; (a \in S)$, respectively.

Chapter 6

Krull's Classics

6.1 The Localization Theorem

As far as the author is in the position to judge the method of *localization* was introduced by WOLFGANG KRULL. This method provides a reduction of consideration to special models, namely the components $\mathfrak{A}_P$ of localization, having exactly one maximal prime element.

6. 1. 1 Krull's Localization Lemma. *In a commutative IDM $\mathfrak{A}$ two elements A, B are equal iff $A_M = B_M$ for all maximal elements M.*

PROOF. First of all
$$\begin{aligned} a \subseteq A &\implies a \subseteq A_M = B_M \\ &\implies a \cdot e_M \subseteq B \ \ (e_M \not\subseteq M)\,. \end{aligned}$$

Hence for each maximal element M there exists some e_M with $a \cdot e_M \subseteq B$. We consider $\sum e_M$ (M maximal) and get $\sum e_M = 1$, since in case of $\sum e_M \neq 1$ there would exist some $e_{M'}$ whose maximal M' is not contained in $\sum e_M$. Hence we get
$$a \;=\; a \cdot \sum e_M \subseteq B \ \ (\forall\, a \in A)$$
and thereby $A \subseteq B$. This completes the proof by symmetry. □

Recall again: If P is prime and $S := \{s \mid s \not\subseteq P\}$ then on the one hand it holds $P_S = P$ and on the other hand any $a \not\subseteq P$ satisfies $a_P = 1_P$,

Remark. Considering the ideal structure of $(\mathbf{Z}, +, \cdot)$ as an AML it becomes obvious that the localization lemma acts as a compensation and generalization, respectively, of the fundamental theorem of elementary number theory – in any commutative ring with identity.

6.2 The Kernel of an Element

The *kernel of an element* was introduced by KRULL, see also [163]. It will play a central role in this section. In particular we will exhibit an equivalent of $\ker A = A$ according to GILMER/MOTT [163] and a characterization of unique representability of $\ker A$ which in the special case of commutative rings with identity is again due to KRULL [251].

To begin with some lemmata, again basically due to KRULL.

6. 2. 1 Krull's Separation Lemma. *Let $\mathfrak{A}$ be a commutative IDM and let S be a multiplication closed system of generators. Then there exists a prime element P with*

$$P \supseteq A \quad \& \quad cs \not\subseteq P \ \ (\forall\, s \in S)\,.$$

PROOF. Let P be maximal among all elements B satisfying

$$B \supseteq A \;\&\; s \not\subseteq B \ \ (\forall\, s \in S)\,.$$

Then $a \cdot b \subseteq P$ implies $a \subseteq P \vee b \subseteq P$ since otherwise $P + a \supset P$ and $P+b \supset P$ would follow implying $P \supseteq (P+a)\cdot(P+b)$ with $P+a \supseteq s \in S$, $P + b \supseteq t \in S$. But this would lead to $s \cdot t \subseteq P$, in spite of $st \in S$. $\square$

6. 2. 2 Proposition. *Let $\mathfrak{A}$ be a commutative IDM and let P be minimal prime over A. Then A_P is P-primary on the one hand and equal to the intersection of all A containing P-primary elements of $\mathfrak{A}$.*

PROOF. We start from $S = \{s \,\big|\, s \not\subseteq P\}$. Since $x^n \subseteq A_P \Longrightarrow sx^n \subseteq A \subseteq P$ we get $\operatorname{Rad} A_P \subseteq P$. But $P \subseteq \operatorname{Rad} A_P$ holds as well, for $p \subseteq P$ yields the existence of at least one sp^n $(s \in S)$ in A since otherwise, by 6.2.1, a prime element $P' \neq P$ containing A would exist in which no sp^n is contained. But this contradicts that each minimal prime $P_m \neq P$ over A must contain at least one $s \not\subseteq P$, according to $P_m \not\supseteq P$.

Assume now $xy \subseteq A_P$. This implies $sx \cdot y \subseteq A$ and thereby in the case of $x \not\subseteq \operatorname{Rad} A_P = P$ first of all $sx \notin P$, that is $sx \in S$, whence we get next $y \subseteq A_P$. Hence A_P is P-primary.

Let finally Q be a further P-primary element with $Q \supseteq A$. Then each $x \subseteq A_P$ by definition satisfies $sx \subseteq A$ $(\exists\, s \not\subseteq P)$, whence $sx \subseteq Q$ and consequently $x \subseteq Q$. □

6. 2. 3 Definition. Let $\mathfrak{A}$ be a commutative IDM and $A \in \mathcal{A}$.

By an *isolated primary component of* A we mean any A_P in the sense of 6.2.2. By the *kernel* of A, abbreviated $\ker A$, we mean the intersection of all *isolated primary components* A_P of A.

6. 2. 4 Krull's Kernel Lemma. *Let* $\mathfrak{A}$ *be a commutative IDM and let* $a \subseteq A^* := \ker A$. *Then each* $P \supseteq a * A$ *properly contains at least one prime element* P_m *minimal over* A.

PROOF. Suppose $A^* \supseteq a$ and $P \supseteq a * A$. Then $P \supseteq a * A \supseteq A$ and thereby $P \supseteq P_m$ for at least one P_m, minimal prime over A.

Assume now even $P = P_m$. Then, according to 6.2.2, we would get

$$sa \subseteq A \ (\exists\, s \not\subseteq P) \ \rightsquigarrow \ s \subseteq a * A \subseteq P,$$

a contradiction! □

Now we are in the position to prove

6. 2. 5 Proposition. *In a commutative IDM* $\mathfrak{A}$ *any* A *is equal to its kernel, iff any prime element* P *satisfies*

$$X \supset P \supseteq p \Longrightarrow pX = p.$$

PROOF. Let the condition be satisfied and suppose $\ker A \supset A$. Then, according to 5.4.8, it follows for at least one $b \subseteq \ker A$ and one prime element Q

$$b \neq bQ \ \&\ Q \supseteq b * b(b * A) \supseteq b * A.$$

But according to 6.2.4 – for at least one P, minimal over A – this leads to the contradiction:

$$Q \supset P \supseteq A \rightsquigarrow Q \supset P \supseteq b \rightsquigarrow b = bQ.$$

Suppose now $\ker A = A$ $(\forall\, A)$ and $X \supset P \supseteq p$, where P is prime and $p \supset pX$. Then there exists a prime element $Q \supseteq X$ satisfying $p \supset pQ$, where p and pQ have the same minimal prime supelements.

We show that p and pQ have in addition the same isolated primary components.

To this end we start from a primary element Q_1 with $\mathrm{Rad}\,(Q_1)$ minimal prime over pQ and $Q_1 \supseteq pQ$, that is $Q_1 \supseteq pq$ $(\forall q \in Q)$. Since Q is not minimal over pQ, recall $Q \supset X \supseteq p$, there exists some $q \subseteq Q$ with $q \not\subseteq \mathrm{Rad}\,(Q_1)$, leading to $p \subseteq \mathrm{Rad}\,(Q_1)$.

But that would imply $pQ = p$, a contradiction. □

Clearly, $A = \ker A$ is equivalent with the assertion that each A is equal to the intersection of all primary elements containing A. So, the fundamental theorem of number theory is again transferred to certain IDMs including the domain $\mathfrak{Z}$ of integers.

In $\mathfrak{Z}$ the intersection of primary components is in addition irredundant. This in mind we turn to a further step up, employing KRULL's Qu-Bedingung, compare [251].

6. 2. 6 Corollary. *Let $\mathfrak{A}$ be a commutative IDM satisfying $A = \ker A$. Then $\ker A$ is irredundant iff the all i.p.c. (isolated primary components) Q_i with $P_i = \mathrm{Rad}\, Q_i$ of A are of type $c * A$.*

PROOF. (a) Let $\bigcap Q_i = A$ be irredundant and suppose that the prime element P contains $D := \bigcap Q_j$ $(j \neq i)$. Then there exists an i.p.c R of D with $\mathrm{Rad}\, R = P$, since P is minimal in D, and with $D \cap R = D$, in spite of the required irredundance. Hence there exists some $c \subseteq D$ with $c \not\subseteq P$. But $\mathrm{Rad}\, Q = P \not\supseteq c \Longrightarrow c * Q \subseteq Q \Longrightarrow c * Q = Q$. So, we get $c * Q = c * D \cap c * Q = c * (D \cap Q) = c * A$.

(b) Let now all primary components Q_i be of type $c_i * A$. Then by $cQ_i \subseteq A$ and $\mathrm{Rad}\, Q_j = P_j \not\supseteq Q_i$ we get $Q_j \supseteq c$ $(\forall j \neq i)$ that is $D := \bigcap Q_{j \neq i} \supseteq c$. But $D \cap Q = D$ would imply

$$Q = c * A = c * D \cap Q_i = 1, ,$$

a contradiction! □

6.3 The Principal Ideal Theorem

We start from a commutative ideal monoid $\mathfrak{A}$. The fundamental structure of this section will be the modular, noetherian, hyper-normal commutative ideal monoid. The developments of this section are along the lines of chapter VII of LARSEN/MCCARTHY [267], consult LEONHARDT [271]. But, for the sake of fairness:

It's Krull time, again.

In algebraic geometry one central and fundamental notion is that of a *dimension.*

Consider a chain of primes $P_0 \subset P_1 \subset \ldots \subseteq P_r$. We say that this chain has *length* r. Its first term is P_0 its last term is P_r.

6. 3. 1 Definition. The *Krull dimension* of $\mathfrak{A}$ is the supreme of the lengths of all chains of distinct proper prime elements of $\mathfrak{A}$. The Krull dimension of $\mathfrak{A}$ is denoted by $\dim \mathfrak{A}$.

Clearly $\dim \mathfrak{A}$ may be equal to ∞ and also equal to 0. Otherwise it is a natural number $(\neq 0)$.

6. 3. 2 Definition. Let P be a proper prime element of $\mathfrak{A}$. The *height* of P, denoted by $\mathrm{ht}(P)$, is the Krull dimension of $\mathfrak{A}_P$. *The depth of* P, denoted by dpt (P) is the Krull dimension of $\mathfrak{A}/P$.

6. 3. 3 Definition. Let A be a proper element of $\mathfrak{A}$. By the *height* of A, denoted $\mathrm{ht}(A)$, we mean the minimum, by the dimension of A, denoted by $\dim(A)$, we mean the supreme of the values of $\mathrm{ht}(P)$, as P runs over all minimal prime divisors of A.

6. 3. 4 Krull's Dimension Theorem. *Let $\mathfrak{R}$ be a noetherian integral domain. Then all ideals $\mathfrak{p}$, minimal prime over the ideal $(a_1, \ldots, a_r)$ are of a height* $\mathrm{ht}(\mathfrak{p}) \leq r$.

Fundamental for this dimension theorem is

6. 3. 5 Krull's Principal Ideal Theorem. *Let $\mathfrak{R}$ be a Noetherian integral domain and choose some $a \in R$ and $\mathfrak{p}$ minimal prime over the principal ideal $\langle a \rangle$. Then* $\mathrm{ht}(\mathfrak{p}) = 1$.

To the opinion of IRVIN KAPLANSKY, [229], this principal ideal theorem is the most important single-theorem of commutative algebra.

Consider now some n-dimensional affine space $\mathbf{A}^n(K)$ over the field $\mathfrak{K}$. Assume that $\mathfrak{p}$ is prime in $\mathfrak{K}[X_1, \ldots, X_n]$ and that

$$\mathcal{V}(\mathfrak{p}) = \{(k_1, \ldots, k_n) \in \mathbf{A}^n(K) : \ f(k_1, \ldots, k_n) = 0 \text{ for } f \in \mathfrak{p}\}$$

is the *affine irreducible variety*, associated with $\mathfrak{p}$. Then, since any maximal chain of prime ideals of $\mathfrak{K}[X_1, \ldots, X_n]$ has length n, the principal ideal theorem implies:

$$\begin{aligned} \dim \mathcal{V}(\mathfrak{p}) &= \dim \mathfrak{K}[X_1, \ldots, X_n]/\mathfrak{p} \\ &= \dim \mathfrak{K}, [X_1, \ldots, X_n] - \mathrm{ht}(\mathfrak{p}) \\ &= n - \text{ minmal number of generators of } \mathfrak{p}\,, \end{aligned}$$

as will turn out by the general principal ideal theorem. And this corresponds, of course, with our vision of a dimension of $\mathcal{V}(P)$.

Another application of the principal ideal theorem leads to a theorem on implicit complex functions.

Let $0 \neq f \in \mathbf{C}[X_1, \ldots, X_n]$, $n \geq 2$ and let $\mathcal{V}(f)$ be a complex manifold. Then by the principal ideal theorem it holds $\mathrm{ht}(f) = 1$, that is $\dim \mathcal{V}(f) = n - 1$.

That the dimension of $\mathcal{V}(f)$ is equal to $n-1$ corresponds in a desirable manner with our visual conceptions. For, if $f \neq 0$ in case of $\dim \mathcal{V}(f) \geq 1$ there exists some $w = (w_1, \ldots, w_n) \in \mathcal{V}(f)$ – by the property of holomorphic functions – and to any neighbourhood U of this w there exist points $z = (z_1, \ldots, z_n) \in U \cap \mathcal{V}(f)$ satisfying

$$\frac{\partial}{\partial X_i} f(X_1, \ldots, X_n)\Big|_{\ X_1 = z_1, \ldots, X_n = z_n} \neq 0\,.$$

Suppose now $i = n$. Then by the theorem on unique continuous implicit functions in complex analysis there exists $g : V \longrightarrow W$, where V is some neighbourhood of $(z_1, \ldots, z_{n-1}) \in \mathbf{C}^{n-1}$ and W some neighbourhood of $z_n \in \mathbf{C}$ with

$$\begin{aligned} g(z_1, \ldots, z_{n-1}) &= z_n \\ &\& \\ f(z_1\,, \ldots\,, z_{n-1}\,, g(z_1, \ldots, z_{n-1})) &= 0\,. \end{aligned}$$

Hence in this neighbourhood the solution set of $f(X_1, \ldots, X_n) \doteq 0$ has dimension $n-1$.

We now turn to the proofs, starting with

6. 3. 6 Krull's Intersection Theorem (KIT). *Let $\mathfrak{A}$ be a hyper-normal and archimedean IDM, that is in particular some modular noetherian hyper-normal ideal monoid. Then the following are equivalent:*

(i) $A + A^* = 1 \;\&\; A^*c = 0 \Longrightarrow c = 0$

(ii) $\bigcap_{n\in N} A^n = 0.$

PROOF. Suppose (i). Then

$$\begin{aligned} \textstyle\bigcap_{n\in N} A^n =: M &\Longrightarrow AM = M \supseteq m \\ &\Longrightarrow Am = m \\ &\Longrightarrow \exists A^* \perp A \text{ with } A^*m = 0 \\ &\overset{(i)}{\Longrightarrow} m = 0\,. \\ &\Longrightarrow M = \textstyle\bigcap_{n\in N} A^n = 0\,. \end{aligned}$$

Let now (ii) be satisfied. Then

$$\begin{aligned} A + A^* = 1 \;\&\; A^*c = 0 &\Longrightarrow c = (A + (A^*))c = Ac \\ &\Longrightarrow c = 0 \vee \textstyle\bigcap_{n\in N} A^n \neq 0\,. \end{aligned}$$ □

As an immediate consequence we get:

6. 3. 7 Corollary. *Let $\mathfrak{A}$ be archimedean and hyper-normal and let A be contained in all maximal elements M. Then $\bigcap_{n\in Nq} A^n = 0$.*

PROOF. $A + A^* = 1 \;\&\; A^*c = 0 \Longrightarrow A^* = 1 \Longrightarrow c = 0\,.$ □

6. 3. 8 Lemma. *Let $\mathfrak{A}$ be noetherian, modular and hyper-normal, and let a be contained in all maximal elements M. Then it follows*

$$B \subseteq A \subseteq B + a \;\&\; a * A = A \Longrightarrow A = B\,.$$

PROOF. Let M be the uniquely determined maximal element of $\mathfrak{A}$. Then $\mathfrak{A}$ and $\overline{\mathfrak{A}} := \mathfrak{A}/B$ are ringlike, and it holds

$$A = (a + B) * A = B + (a + B) * A = \overline{a} \star \overline{A}\,.$$

But, $\overline{a} \in \overline{\mathfrak{A}}$ is a divisor. This means next

$$\overline{A} = \overline{a} \circ (\overline{a} \star \overline{A}) = \overline{a} \circ \overline{A}.$$

So, it follows $\overline{M} \circ \overline{A} = \overline{A}$. We now apply hyper-normality and the archimedean property of $\overline{\mathfrak{A}}$. Then (KIT) implies $\overline{A} = \overline{B}$ that is $a + B = B$ and thereby $A = B$. $\square$

6. 3. 9 Lemma. *Let $\mathfrak{A}$ be noetherian with unique maximal P, modular and hyper-normal and let P be minimal prime over a. Then $\mathfrak{A}$ satisfies the descending chain condition* DCC.

PROOF. First of all $\mathfrak{A}/a$ satisfies the conditions above (again) if $\mathfrak{A}$ satisfies these conditions, and obviously is suffices here to prove the ascending chain condition ACC. So we may start already from $\mathfrak{A}/a$ and on this account suppose $a = 0$. Here we observe first

$$x \supset y \Longrightarrow x * 0 \subset y * 0\,,$$

since otherwise – by $P \supseteq x * y$ – we would get $xP = x$, that is by hyper-normality $xP^* = 0$ with some $P^* \perp P$, a contradiction.

Hence the chain $a_1 \supset a_2 \supset \ldots a_i \supset \ldots$ must be finite by the Noether property. Consequently there is a minimal generator m above 0, which is necessarily minimal in the set of all $X \supset 0$.

So, in our original $\mathfrak{A}/a$ there exists a minimal $\overline{m} =: a + m$ by which the procedure can be continued, recall that by modularity divisors are sent to divisors. Thus we are led to a minimal $\overline{\overline{m}}$ over $\overline{m}$ etc. until this procedure stops, according to the Noether property.

Thus a finite maximal chain is constructed, which by the modular chain theorem, consult 3.3.9, is even of maximal length. Hence all descending chains between a and P are finite. $\square$

Now we are in the position to prove:

6. 3. 10 Krull's Principal ideal theorem (KPIT). *Let $\mathfrak{A}$ have the Noether property and suppose that $\mathfrak{A}$ is modular and hyper-normal and let* 0 *be prime. Suppose moreover that P is minimal prime over $a \neq 0, 1$. Then* $\mathrm{ht}(P) = 1$.

PROOF. Let P be minimal prime over a and let Q be prime and contained in P. We have to verify $Q = 0$. To this end some pre-consideration, compare also [3]:

First of all the prepositions for $\mathfrak{A}$ are transferred to all $\mathfrak{A}_P$ (P prime).

Next in $\mathfrak{A}_P$ by 5.6.4 $P = P_P$ is the unique minimal prime element over a_P. And, if Q is prime in $\mathfrak{A}$ and contained in P, then also $Q_P = Q \subseteq P_P = P$ is prime in $\mathfrak{A}_P$. Moreover it holds

$$Q^k{}_Q = 0_Q \Longrightarrow Q^k \subseteq 0 \Longrightarrow Q = 0\,.$$

Hence we are through, once it is shown $Q^k{}_Q = 0_Q$ for at least one $k \in \mathbf{N}$. To this end we start from some modular, noetherian hyper-normal $\mathfrak{A}$ with P as unique maximal element, which is assumed to be prime over a, and some prime $Q \subset P$ with $a \not\subseteq Q$, which will turn out as 0.

Again, let $\mathfrak{A}$, a, P and Q be chosen as above.

We consider $\mathfrak{A}/a =: \overline{\mathfrak{A}}$. Here $a + P = P$ is the unique maximal element, and by the Noether property we get: $P^n \subseteq a$ $(\exists n \in \mathbf{N})$, that is $\overline{P}^n = \overline{a}$. So, by DCC there exists some suitable $n \in \mathbf{N}$, satisfying the equality $a + Q^k{}_Q = a + Q^n{}_Q$ $(\forall k > n)$ and thereby

$$Q^k{}_Q \subseteq Q^n{}_Q \subseteq a + Q^k{}_Q\,.$$

From this, since $Q^n{}_Q$ is Q-primary in $\mathfrak{A}$ and $a \not\subseteq Q$ it follows next

$$a * Q^n{}_Q = Q^n{}_Q\,,$$

that is – by 6.3.8 – finally $Q^k{}_Q = Q^n{}_Q$ for all $k > n$.

Thus, lastly we get $Q^n{}_Q = 0_Q$ in $\mathfrak{A}_Q$, by corollary 6.3.7, meaning that the height of P equals 1. □

Applying KPIT we are now in the position to prove

6. 3. 11 Krull's Dimension Theorem (KDT). *Let $\mathfrak{A}$ have the Noether property and suppose that $\mathfrak{A}$ is modular and hyper-normal and that 0 is prime. Suppose furthermore that P is minimal prime over $(a_1 + \ldots + a_r)$. Then* $\mathrm{ht}(P) \leq r$, *that is by definition* $\dim(a_1 + \ldots + a_r) \leq r$.

PROOF. Let P be minimal prime over $a_1 + a_2 + \ldots + a_n$. We shall show $\mathrm{ht}P \leq r$. We may assume that P is the uniquely determined maximal element of $\mathfrak{A}$ and have to show that prime element chains $P = P_0 \supset P_1 \supset \ldots \supset P_s$ satisfy $s \leq r$. Furthermore we may replace $\mathfrak{A}$ by $\mathfrak{A}/P_s$ and suppose on this account that the generators of $\mathfrak{A}$ form an ideal semigroup with prime element 0. Moreover we may suppose that there is no prime element strictly between P and P_1.

Now, P is minimal prime over $a_1+\ldots+a_r$. Consequently $a_1+\ldots+a_r \not\supseteq P_1$, say $a_1 \not\subseteq P_1$. But then there cannot exist any prime element P' with $P_1 + a_1 \subseteq P' \subset P$. Hence P is uniquely prime over $P_1 + a_1$, which implies $P = \mathrm{Rad}\,(P_1 + a_1)$. So, there exists a natural number t satisfying ${a_i}^t \subseteq P_1 + a_1 \ \ (i = 1, \ldots r)$.

We suppose ${a_i}^t = a_1 \cdot b_i + c_i \ \ (b_i \subseteq \mathcal{A}_0)\,, c_i \subseteq P_1$ and consider $c_2 + \ldots + c_r$. By $c_2+\ldots+c_r \subseteq P_1$ there exists some minimal prime ${P_1}'$ over $c_2+\ldots+c_r$ with ${P_1}' \subseteq P_1$. And according to $a_i \subseteq \mathrm{Rad}\,(a_1 + \ldots + c_r) \ \ (i = 1, \ldots r)$ P is the unique prime over $a_1 + c_2 + \ldots + c_r$. Consequently in $\overline{\mathfrak{A}}_1 := \mathfrak{A}/{P_1}'$ the element $P/{P_1}'$ is the unique minimal prime over $\overline{a}_1 = a_1 + {P_1}'$, which is shown as follows:

Case 1. Suppose $a_1 \subseteq {P_1}'$.

Then $a_1 + \ldots + a_r$ is contained in ${P_1}'$, too. This leads to $P_1 = P$, since P is the uniquely determined minimal prime over $a_1 + \ldots + a_r$.

Case 2. Suppose $a_1 \not\subseteq {P_1}'$.

Then a_1+P_1 is in $\overline{A}/{P_1}'$ neither *zero* nor identity, observe $a_1+P_1 \subseteq P \neq 1$. Consequently, by PIT we get $\mathrm{ht}(P/{P_1}') = 1$, whence we may conclude ${P_1}' = P_1$.

The rest follows by induction:

In case of $r = 1$ the proposition follows by the PIT.

We suppose that the assertion is verified for all $b_1+\ldots+b_s$ with $s \leq r-1$.

Then by minimal primeness of P_1 over $c_2+\ldots+c_r$, for s in the sense above it follows $s - 1 \leq r - 1$, that is $s \leq r$. □

Chapter 7

Prüfer Structures

7.1 Left Prüfer Structures

Rings with a *distributive ideal lattice* have a strong structure theory, not only in the commutative case. The crucial reason: Rings are always *congruence permutable* therefore the class of rings with a distributive ideal lattice forms an *arithmetical variety,* and – arithmetical varieties do have a very strong structure theory, whence they are objects in their own right, consult for instance BURRIS/SANKAPPANAVAR, [87].

Commutative rings with a distributive ideal lattice were investigated by C. U. JENSEN in a series of papers, cf. [220] through [223].

One main result: The class of arithmetical commutative rings with identity is exactly the class of commutative rings with identity having the divisor property (P) for finitely generated ideals. Hence [77] applies to them in any case. But, of course, their divisibility theory is much stronger than that of commutative *d-semigroups.* One reason: Given a commutative arithmetical ring, there exists some *Bézout ring,* that is a ring in which finitely generated ideals are principal, with an isomorphic divisibility theory. This was shown by D. D. ANDERSON in [3]. For the theory of d-semigroups the reader is referred to [77]. [1)]

Arithmetical rings are stronger than Prüfer rings, which are defined as commutative rings whose finitely generated regular ideals – these are the ideals containing at least one cancellable element – are required to be invertible. So the best name for the structures below might be something

[1)] unpublished but available

like *ideal left divisibility semigroup,* briefly *ideal ld-semigroup* or *ideal divisibility semigroup,* briefly *ideal d-semigroup.*

Nevertheless we think that there will arise no ambiguity if we give the honor of structures of this type to HEINZ PRÜFER. "Prüfer properties" from a general point of view were studied by I. FLEISCHER in [124] and [125].

7. 1. 1 Definition. By a *left Prüfer structure* we mean an AML $\mathfrak{A} = (\mathcal{A}, \mathcal{A}_c, \cdot, \cap, \Sigma)$ with:

(LP) $$a_1 + \ldots + a_n \supseteq B \implies a_1 + \ldots + a_n \,|_\ell\, B\,.$$

Hence any left Prüfer structure is an LD-AML. But, of course, $\mathcal{A}_c$ need not be closed under multiplication, compare 5.2.5. Left Prüfer structures are defined from the left. Dually *right Prüfer structures* are defined. Consequently, by a *Prüfer structure* we mean an AML which is both, a left and a right Prüfer structure.

7. 1. 2 Lemma. *If $\mathfrak{A}$ is an AML and B is compact in $\mathfrak{A}$ with $AX = B$, then there exists even a finite sum $x_1 + \ldots + x_n \subseteq X$ satisfying the equation $A \cdot (x_1 + \ldots + x_n) = B$.*

PROOF. $$\begin{aligned} A \cdot X = B &\implies A \cdot X \subseteq B \subseteq A \cdot (x_1 + \ldots + x_n) \\ &\qquad (\exists\, x_i \in X \ \ (1 \leq i \leq n)) \\ &\implies A \cdot X = B = A \cdot (x_1 + \ldots + x_n)\,. \end{aligned}$$ □

7. 1. 3 Proposition. *Let $\mathfrak{A}$ be an LD-AML. Then $\mathfrak{A}$ is a left Prüfer structure if and only if $\mathfrak{A}$ satisfies the equations:*

(e) $$a + b = (a + b) \cdot (a * b + b * a)$$

(D) $$A \cap (B + C) = (A \cap B) + (A \cap C).$$

PROOF. (a) Let $\mathfrak{A}$ satisfy (e) and (D).

We say that an element A is n-generated if it is a sum of n elements but no sum of less than n elements. In this case we say also that A has *length* n. We say that an element A is at most n-generated if it is k-generated with $1 \leq k \leq n$.

We will carry out the proof by induction along the length of A, B. To begin with:

STEP 1: If A and B are left divisors satisfying

$$A + B = (A + B) \cdot (A * B + B * A)\,, \tag{E}$$

then $A + B$ is again a left divisor.

VERIFICATION: By (E) and (D) we get:

$$\begin{array}{rcl} A + (A + B) \cdot (A * B) & \supseteq & (A + B) \cdot (A * B) \\ & & \qquad + A(B * A) + B(B * A) \\ & = & (A + B) \cdot (A * B + B * A) \\ & \overset{(E)}{\rightsquigarrow} & \\ A + \underline{(A + B) \cdot (A * B)} & = & A + \underline{B} \\ & \text{and} & \\ A \cap (A + B) \cdot (A * B) & = & A \cap (\, A(A * B) + B(A * B)\,) \\ & = & (A \cap A \cap B) + (\, A \cap B(A * B)\,) \\ & = & A \cap B \\ & \rightsquigarrow & \\ A \cap \underline{(A + B) \cdot (A * B)} & = & A \cap \underline{B}\,. \end{array}$$

Hence it holds by (COM):

$$(A + B) \cdot (A * B) = B\,. \tag{7.5}$$

Suppose now $A + B \supseteq C$. Then it follows by (D) and (7.5) :

$$\begin{aligned} C &= (A \cap C) + (B \cap C) \\ &= A(A * C) + B(B * C) \\ &= (A + B) \cdot (B * A) \cdot (A * C) + (A + B) \cdot (A * B) \cdot (B * C) \\ &= (A + B) \cdot (\, (B * A) \cdot (A * C) + (A * B) \cdot (B * C)\,)\,. \end{aligned}$$

Thus we get $(A + B) \,\Big|_{\ell}\, C$.

Once more, the preceding step was done for arbitrary left divisors A, B under condition (E). In particular so far we obtained that any $a + b$ is a left divisor, since all generators are left divisors satisfying condition (e).

STEP 2: First we notice

$$AU = A = AV \Longrightarrow A(U \cap V) \supseteq (AU)V \supseteq AV = A\,. \tag{7.6}$$

Now we assume that all k-generated ($1 \leq k \leq n$) elements are (already) verified as left divisors and that all ℓ-generated ($1 \leq \ell \leq n-1$) elements A satisfy

$$A + b = (A + b) \cdot (A * b + b * A)\,. \tag{7.7}$$

Then every n-generated element satisfies (7.7) , too, as is shown now:

Assume $D = A + B$ with D of length n and A, B both of length $\leq n-1$. Then

$$\begin{array}{cl} & D + c \\ \supseteq & (D + c) \cdot (A * c + c * A + c * B) \\ \supseteq & ((A + c) + (B + c)) \cdot (A * c + c * A + c * B) \\ = & ((A + c) \cdot (A * c + c * A + c * B) \\ + & ((B + c) \cdot (A * c + c * A + c * B) \\ \supseteq & ((A + c) \cdot (A * c + c * A) + ((B + c) \cdot (c * B) \\ = & (A + c) + B \\ = & (A + B) + c \\ = & D + c\,. \end{array}$$

So, by symmetry and (7.6) we obtain

$$\begin{array}{cl} & D + c \\ \supseteq & (D + c) \cdot (D * c + c * D) \\ = & (D + c) \cdot (\,(A + B) * c + c * (A + B)\,) \\ \supseteq & (D + c) \cdot (\,(A * c \cap B * c) + (c * A + c * B)\,) \\ \overset{(D)}{=} & (D + c) \cdot (\,(A * c + c * A + c * B) \cap (B * c + c * B + c * A)\,) \\ \overset{(7.6)}{=} & D + c\,. \end{array}$$

Thus condition (7.7) is verified for D.

Now, combining STEP 1 and STEP 2, we get that any finitely generated element is a left divisor.

So far the algebraic property has not yet been applied.

(b) Let now $\mathfrak{A}$ be a left Prüfer structure. Then condition (e) results by

$$(a + b)(b * a) = a \ \&\ (a + b)(a * b) = b \rightsquigarrow (a + b)(a * b + b * a) = a + b\,.$$

Next for any finitely generated triple A, B, C we get

$$\begin{aligned} A \cap (B + C) &= (B + C)(\,(B + C) * A\,) \\ &= B(\,(B + C) * A\,) + C(\,(B + C) * A\,) \\ &\subseteq B(B * A) + C(C * A) \\ &= (A \cap B) + (A \cap C) \\ &\subseteq A \cap (B + C). \end{aligned}$$

Suppose now that $\mathfrak{A}$ is an AML satisfying (D) only for finitely generated elements and consider $A = \sum\limits_{i \in I} a_i$ and $B = \sum\limits_{j \in J} b_j$. Then we get by definition:

$$\begin{aligned} A \cdot B &= \textstyle\sum(a_i \cdot b_j) \qquad (\,(i,j) \in I \times J\,) \\ A + B &= \textstyle\sum(a_i + b_j) \qquad (\,(i,j) \in I \times J\,) \end{aligned}$$

and it results by calculation

$$A \cap B = \textstyle\sum(a_i \cap b_j) \qquad (\,(i,j) \in I \times J\,).$$

FOR: It suffices to prove that the left side is contained in the right side. So we start with some $x \subseteq A \cap B$. Then there exist elements $a_1, \ldots, a_m \subseteq A$, and $b_1, \ldots, b_n \subseteq B$ satisfying:

$$\begin{aligned} x \subseteq a_1 + \ldots + a_m \quad &\& \quad x \subseteq b_1 + \ldots + b_n \\ &\leadsto \\ x \quad &\subseteq \quad (a_1 + \ldots + a_m) \cap (b_1 + \ldots + b_n) \\ &= \quad (a_1 \cap b_1) + (a_1 \cap b_2) + \ldots (a_m \cap b_n) \\ & \quad\;\; \text{(since } \mathfrak{A} \text{ is finitely distributive)} \\ &\leadsto \\ x \quad &\subseteq \quad \textstyle\sum \ldots . \end{aligned}$$

And this leads to (D) *via*

$$\begin{aligned} x \;&\subseteq\; A \cap (B + C) \\ &\Rightarrow \\ x \;&\subseteq\; (a_1 \cap b_1) + (a_1 \cap b_2) + \ldots + (a_\ell \cap b_m) \\ &\quad + \quad (a_1 \cap c_1) + (a_1 \cap c_2) + \ldots + (a_\ell \cap c_n) \\ &\Rightarrow \\ x \;&\subseteq\; (A \cap B) + (A \cap C) \end{aligned}$$

□

It is noteworthy that a left Prüfer structure need not satisfy the equation $a(a{*}b{+}b{*}a) = a$. Recall Example 5.2.3. But in an AML whose generators are both, left and right divisors, this equation is valid if only the underlying lattice is distributive, as was shown under 5.3.5.

In particular this provides:

7. 1. 4 Proposition. *Let $\mathfrak{A}$ be a D-AML. Then $\mathfrak{A}$ is a left Prüfer structure if and only if $\mathfrak{A}$ satisfies the equations:*

$$\begin{array}{lrcl}
\text{(e')} & a & = & a\,(a*b+b*a) \\
(\mathrm{K}^r) & A(B\cap C) & = & AB\cap AC\,.
\end{array}$$

PROOF. (a) Condition (e') implies, recall the proof of (a) below proposition 7.1.3, that any $a+b$ is a left divisor of its components.

$$\begin{aligned}
b &= b(a*b+b*a) \\
&= b(a*b)+(b\cap a) \\
&= b(a*b)+a(a*b) \\
&= (a+b)(a*b)\,.
\end{aligned}$$

Suppose now

$$A \;:=\; a_1+\ldots+a_n \supseteq c\,.$$

Then (K^r) implies

$$AB=CD \implies (A+C)\cdot(B\cap D)=AB$$

whence we get by induction:

$$\begin{array}{lrcl}
 & c & = & (a_1+c)\cdot(a_1*c)=\ldots=(a_n+c)\cdot(a_n*c) \\
\leadsto & c & = & (\,(a_1+c)+\ldots+(a_n+c)\,)\cdot(\,a_1*c\cap\ldots\cap a_n*c\,) \\
 & & = & (a_1+\ldots+a_n)\cdot(a_1*c\cap\ldots\cap a_n*c) \\
\leadsto & A\mid_\ell c\,. & &
\end{array}$$

(b) Let now $\mathfrak{A}$ be Prüfer D-AML . Then it results first

$$\begin{aligned}
A(b\cap c) &= Ab(b*c)+Ac(c*b) \\
&\supseteq (Ab\cap Ac)\cdot(b*c+c*b) \\
&= Ab\cap Ac \\
&\supseteq A(b\cap c),
\end{aligned}$$

and thereby next

$$\begin{aligned}
a_1b\cap a_2c &\subseteq (a_1+a_2)b\cap(a_1+a_2)c \\
&= (a_1+a_2)\cdot(b\cap c)\,.
\end{aligned}$$

Thus, consult 5.3.3, we get (K^r), which completes the proof. $\square$

7. 1. 5 Corollary. *Let $\mathfrak{A}$ be generated by a set of divisors such that all elements have finite length, say that $\mathfrak{A}$ has the Noether property. Then $\mathfrak{A}$ is a left Prüfer structure if and only if it satisfies:*

$$\text{(j)} \qquad (a * b + b * a)^2 = a * b + b * a$$

$$\text{(D)} \qquad A \cap (B + C) = (A \cap B) + (A \cap C)\,.$$

PROOF. All we have to show is the necessity of (j). But in any left Prüfer structure finitely generated elements A, B satisfy $(A + B) \cdot (B * A) = A$. Hence any divisor generated Noether AML with the left Prüfer property satisfies:

$$\begin{aligned} a * b &= (a + b) \cdot (b * a) * b \\ &= (b * a) * ((a + b) * b) \\ &= (b * a) * (a * b) \\ &= (a * b + b * a) * (a * b) \\ &\rightsquigarrow \\ (a * b + b * a)^2 &= \quad (a * b + b * a) \cdot (a * b) \\ &\quad + (a * b + b * a) \cdot (b * a) \\ &= a * b + b * a\,. \end{aligned}$$ $\square$

Some remarks: The question arises whether in 7.1.3 and 7.1.4 condition (e) and (e'), respectively, are necessary. The answer is given by monoids since the Rees ideal lattice is always distributive.

Furthermore: The reader should take into account that in the preceding proofs the algebraic property has not been applied to verify sufficiency. Hence the corresponding parts remain valid also for v-ideals, for instance.

If $\mathfrak{A}$ is even a Prüfer monoid then of course $(A \cap B)C = AC \cap BC$ is valid as well.

Next: Since by condition (K^r) left divisors A, B satisfy

$$AB \supseteq C \Longrightarrow C = A(B \cap A * C) = AB(B * C)\,,$$

condition (K^r) yields that products of left divisors A, B are again left divisors. Thus we are led to:

7. 1. 6 Lemma. *In a left Prüfer structure satisfying (K^r) any divisor A satisfies $A \cap B = A(A * B) = A((A + B) * B)$. Hence in these structures the* *set submonoid generated by the basis is closed under* $\cdot\,, +\ \cap$, *and* $|$ *on the grounds of 7.1.2, that is forms a submonoid, for the insider a divisibility submonoid* $\mathfrak{C} =: (\mathcal{C}, \cdot\,, +\,, \cap)$.

7.2 Normal Prüfer monoids

According to the results exhibited so far, a commutative ring with *fixing elements* ($\forall\, a\ \exists\, e_a : ae_a = a$) is a Prüfer ring in the sense of this paper if and only if it is *arithmetical* , i. e. iff the ideal lattice is distributive.

Hint: Let $\mathfrak{R}$ be arithmetical and let u be a common fixing element (private unit) of a and b for instance $u = v - vw + w$ with $av = a$, $bw = b$. Then it holds

$$\begin{array}{rrcl} & a & \in & \langle a\rangle \cap (\,\langle b\rangle + \langle a-b\rangle\,) \\ & & = & (\,\langle a\rangle \cap \langle b\rangle\,) + (\,\langle a\rangle \cap \langle a-b\rangle\,) \\ \rightsquigarrow & au & = & t + c(a-b)\ \ (\,t \in \langle a\rangle \cap \langle b\rangle, c \in \langle a\rangle : \langle b\rangle\,) \\ \rightsquigarrow & a\,(u-c) & = & t - cb\ \ (\,u-c \in \langle b\rangle : \langle a\rangle\,), \end{array}$$

and this means $u = c + (u-c) \in \langle a\rangle : \langle b\rangle + \langle b\rangle : \langle a\rangle$, whence

$$\langle a, b\rangle \ \ = \ \ \langle a, b\rangle(\,\langle a\rangle : \langle b\rangle + \langle b\rangle : \langle a\rangle\,)\,.$$

Thus for arithmetical commutative rings we even get

$$\langle 1\rangle \ \ = \ \ \langle a\rangle : \langle b\rangle + \langle b\rangle : \langle a\rangle\,,$$

choose $u = 1$. Similar, if all $x \in \mathcal{A}_0$ are left cancellable in $\mathfrak{A}$, then

$$a \cdot 1 = a\,(a * b + b * a)\ \rightsquigarrow\ a * b + b * a = 1\,.$$

This motivates a study of *normal* IDMs, that is IDMs satisfying

$$(\mathrm{jn}^*)\quad a * b + b * a = 1 \quad \text{and} \quad (\mathrm{jn}^{\cdot})\quad a : b + b : a = 1$$

in a particular manner.

7. 2. 1 Proposition. *Let* $\mathfrak{A}$ *be an arbitrary IDM. Then* $\mathfrak{A}$ *is normal if and only if it satisfies one of the two subsequent conditions:*

(D^*_+) $\qquad A * (B + C) = A * B + A * C \quad$ (*A,B,C finitely generated*) .

$(\mathrm{D}^*_\cap) \qquad (A\cap B)*C = A*C + B*C \quad (A{,}B \quad \textit{finitely generated}\,)\,.$

If moreover $\mathfrak{A}$ is commutative then we get even

$$\textit{(JN*)} \iff \textit{(D}^*_\cap\textit{)} \iff \textit{(D}^*_+\textit{)}\ .$$

PROOF. First we verify

$$(\mathrm{jn}^*) \iff (\mathrm{JN}^*) \quad A*B+B*A=1 \quad (\mathrm{A,B} \quad \text{finitely generated})\,.$$

To this end we suppose that $A*B+B*A=1$ is already proven for all at most n-generated elements, and infer from this $A*B+B*A=1$ for all at most $(n+1)$-generated components.

So, let B and C be at most n-generated. We put

$$T \ := \quad (B+b)*(C+c)+(C+c)*(B+b)\,.$$

It follows for at most n-generated elements X

$$\begin{aligned} 1 &\supseteq (B{+}b)*X{+}X*(B{+}b)\\ &\supseteq (B*X)\cdot(b*X){+}(X*B){+}(X*b)\\ &\supseteq (B*X{+}X*B{+}X*b)\cdot(b*X{+}X*B{+}X*b)=1\,, \end{aligned}$$

and furthermore

$$\begin{aligned} T &= (B{+}b)*(C{+}c){+}(C{+}c)*(B{+}b)\\ &\supseteq (\,(B{+}b)*C{+}(B{+}b)*c\,){+}(\,C*(B{+}b)\cap c*(B{+}b)\,)\\ &\supseteq (\,(B{+}b)*C{+}(B{+}b)*c\,){+}(\,C*(B{+}b)\,)\cdot(\,c*(B{+}b)\,)\\ &\supseteq (\,(B{+}b)*C{+}C*(B{+}b)\,)\cdot(\,(B{+}b)*c{+}c*(B{+}b)\,)\\ &\supseteq 1\,. \end{aligned}$$

Let now B,C be finitely generated. Then we get:

$$\begin{aligned} 1 &\supseteq (\,A*(B+C)\,)*(\,A*B{+}A*C\,)\\ &\supseteq (\,A*(B{+}C)\,)*(A*B){+}(\,A*(B{+}C)\,)*(A*C)\\ &= A(\,A*(B{+}C)\,)*B{+}A(\,A*(B{+}C)\,)*C\\ &\supseteq C*B{+}B*C=1\,. \end{aligned}$$

This verifies $(\mathrm{JN}^*) \Longrightarrow (\mathrm{D}^*_+)$ because $A*(B{+}C)\supseteq A*B{+}A*C\,.$

We now turn to (D_{+}^{*}). Here finitely generated elements A, B satisfy

$$\begin{aligned} A * B + B * A &= (A + B) * B + (A + B) * A \\ &= (A + B) * (B + A) = 1\,, \end{aligned}$$

meaning $(\mathrm{D}_{+}^{*}) \Longrightarrow (\mathrm{JN}^{*})$. –

Finally we consider the commutative case. Here we get first, as above, condition (JN^{*}) and thereby

$$\begin{aligned} 1 &\supseteq (\,(A \cap B) * C\,) * (A * C + B * C) \\ &\supseteq (\,(A \cap B) * C\,) * (A * C) + (\,(A \cap B) * C\,) * (B * C) \\ &= A * (\,(\,(A \cap B) * C\,) * C\,) + B * (\,(\,(A \cap B) * C\,) * C\,) \\ &\supseteq A * (A \cap B) + B * (B \cap A) \quad (\mathrm{R4}) \\ &\supseteq A * B + B * A = 1\,. \end{aligned}$$

This means $(\mathrm{JN}^{*}) \Longrightarrow (\mathrm{D}_{\cap}^{*})$, observe $(A \cap B) * C \supseteq (A * C) + (B * C)$.

On the other hand $\mathrm{D}(_{\cap}^{*})$ implies for finitely generated elements A, B

$$\begin{aligned} A * B + B * A &= A * (A \cap B) + B * (A \cap B) \qquad (\mathrm{R2}) \\ &= (A \cap B) * (A \cap B) = 1\,. \end{aligned}$$

Hence $(\mathrm{D}_{\cap}^{*}) \Longleftrightarrow (\mathrm{JN}^{*})$. □

Caution: If $\mathfrak{R}$ is a commutative ring with identity then obviously the implication holds: *d-normal* $\Longrightarrow$ *t-normal* $\Longrightarrow$ *v-normal.* But the arrows must not be turned.

7. 2. 2 Lemma. *Let $\mathfrak{A}$ satisfy condition* (JN^{*}). *Then $\mathfrak{A}$ is lattice distributive.*

PROOF. Suppose that B, C are finitely generated. Then it follows:

$$(\mathrm{D}\cap) \qquad A \cap (B + C) = (a \cap B) + (A \cap C)\,,$$

SINCE
$$\begin{aligned} 1 &\supseteq A \cap (B + C) * (\,(A \cap B) + (A \cap C)\,) \\ &\supseteq (\,A \cap (B + C)\,) * (A \cap B) + (\,A \cap (B + C)\,) * (A \cap C) \\ &\supseteq (B + C) * (A \cap B) + (B + C) * (A \cap C) \\ &\supseteq C * B + B * C = 1\,. \end{aligned}$$

This completes the proof. □

7. 2. 3 Corollary. *An IDM satisfying* (jn^{*}) *is a Prüfer monoid.*

Next we apply the preceding propositions to special cases. To begin with

7. 2. 4 Definition. By a *valuation monoid* we mean a totally ordered IDM .

7. 2. 5 Proposition. *A commutative Prüfer IDM is normal if and only if each* $\mathfrak{A}_M$ *is a valuation monoid.*

PROOF. We put $S := \{s \mid s \not\subseteq M\}$. Then we get – as pointed out above – $a_S * b_S = (a*b)_S$, and this means comparability for each pair of elements a_S, b_S, since $a*b$ and $b*a$ cannot be contained in the same M, recall $a*b + b*a = 1$. From this we get *straightforwardly* the comparability of each pair of elements $A_S, B_S \in \mathfrak{A}_M$. □

Recall, an integral IDM is an IDM with cancellable generators.

7. 2. 6 Proposition. *Let* $\mathfrak{A}$ *be a commutative integral semigroup of ideals, not necessarily of finite character, that is v-ideals not excluded. Then the following properties are pairwise equivalent:*

$$
\begin{array}{llcll}
(i) & ab & = & (a+b)\cdot(a\cap b) & \\
(ii) & A(B\cap C) & = & AB\cap AC & \\
(iii) & a\cap(b+c) & = & (a\cap b)+(a\cap c) & \text{(d)} \\
 & (a+b)^2 & = & a^2+b^2 & \text{(0)} \\
(iv) & \textit{Each } \mathfrak{A}_P & \textit{is} & \textit{a valuation monoid.} & \\
(v) & \mathfrak{A} & \textit{is} & \textit{a Prüfer monoid.} &
\end{array}
$$

PROOF. By assumption each generating divisor is cancellable and the product of cancellable divisors is again cancellable,

$$
\text{SINCE} \qquad AB \supseteq X \neq 0 \implies AB \supseteq A(A*X) = X
$$
$$
\begin{aligned}
&\implies AB = A(B + A*X) \\
&\implies B = B + A*X \\
&\implies B \,\Big|\, (A*X) \\
&\implies AB \mid A(A*X) = X\,.
\end{aligned}
$$

Hence $\mathfrak{A}$ is even a commutative IDM.

Next, recall that cancellable divisors A satisfy

$$A(B\cap C) \;=\; AB\cap AC$$

since
$$\begin{aligned} AB \cap AC = AX &\Longrightarrow AB \supseteq AX \subseteq AC \\ &\Longrightarrow B \supseteq X \subseteq C \\ &\Longrightarrow B \cap C \supseteq X \\ &\Longrightarrow A(B \cap C) = AB \cap AC\,. \end{aligned}$$

Finally observe, that the conditions above are always satisfied if one of the elements is equal to 0, and that $0 * a + a * 0 = 1$ is valid *a fortiori.* Consequently we may restrict our considerations to non vanishing elements $a, b, c, \ldots$.

$(i) \Longleftrightarrow (v)$. By (i) we get:

$$\begin{aligned} ab \cdot (b * a + a * b) &= ab\,(b * a) + ba\,(a * b) \\ &= a\,(a \cap b) + b\,(a \cap b) \\ &= (a + b) \cdot (a \cap b) \\ &= ab \cdot 1 \\ &\rightsquigarrow \\ a * b + b * a &= 1\,. \end{aligned}$$

$(ii) \Longleftrightarrow (v)$. It holds $(ii) \Longrightarrow (i)$ and $(v) \Longrightarrow (ii)$.

$(iii) \Longleftrightarrow (v)$. (iii) implies (i) by

$$\begin{aligned} ab &= ab \cap (a^2 + b^2) \\ &= (ab \cap a^2) + (ab \cap b^2) \\ &= a(b \cap a) + b(a \cap b) \\ &= (a + b)(a \cap b)\,. \end{aligned}$$

Let now $\mathfrak{A}$ satisfy the Prüfer condition. Then (d) is valid *a fortiori*, and from (D) and (K) it follows:

$$\begin{aligned} ab \cap (a^2 + b^2) &= (ab \cap a^2) + (ab \cap b^2) \\ &= a(b \cap a) + b(a \cap b) \\ &= (a + b)(a \cap b) \\ &= ab\,, \end{aligned}$$

meaning
$$\begin{aligned} (a + b)^2 &= a^2 + ab + b^2 \\ &= a^2 + b^2\,. \end{aligned}$$

$(iv) \Longleftrightarrow (v)$. (i) and thereby (v) follow immediately if each $\mathfrak{A}_P$ is totally ordered.

Let now (v) be satisfied. Then $a * b + b * a = 1$ follows by cancellation, and (iv) results in a manner, similar to that in the proof of 7.2.5 $\square$

Again: The results given here for the normal case remain valid, of course, for monoids of ideals of commutative monoids since the algebraic property didn't play any role in the proof of 7.1.3 and hasn't either been involved in the preceding proof. This will turn out as most relevant in the later chapter on monoids of v-ideals.

Excursion: As already referred in the introduction KRONECKER emphasized that the essential advantage of a UF-extension is that of an ideal GCD-extension. So we take the chance of discussing the preceding results.

Any ideal theory begins with some *reduced monoid,* i. e. a monoid satisfying

$$a \,|_{\ell}\, b \Longleftrightarrow a \,|_{r}\, b \quad \text{and} \quad a \,|\, b \;\&\; b \,|\, a \Longrightarrow a = b.$$

So, given a reduced monoid $\mathfrak{S}$, we are faced with the question whether there exists a reduced monoid extension $\sum$ such that *not divisible in* $\mathfrak{S}$ remains *valid in* $\sum$.

7. 2. 7 Definition. Let $\mathfrak{S}$ be a reduced monoid. By a $|$-*normal* divisibility extension of $\mathfrak{S}$ we mean a reduced inf-closed supmonoid $\sum$ satisfying

(PE0) $\qquad \alpha \supseteq \beta \implies \alpha \,|\, \beta$

(PE1) $\qquad \alpha \,|_{\Sigma}\, \beta \implies \alpha \,|_{\mathfrak{S}}\, \beta$

(PE2) $\qquad \alpha \in \sum \implies \alpha = \sum_1^n a_i \;\; (\exists\; a_i \in S)\,.$

In this language we get *via* 7.1.3.

7. 2. 8 Corollary. *Let* $\mathfrak{S}$ *be a holoid. Then* $\mathfrak{S}$ *admits a* $|$-*normal Prüfer extension* $\mathfrak{P}$ *iff the* t-*ideal monoid* $\mathfrak{T}$ *is distributive and in addition satisfies condition* (e) *and its left dual.*

PROOF. The one direction is obvious.

Assume now that $\mathfrak{P}$ satisfies (PE0) through (PE2). We consider the implication $a_1 \wedge \ldots \wedge a_n \longmapsto \langle a_1, \ldots, a_n \rangle_v$. This is a function which $\mathfrak{P}$ maps m-homomorphically on the monoid of the finitely generated v-ideals. Hence $\mathfrak{T}$ is a Prüfer extension. $\square$

Requiring the algebraic property, things become essentially restricted, and it might be that there exist non algebraic $|$-normal divisibility extensions but no algebraic $|$-normal divisibility extension. In this case we may change to the v-IDM, thus getting an extension whose finite infima are divisors of their components, but maybe by factors not necessarily finitely generated.

As an example of this type we present the monoid $(\mathbf{Q}^{\geq 0}, +, \min)$, extended by π. It is easily seen that the elements of this monoid, considered as principal ideals, are divisors of the v-IDM – but not w.r.t. finitely generated v-ideals.

In general, of course, the quality of v-ideal extensions depends essentially on the quality of the basic monoid.

If, for instance, $\mathfrak{S}$ satisfies (D) and (K^r), then according to [72] $\mathfrak{S}$ is representable.

Since the combination (D) & (K^r) is a necessary condition in order that $\mathfrak{S}$ have a *d-monoid extension* we could solve the commutative embedding problem once we had good descriptions of totally ordered monoids admitting a d-monoid extension.

But: It seems to be very unlikely that there exist *nice descriptions* at all.

7.3 Prüfer Implications

In this final section we develop some properties of Prüfer monoids w.r.t. further investigations. We start with a most important implication:

7. 3. 1 Lemma. *Let $\mathfrak{A}$ be a lattice modular LD-IDM. Then the implication holds:*

$$A \succeq A^2 \textit{ implies } A^s \supseteq B \supseteq A^{s+k} = A^n \Longrightarrow B = A^\ell \ \ (\exists\, \ell).$$

PROOF. In a lattice modular LD-IDM in case of $A \succ A^2$ for each triple s, k, n of natural numbers satisfies the implication

$$A^s \supseteq B \supseteq A^{s+k} = A^n \implies B = A^\ell\,.$$

HINT: According to (5.8) $x \subseteq A$ but $x \not\subseteq A^2$ implies successively $A + x = A^2 + x = A(A^2 + x) + x = A^3 + x \ldots$ and thereby

$$\begin{array}{rcl} A + x & = & A^n + x \\ & \rightsquigarrow & \\ A^s & \supseteq & A^n + x^s \\ & \supseteq & (A^n + x)^s = A^s \quad (5.8) \\ & \rightsquigarrow & \\ A^s & = & A^n + x^s \,. \end{array}$$

If now B lies between A^s and A^n and if in addition $B \not\subseteq A^{s+1}$, then by lattice modularity and the left divisor property of x^s it results for some C

$$B \;=\; A^n + x^s \cdot C$$

with $x^s \cdot C = B \cap x^s \not\subseteq A^{s+1}$. Hence there exists some $c \subseteq C$ satisfying $xc \not\subseteq A^2$ and thereby – recall $xc \subseteq A$ & $xc \not\subseteq A^2$ – satisfying

$$\begin{array}{rcl} A^s & = & A^n + (xc)^s \\ & \subseteq & A^n + B = B \,. \end{array}$$

This completes the proof. □

7. 3. 2 Lemma. *Let $\mathfrak{A}$ be a Prüfer monoid and suppose $a, b \subseteq P^n$ but $a, b \not\subseteq P^{n+1}$. Then it follows $(P^{n+1} + (a+b)) \cdot (P + a * b) = P^{n+1} + b$.*

PROOF. From $b \in P^n$ & $b \not\subseteq P^{n+1}$ it follows $a * b = (a+b) * b \not\subseteq P$. Hence it holds $P + a * b \supset P$, whence we get according to 7.3.7:

$$\begin{array}{rl} & (P^{n+1} + (a+b)) \cdot (P + a * b) \\ = & P^{n+1}(P + a * b) + (a+b)P + (a+b) \cdot (a * b) \\ = & P^{n+1} + b \;. \end{array}$$

□

7. 3. 3 Corollary. *Let $\mathfrak{A}$ be a Prüfer monoid. Then each maximal M satisfies $M^n \succeq M^{n+1}$ $(\forall\, n \in \mathbf{N})$.*

PROOF. Suppose $M^n \supset X \supset M^{n+1}$ and $a, b \in M^n$. Then by the preceding method of proof it would result $M^{n+1} + a = M^{n+1} + b$ and hence in the case of $a \not\subseteq X, b \subseteq X$ it would follow $M^{n+1} + a \subseteq X$. This completes the proof by contradiction. $\square$

7. 3. 4 Lemma. *In any Prüfer monoid any prime element is completely prime. So prime divisors satisfy* $P^{m+k} \neq P^{(m+k)-1} \Longrightarrow P^m * P^{m+k} = P^k$.

PROOF. First we get:

$$\begin{aligned} P^n \supseteq AB \;\&\; P \not\supseteq B &\Longrightarrow P^n \supseteq (P^n + A) \cdot (P^n + B) \\ &\Longrightarrow P^n \supseteq (P^n + A) \cdot (P + B)^n \\ &\Longrightarrow P^n \supseteq P^n + A \quad (7.3.7(\mathrm{A}))\,. \end{aligned}$$

Let now P be a prime divisor and $P^{m+k} \supseteq P^m \cdot x$. Then $P^1 \cdot (P^1 * x) = x$ and we get successively $P^\ell \cdot (P^\ell * x) = x$ for all $(2 \leq \ell \leq k)$, that is finally $P^k \,\Big|\, x$ and thereby $P^m * P^{m+k} = P^k$. $\square$

Finally we remark:

7. 3. 5 Proposition. *Let* $\mathfrak{A}$ *be an arbitrary AML and let* P *be prime in* $\mathfrak{A}$, *satisfying the implication* $P^n \supseteq X \supseteq P^{n+k} \Longrightarrow X = P^\ell \;\; (\exists 1 \leq \ell \leq k)$. *Then from* $P^n \neq P^{n+1} \;\; (\forall\, n \in \mathbf{N})$ *it follows that* $Q := \bigcap P^n \;\; (n \in \mathbf{N})$ *is prime.*

PROOF. Suppose $Q \supseteq ab$ and $Q \not\supseteq a, b$. Let moreover $k \geq 0$ be highest exponent with $P^k \supseteq a$ but $P^{k+1} \not\supseteq a$ and let $\ell \geq 0$ be the highest exponent with $P^\ell \supseteq b$ but $P^{\ell+1} \not\supseteq b$. Then it results $P^{k+1}+a = P^k$ and $P^{\ell+1}+b = P^\ell$ and thereby

$$\begin{array}{rcl} P^{k+\ell+1} & \supseteq & ab \\ & \leadsto & \\ P^{k+\ell+1} & = & P^{k+\ell+1} + ab \\ & = & P^{k+\ell+1} + (P^{k+\ell+1} + a) \cdot (P^{k+\ell+1} + b) \\ & = & P^{k+\ell+1} + (P^{k+1} + a)P^\ell \cdot (P^{\ell+1} + b)P^k \\ & = & P^{k+\ell+1} + (P^k P^\ell + a) \cdot (P^\ell P^k + b) \\ & \vdots & \\ & = & P^{k+\ell+1} + (P^{k+1} + a) \cdot (P^{\ell+1} + b) \\ & = & P^{k+\ell+1} + P^k \cdot P^\ell \\ & = & P^k \cdot P^\ell\,, \end{array}$$

a contradiction! □

7. 3. 6 Corollary. *Let $\mathfrak{A}$ be a left Prüfer monoid and let M be maximal with $M^n \neq M^{n+1}$. Then $Q := \bigcap M^n$ $(n \in \mathbf{N})$ is prime.*

7. 3. 7 Lemma. *Let $\mathfrak{A}$ be a left Prüfer monoid and let $P \in A$ be a prime element. Then*

$$(\mathrm{I}^\ell) \qquad A \supset P \implies AP = P\,.$$

PROOF. From $A \supseteq a$ & $P \not\supseteq a$ & $P \supseteq p$, we get $(a+p)(a*p) = p$ with $P \supseteq a*p$, and thereby $AP \supseteq A(a*p) \supseteq p$ which leads to $AP = P$. □

Summarizing we keep in mind:

7. 3. 8 Proposition. *Let $\mathfrak{A}$ be a Prüfer IDM. Then $\mathfrak{A}$ satisfies:*

$$(\mathbf{D}) \qquad A \cap (B+C) \;=\; (A\cap B) + (A \cap C).$$

$$(\mathbf{I}) \qquad A \supset P \;\Rightarrow\; AP = P = PA$$

$$(\mathbf{K}) \qquad A(B\cap C) \;=\; AB \cap AC$$

$$(\mathbf{L}) \qquad \begin{aligned} AB = CD \Rightarrow AB &= (A\cap C)\cdot(B+D) \\ &= (A+C)\cdot(B\cap D) = CD \end{aligned}$$

$$(\mathbf{P}) \qquad A := a_1 + \ldots + a_m \supseteq b \;\Rightarrow\; b = A(x_1 + \ldots x_n) \quad (\exists\, x_1, \ldots, x_n\,)$$

$$(\mathbf{Q}) \qquad AB = BA \;\Rightarrow\; (A+B)^n = A^n + B^n$$

$$(\mathbf{R}) \qquad AB = BA \;\Rightarrow\; (A\cap B)^n = A^n \cap B^n\,.$$

PROOF. The properties above result successively as follows:

(D): Compare 7.1.3.

(I): Apply (I^ℓ).

(K): Compare 7.1.4.

(L): Distribute once over $\cap$ – and once over $+$.

(P): Compare 7.1.2

(Q): Observe (L), and continue by induction:

Assuming that (Q) holds for all k between 1 and n it results:

$$\begin{aligned} A^{n+1}+B^{n+1} &\supseteq (A\cap B)^k(A^{n+1-k}+B^{n+1-k}) \quad (2k\le n+1)\\ &= (A\cap B)^k(A+B)^{n+1-k}\\ &= (AB)^k\cdot(A+B)^{n+1-2k} \qquad\qquad (\text{apply } (\mathbf{L}))\\ &= A^{n+1-k}B^k+A^kB^{n+1-k}\,. \end{aligned}$$

(R). Operate dually to the preceding conclusion (below (Q)). □

7. 3. 9 Lemma. *Let $\mathfrak{A}$ be a Prüfer IDM, and let $P\in\mathcal{A}$ be prime. Then*

$$(\forall\, C\subseteq P)\ A\supset P\succ P^2 \implies AC=C=CA\,.$$

PROOF. On the grounds of duality we may restrict our considerations to a proof of $AC=C$.

We start from $A\supset P\succ P^2$ and suppose $b,p\subseteq P$ but $b\not\subseteq P^2$. We denote $b+p$ by B. Then it follows $P\supseteq B$ & $B\,|\,p$, whence it suffices to prove $AB=B$ for this particular element B. So assume $XB\subseteq P^2$. Then – by $P^2+B=P$ – it follows

$$\begin{aligned} P^2\supseteq XB &\implies P^2\supseteq(P^2+X)\cdot(P^2+B)\\ &\implies P^2\supseteq(P+X)^2\cdot P \end{aligned}$$

But because $P^2\not\supseteq P$ and because of 7.3.7 this means $P+X=P \rightsquigarrow P\supseteq X$ and thereby $P^2:B=P$. So, because $A\supset P \rightsquigarrow AP=P$, we get:

$$\begin{aligned} P^2+\underline{AB} &= A(\,P^2+B\,)=AP=P\\ &= P^2+\underline{B} \end{aligned}$$

and

$$\begin{aligned} P^2\cap\underline{AB} &= A(\,P^2\cap B\,)\\ &= A(\,P^2:B\,)B\\ &= AP\cdot B\\ &= P\cdot B\\ &= (\,P^2:B\,)B\\ &= P^2\cap\underline{B}\,, \end{aligned}$$

which provides $AB=B$ – by lattice distributivity. □

Chapter 8

Mori Structures

8.1 The Prime Criterion

In this section we investigate algebraic multiplication lattices whose *prime elements* are *divisors*, also called *prime divisors.* In particular by this requirement any maximal element is a prime divisor, observe $xy \subseteq M \Longrightarrow x \subseteq M \vee y \subseteq M$.

The main result will be that an AML of this type is a commutative AML, satisfying condition (M), including the result of SMITH, [278], that a ring is an AM-ring iff any prime ideal is a divisor.

8. 1. 1 Lemma. *Let $\mathfrak{A}$ be an AML whose prime elements are left divisors, and let P be prime. Then it results*

$$\text{(I)} \qquad A \supset P \implies AP = P\,.$$

PROOF.
$$\begin{aligned} A \cdot P \subset P &\implies Ap \subset p = PX \quad (\exists p \in P) \\ &\implies Q \cdot p \subset p \quad (\exists\, Q \text{ prime } \supseteq A \supset P) \\ &\ \ \& \quad Q \cdot p = Q \cdot PX = PX = p\,, \end{aligned}$$

the last line by $QY = P \Longrightarrow Y = P$, that is a contradiction. □

8. 1. 2 Lemma. *Let $\mathfrak{A}$ be an AML and let P be a prime left divisor satisfying $A \supset P \Longrightarrow AP = P$. Then all prime powers of P are left divisors, too.*

PROOF. Consider some prime element P together with some B satisfying $P^n \Big|_\ell B$ and $P^{n+1} \supseteq B$ for some $n \geq 1$. Then we get first $P^n(P^n * B) = B$, from which follows $P^n \cdot P = P^n \cdot (P + (P^n * B))$. We consider the cases $P + (P^n * B) = P$ and $P + (P^n * B) \supset P$. In the first case we get $P \Big|_\ell P^n * B$ and thereby $P^{n+1} |_\ell B$, in the second case we get $P^{n+1} = P^n \Big|_\ell B$ by assumption. □

8. 1. 3 Lemma. *Let $\mathfrak{A}$ be an AML and let P be a prime left divisor satisfying $A \supset P \Longrightarrow AP = P$. Then*

$$P \supseteq A \supseteq P^n \implies A = P^m \ (\exists\, 1 \neq m \leq n).$$

PROOF. By the premiss in case of $P^m \supseteq A \not\subseteq P^{m+1}$ $(m+1 \leq n)$ we get $P + P^m * A \supset P$, recall 8.1.2, and thereby

$$\begin{aligned} A &= P^m \cdot (P^m * A) \\ &\supseteq P^m \cdot (\,(P^m * A) + P^{n-m}\,) \\ &\supseteq P^m(\,(P^m * A) + P\,)^{n-m} (5.8) \\ &= P^m \qquad\qquad \text{(by assumption)}. \end{aligned}$$

□

8. 1. 4 Lemma. *Let $\mathfrak{A}$ be an AML and let P be a prime element satisfying $A \supset P \Longrightarrow AP = P$. Then it holds*

$$\begin{array}{ccc} P^{m-1} \neq P^m & \supseteq & A \cdot B \\ & \Longrightarrow & \\ (\exists\, k, \ell \geq 0 :\ P^k \supseteq A & \& & P^\ell \supseteq B \quad \& \quad k + \ell \geq m). \end{array}$$

This means that under the condition above prime elements P satisfy the implication:

$$P^{m+k} \neq P^{(m+k)+1} \implies P^m * P^{m+(k+1)} = P^{k+1}.$$

PROOF. Evidently

$$P^m \supseteq A\,B \implies P^m \supseteq (P^m + A) \cdot (P^m + B).$$

Suppose now $P \supseteq A, B$. Then – according to 8.1.3 – it follows

$$P^m + A = P^k \quad \& \quad P^m + B = P^\ell \text{ where } k + \ell \geq m.$$

Otherwise, assume $P \supseteq A$ and $P \not\supseteq B$. Then it holds

$$P^m \ \supseteq\ P^k \cdot (P + B)^m = P^k \quad (8.1.1)$$

and thereby $k = m$. The rest follows by analogy. $\square$

As an immediate consequence of the preceding lemmata we get:

8. 1. 5 Corollary. *If all prime elements P of an AML $\mathfrak{A}$ are left divisors then*

$$P^m \neq P^{m+1} \;\; (\forall\, m \in \mathbf{N}) \implies \bigcap P^m =: Q \textit{ is prime}\,.$$

8. 1. 6 Lemma. *If all prime elements P of an AML $\mathfrak{A}$ are (not only left, but even left/right-) divisors then each pair U, V commutes.*

PROOF. First we obtain for any A

$$A \;=\; \bigcap {P_i}^{e_i} \quad ({P_i}^{e_i} \supseteq A)\,.$$

Suppose $\bigcap {P_i}^{e_i}$ $({P_i}^{e_i} \supseteq A) =: B \supset A$. Then there would exist at least one $b \subseteq B$ satisfying $b\,(B * A) \subset b$ which by 5.4.8 would provide a prime element $P \supseteq B * A$ with $b \cdot P \subset b$.

We assume $P^n \supseteq A$ $(\forall\, n \in \mathbf{N})$, leading to $P^n \supseteq B$ $(\forall\, n \in \mathbf{N})$. Then it follows either $P^m = P^{m+1} \,\Big|\, b$ $(\exists m \in \mathbf{N})$ or $\bigcap {P_i}^{e_i} = Q$ by 8.1.5 is a prime divisor with $P \supset Q \,\Big|\, B \supseteq b$. Therefore, in any case we would get $bP = b$, a contradiction! Consequently there is an $m \in \mathbf{N}$ with

$$P^m \supseteq A \quad \& \quad P^{m+1} \not\supseteq A\,.$$

But this leads to the contradiction

$$P \not\supseteq P^m * A \;\subseteq\; B * A \subseteq P\,.$$

Hence each $U, V \in \mathcal{A}$ commutes, since $P^e \supseteq UV \Longrightarrow P^e \supseteq VU$ by lemma 8.1.4. $\square$

Now we are in the position to prove:

8. 1. 7 The Prime Criterion. *$\mathfrak{A}$ is a multiplication AML if and only if all prime elements are prime divisors,*

PROOF. First of all recall that by the preceding lemma $\mathfrak{A}$ is commutative. Next observe:

Obviously it suffices to verify that $A \supseteq b \Longrightarrow A \,\Big|\, b$.

Start now from $A \supseteq b$ and $A(A*b) \subset b$. It follows $b(\,b*A(A*b)\,) \subset b$ and this leads by 5.4.8 to some prime element P satisfying

$$1 \neq P \quad \supseteq \quad b*A(A*b) \tag{8.2}$$

$$\& \quad bP \subset b \quad \& \quad b*bP = P\,. \tag{8.3}$$

Let $E(n)$ mean $P^n \,|\, A$. We will show that $E(n)$ is satisfied for all $n \in \mathbf{N}$. By (5.19) and (8.2) we are led to the inclusion:

$$\begin{aligned} P &\supseteq (A*b)*A(A*b) \\ &= (A*b)*(A*b)A \supseteq A\,. \end{aligned}$$

Hence it holds

$$P^1 \,\Big|\, A\,. \tag{E1}$$

This means in particular $P \Big| b$. Next we show

$$P \cdot b \supseteq A \cdot (A*b)\,. \tag{8.5}$$

This is evident if b is a divisor, since then $bP \supseteq b(b*A(A*b)) = A(A*b)$, apply (8.2). However, the inclusion holds also in the general case which is shown as follows:

By assumption and by 8.1.2 and 8.1.5 the element $\bigcap P^n \ \ (n \in \mathbf{N})$ in any case is a divisor of b, provided every power P^m is a divisor of b, more precisely an idempotent divisor, if $P^m = P^{m+1}$ $(\exists m \in \mathbf{N})$, and a prime divisor otherwise. So in case of $P^n \supseteq b$ $(\forall\, n \in \mathbf{N})$ we get in particular $bP = b$. Hence we may restrict our attention to considering the case in which there exists some $e \in \mathbf{N}$ with $P^e \supseteq b$ & $P^{e+1} \not\supseteq b$, satisfying:

$$\begin{aligned} P \cdot b &= P \cdot P^e(P^e * b) \\ &\supseteq (P^{e+1} \cap (P^e * b)) \cdot (P^{e+1} + (P^e * b)) \\ &\supseteq (P^{e+1} \cap (P^e * b)) \cdot (P + (P^e * b))^{e+1} \\ &= P^{e+1} \cap (P^e * b) \quad (8.1.1) \\ &\supseteq P \cdot b\,, \end{aligned}$$

$$\leadsto$$

$$\begin{aligned} Pb &= P^{e+1} \cap (P^e * b) \\ &\supseteq P^{e+1} \cap (P^e * A(A*b)) \\ &\supseteq A(A*b)\,, \end{aligned}$$

the last line since $P^{e+1} \not\supseteq A(A*b)$ by 8.1.2 would imply

$$\begin{array}{rcl} P^{e+1} & \not\supseteq & A(A*b) \\ & \overset{(8.2)}{\rightsquigarrow} & \\ P \not\supseteq P^e * A(A*b) & \subseteq & b * A(A*b)\,) \subseteq P\,. \end{array}$$

Now we are in the position to verify

$$\text{(Ek)} \qquad P^k \,\Big|\, A \qquad (\forall k \in \mathbf{N})$$

by showing $$E\,(n) \implies E\,(n+1)$$

in order to construct a contradiction to $b \supset b \cdot P$. To this end suppose $E\,(n)$. Then it follows:

$$\begin{array}{rcl} b \cdot P & \overset{(8.5)}{\supseteq} & A \cdot (A * b) \\ & \overset{(5.19)}{\supseteq} & A \cdot (P^n * b) \\ & \overset{(E\,(n)}{=} & P^n(P^n * b) \cdot (P^n * A) \\ & = & b \cdot (P^n * A) \\ & \rightsquigarrow & \\ P & | & P^n * A \qquad\qquad (\text{by } b * bP = P) \\ & \rightsquigarrow & \\ P^{n+1} & \Big| & A\,. \end{array}$$

Thus $E(n)$ entails $E(n+1)$.

This completes the proof. □

A final Remark: The prime criterion is proven for commutative rings with identity in Mott, [304], for arbitrary commutative rings by Gilmer/Mott in [163], and for arbitrary not necessarily commutative rings by Smith in [278]. But these papers are based on ring theoretical particularities. Hence they do not present general AML-results, although, of course, parts remain correct also in the general case.

However, it should be emphasized that Smith, in [278], presents a series of non-commutative classical examples of AM-rings, justifying this way the present investigation.

That in [163] and in [278] the identity requirement is dropped turns out to be irrelevant, since the lattice of ideals may be extended to an AML with identity by adjoining some compact identity element 1.

So AM-ring-ideal-semigroups form an AML, generated by compact elements which are not divisors *a priori.* This points out, that structures of the investigated type above "in fact do live in the real (mathematical) world."

8.2 Mori Implications

Again, let $\mathfrak{A}$ denote an AML. We call $\mathfrak{A}$ a *Mori* [1)] also a *multiplication structure*, briefly an M-structure, if $\mathfrak{A}$ satisfies a *multiplication AML,* also synonymously an *M-structure* if $\mathfrak{A}$ satisfies

$$A \supseteq B \Longrightarrow A \cdot X = B = Y \cdot A \ \ (\exists X, Y)\,,$$

briefly if $\mathfrak{A}$ satisfies

$$\text{(M)} \qquad A \supseteq B \implies A \,\Big|\, B\,.$$

Clearly, by definition every M-structure is even an ideal structure since each of its elements is a divisor. But, since 1 is not required to be compact, an M-structure need not be an ideal semigroup! Consider for instance the semigroup of ideals of a boolean ring $\mathfrak{B}$ without identity. Although $\mathfrak{B}$ fails to have an identity, its ideal semigroup does have an identity, namely B, but, of course, not necessarily compact. Next recall:

Investigating M-structures means investigating Dedekind domains from a general point of view and hence it means moreover an abstract treating of classical ideal theory.

So it doesn't surprise that the arithmetic of M-structures is dominated by classical regularities, since missing prime decompositions are strongly substituted by condition (M).

In order to make this most general assertion a bit clearer we start with a series of rules most familiar to ring theoretists in the Dedekindian situation.

---

1) This might lead to some irritation with respect to *Mori domains*, which are defined as integral domains with ACC on v-ideals. But it seems adequate w.r.t. to the pioneer Shinziro Mori.

However we restrict our attention to those implications, which play some role with respect to this paper. A series of results holding already in AMLs satisfying condition (M) merely for finitely generated elements will be given within an investigation of ideal d-semigroups.

8. 2. 1 Proposition. *Let $\mathfrak{A}$ be an M-structure and $P \in \mathcal{A}$ be a prime Then it holds: in addition to the Prüfer rules* **(D), (I), (K), (L), (P), (Q), (R)** $\mathfrak{A}$ *satisfies:*

$$
\begin{array}{lrcl}
(\mathbf{AB}) & AB & = & BA \\
(\mathbf{A}^\ell) & A^n \supseteq B \ \ (\forall\, n \in \mathbf{N}) & \Rightarrow & A \cdot B = B \\
(\mathbf{B}^\ell) & A \supseteq A^n * B \ \ (\forall\, n \in \mathbf{N}) & \Rightarrow & A \cdot B = B \\
(\mathbf{C}^*\ ) & A \supseteq A^n * B & \Rightarrow & A^{n+1} \supseteq B \\
(\mathbf{E}^*) & P^n \supseteq B \ \&\ P^{n+1} \not\supseteq B & \Rightarrow & \exists\, a \not\subseteq P : P^n = a * B \\
(\mathbf{F}) & A & = & \bigcap {P_i}^{e_i} \, ({P_i}^{e_i} \supseteq A) =: \ker' A \\
(\mathbf{G}^\ell\ ) & A \supset P \supseteq B & \Rightarrow & A \cdot B = B \\
(\mathbf{H}^0) & \operatorname{Rad} Q \ \textit{prime} & \Rightarrow & Q = (\operatorname{Rad} Q)^n \\
(\mathbf{H}) & \operatorname{Rad} Q \ \textit{prime} & \Rightarrow & Q \ \textit{primary} \\
(\mathbf{I}^*) & A \supset P & \Rightarrow & AP = P \\
(\mathbf{J}^*) & A * B + B * A & =: & U = U^2 \\
(\mathbf{N}^*\ ) & a * b + b * a & := & U = U^2 \\
(\mathbf{S}) & P^m & \succeq & P^{m+1} \ \ (\forall m \geq 1) \\
(\mathbf{T}^\ell) & U = U^2 \supseteq B & \Longrightarrow & UB = B \\
(\mathbf{U}) & (A \cap B) \cdot U = A \cap B & \Rightarrow & A \cdot U = A \\
 & U \cdot (A \cap B) = A \cap B & \Rightarrow & U \cdot A = A. \\
(\mathbf{X}) & P \supseteq X \supseteq P^n & \Rightarrow & X = P^\ell \ \ (\exists \ell \in \mathbf{N})
\end{array}
$$

together with the right/left dual versions $(\mathrm{A}^r), (\mathrm{C}^*), \ldots$ *which will be combined with the "opposite" cases to* (A), (C), ...

PROOF. First of all it holds **(AB)**, that is $\mathfrak{A}$ is commutative, recall lemma 8.1.6. Applying this without further hint we get successively:

$(\mathbf{A}^\ell)$**:** Suppose $A^n \supseteq B$ $(\forall\, n \in \mathbf{N})$ and $B \supseteq b$ and let moreover P be prime with $P \supseteq A$ and $Pb \subset b$. Then $\bigcap P^n$ $(n \in \mathbf{N}) =: Q$ is a divisor of B, and Q is idempotent or prime. This leads to $Pb = b$ and hence to $Ab = b$, according to 5.4.8.

The proof just given heavily depends on the algebraic property. But actually, conditions (A) (and thereby (B)) follow from condition (M) even though $\mathfrak{A}$ might fail to be algebraic. This was shown in [68] through [70].

(B$^\ell$): $A \supseteq A^n * B$ $(\forall\, n \in \mathbf{N})$ implies $A^n \supseteq B$ $(\forall\, n \in N)$, whence we get $AB = B$, according to **(A)**.

(C*): **(C*)** is equivalent to

$$(\mathbf{C}^{*\prime}) \qquad A^n \supseteq B \;\&\; A^{n+1} \not\supseteq B \implies A \not\supseteq A^n * B \;\; (n \in \mathbf{N}),$$

which is inductively shown by $A \supseteq A^n * B \Longrightarrow A \supseteq A^{n-k} * B$. So, we prove

$(\mathbf{C}^{*\prime})$: If $\mathfrak{A}$ is an M-structure and if $A^{n+1} \not\supseteq B$ then there exists a smallest $k \in \mathbf{N}$ with $A^k \supseteq B \;\&\; A^{k+1} \not\supseteq B$, maybe $k = 0$. But this leads to $A^k(A^k * B) = B$ with $A \not\supseteq A^k * B$ and thereby *a fortiori* with $A \not\supseteq A^n * B$, because $A^n * B \supseteq A^k * B$.

(E*): Suppose $X \cdot P^n = B$. It follows $P \not\supseteq X$ since $P^{n+1} \not\supseteq B$. Consequently there exists some $a \subseteq X$ with $a \not\subseteq P$. And this means

$$\begin{aligned} a \cdot P^n \subseteq B \;\&\; a \cdot Y \subseteq B &\implies P^n \supseteq a \cdot Y \\ &\implies P^n \supseteq Y, \\ \text{whence we get} \qquad P^n &= a * B. \end{aligned}$$

according to 8.1.4

(F): Recall the proof of 8.1.6

(G): Combine condition **(I)** of the preceding section with condition **(A)**.

(H^0): Put $\operatorname{Rad} Q =: P$ and suppose $P^n \neq Q$ $(\forall n \in \mathbf{N})$. We falsify the cases (a) through (c) below:

$$\begin{array}{lll} (\mathbf{1}) & P^n \neq P^{n+1} \;(\forall\, n \in \mathbf{N}) \;\&\; \bigcap P^n =: T \supseteq Q & \\ (\mathbf{2}) & P^m = P^{m+1} \supset Q & (\exists\, m \in \mathbf{N}) \\ (\mathbf{3}) & P^m \supset Q \;\&\; P^{m+1} \not\supseteq Q & (\exists\, m \in \mathbf{N}). \end{array}$$

$(\mathbf{1})$ In this case it would hold $T \subset P$ and hence there would exist some a satisfying $a \subseteq P \;\&\; a \not\subseteq T$ and $a^k \subseteq Q \subseteq T$ $(\exists\, k \in \mathbf{N}) \rightsquigarrow a \subseteq T$, as well, a contradiction!

(**2**) Suppose $a \subseteq P^m$ & $a \not\subseteq Q$. Then by to $(\mathbf{A}^{\ell})$ it follows $Pa = a \not\subseteq Q$ on the one hand and $a = (\sum_1^n p_i)a = (\sum_1^n p_i)^k a \subseteq Q$ $(\exists\, k \in \mathbf{N})$ on the other hand, recall: $a^u \subseteq Q$ & $b^v \subseteq Q \Longrightarrow (a+b)^{u+v} \subseteq Q$.

(**3**) By **(F)** and 8.1.1 we get $Q \subseteq P^m \cap R$ with some prime $R \not\supseteq P$. But this entails some $p \subseteq P$ with $p \not\subseteq R$ & $p^k \subseteq Q \subseteq R$ $(\exists\, k \in \mathbf{N})$ that is $p \subseteq R$, a contradiction!

(H): **(H)** follows from $(\mathbf{H}^0)$ since $P^n \Big| AB \Longrightarrow P \Big| A \vee P^n \Big| B$.

$(\mathbf{I}^*)$**:** Recall 8.1.1

$(\mathbf{J}^*)$**:** Starting from $(A+B)(A*B) = B$ we get

$$\begin{aligned} A*B &= (A+B)\cdot(B*A)*B \\ &= (B*A)*(A*B). \end{aligned}$$

$$\rightsquigarrow$$

$$\begin{aligned} (A*B+B*A)^2 &= (A*B+B*A)\cdot(A*B) \\ &\quad +(A*B+B*A)\cdot(B*A) \\ &= A*B+B*A. \end{aligned}$$

$(\mathbf{N}^*)$**:** Observe $(\mathbf{J}^*)$.

(S): $X = P^m(Y+P)$ $(\exists Y) \rightsquigarrow X = P^m \vee X = P^{m+1}$.

(U). Observe $(\mathbf{A}^r)$.

$(\mathbf{T}^{\ell})$**:** Apply $(\mathbf{A}^{\ell})$.

(X): Recall 8.1.3. □

Some remarks:

FIRST OF ALL, the reader should notice that condition **(A)** by 5.4.8 results already from

(A') $$P^n \supseteq B \;\; (\forall n \in \mathbf{N}) \implies PB = B = BP,$$

and that condition (C*) is equivalent to

$(\mathbf{C}^*\mathbf{'})$ $$A^n \supseteq B \;\&\; A^{n+1} \not\supseteq B \implies A \not\supseteq A^n * B.$$

As will turn out, this second version will fit most conveniently in many of our proofs.

NEXT WE EMPHASIZE the evidence of $(\mathbf{E}^{\cdot}) \Longrightarrow (\mathbf{C}^*)$, whence, required in a Mori criterion, condition $(\mathbf{C}^*)$ may be replaced by the GILMER/MOTT-condition $(\mathbf{E}^{\cdot})$, "which resembles what KRULL calls Qu-Bedingung für i.K.I." in [251] ["Jedes $\mathfrak{a}_S$ ist ein $\mathfrak{a} : (s)$"] , compare [163].

Obviously the power of $(\mathbf{E}^*)$ results from the fact that it does not only certify condition $(\mathbf{C}^*)$ but moreover yields also $P^m \supseteq B \;\&\; P^{m+1} \not\supseteq B \Longrightarrow P^m = a * B \ (\exists a)$, which means that each not idempotent prime power $P^m \in \mathcal{A}$ is of type $a * b$, observe:

$$\begin{aligned} P^m \supseteq B \;\&\; P^{m+1} \not\supseteq B &\Longrightarrow \exists\, b \subseteq B :\ P^m \supseteq b \;\&\; P^{m+1} \not\supseteq b \\ &\Longrightarrow P^m = a * b\,. \end{aligned}$$

8.3 M-Equivalents

8. 3. 1 Proposition. *An arbitrary AML $\mathfrak{A}$ is a multiplication AML iff it satisfies the conditions* (B), (U), *and* (S) . [2)]

PROOF. Any prime element P satisfies

$$A \supset P \Longrightarrow AP \subseteq P \;\&\; AX \subseteq P \Longrightarrow P \supseteq X\,,$$

meaning $A * P = P$. Hence we are further led to:

$$\begin{aligned} A \supset P \supseteq B &\Longrightarrow A \supset P = A^n * P \supseteq A^n * B \quad (\forall\, n \in \mathbf{N}) \\ &\Longrightarrow BA = B\,, \end{aligned}$$

that is – by duality – to condition (G).

Next assume $P^s \supseteq B \;\&\; P^{s+1} \not\supseteq B$. By (S) $\Longrightarrow P^n \succeq P^{n+1}$ $(\forall n \in \mathbf{N})$ this leads to $P \not\supseteq P^s * B$,

$$\begin{array}{llcl} \text{SINCE:} & P^s \supseteq B & \& & P^{s+1} \not\supseteq B\,, \\ \text{implies} & P * (P^s * B) & = & P^{s+1} * B \\ & & = & (P^{s+1} + B) * B \\ & & = & P^s * B \\ \text{whence} & P^k * (P^s * B) & = & P^{k+s} * B \ (\forall k \in \mathbf{N}) \\ & & = & P^s * B \\ \text{that is} & P & \not\supseteq & P^s * B \qquad (\star) \end{array}$$

[2)] Condition (U) may be replaced by condition (AB), as is approved by the subsequent development.

where $(\star)$ results from the fact that otherwise (B) would imply $(P^s * B)\cdot P = P^s * B$ and thereby $P^{s+1} \supseteq P^s * B \supseteq B$. This proves the assertion.

Hereby – on the grounds of (S) – it results next

$$\text{(X)} \qquad P \supseteq X \supseteq P^n \implies X = P^\ell \ \ (\exists \ell \in \mathbf{N}),$$

observe that in case of $P^e \supseteq X$ & $P^{e+1} \not\supseteq X$ it follows:

$$\begin{aligned}(\Delta) \qquad X \supseteq P^e \cdot (P^e * X) \ &= \ P^e \cdot (P^e * X + P^{n-e}) \\ &\supseteq \ P^e \cdot (P^e * X + P)^{n-e} \overset{(\star)}{=} P^e\,.\end{aligned}$$

In particular this implies 8.1.5 which follows along the line of the corresponding proof. So by (U) and (G) we get that is the archimedean property for prime elements P, that is

$$\text{(AP)} \qquad P^n \supseteq A \ \ (\forall n \in \mathbf{N}) \implies PA = A = AP$$

Next we show that condition (F) is satisfied, recall that ist

$$A = \bigcap {P_i}^{e_i} \ \ (P_i \text{ prime and } {P_i}^{e_i} \supseteq A)\,.$$

To this end we suppose $\bigcap {P_i}^{e_i} \ ({P_i}^{e_i} \supseteq A) =: B \supset A$. Then there would exist at least one $b \subseteq B$ satisfying $b\,(B * A) \subset b$ which by 5.4.8 would provide a prime element $P \supseteq B * A$ with $b \cdot P \subset b$, and it would exist some $m \in \mathbf{N}$ with $P \not\supseteq P^m * A$, because otherwise $P^n \mid A \implies P^n \mid B \mid b \implies bP = b$ would follow. But this would lead to the contradiction

$$P \supseteq B * A \ \supseteq \ P^m * A \not\subseteq P$$

Hence each $U, V \in \mathcal{A}$ commutes, observe that by (X) in case of $P \supseteq U, V$ and $P^e \supseteq UV$ we get

$$P^e = P^e + UV = P^e + (P^e + U)\cdot(P^e + V) = P^e + VU\,.$$

and that in case of $P \supseteq A$ & $P \not\supseteq B$ we get the same equation by applying (5.8) and condition (G) – see above.

Now we are in the position to show that any prime element is even a prime divisor.

To this end suppose first $P \supseteq B$ and $P \supseteq P^n * B$ $(\forall n \in \mathbf{N})$. Then we succeed by condition (B).

Otherwise there is some $m \in \mathbf{N}$ satisfying $P^m \supseteq B$ & $P \not\supseteq P^m * B$. In this case we get by commutativity:

$$\begin{array}{rcl} B & \supseteq & P^m \cdot (P^m * B) \\ & \overset{(AB)}{=} & (P^m \cap (P^m * B)) \cdot (P^m + (P^m * B)) \\ & \overset{(5.8)}{\supseteq} & (P^m \cap (P^m * B)) \cdot (P + (P^m * B))^m \\ & \supseteq & P^m \cap (P^m * B) \qquad\qquad (\mathrm{G}) \\ & \supseteq & B \\ & & \\ & \rightsquigarrow & \\ B & = & P^m \cdot (P^m * B) \rightsquigarrow P^m \Big| B\ . \end{array}$$

This completes the proof by the prime criterion. □

8. 3. 2 Proposition. *An arbitrary AML $\mathfrak{A}$ is a multiplication AML iff it satisfies the conditions* (A) *and* (C) *.*

PROOF. By 8.3.1 it suffices to show that (A) combined with (C) implies the conditions (B) and (S).

So, combine (A) and (C). This leads to (B) and thereby to (G), because $P \supseteq P^n * A\ \ (\forall n \in \mathbf{N}) \Longrightarrow P^n \supseteq A\ \ (\forall n \in \mathbf{N})$.

Let now (G) be satisfied. Then it holds $P^m * X \supseteq P$. Suppose $P^m * X = P$. Then – according to (C) – we get $P^{m+1} \supseteq X$ and thereby $P^{m+1} = X$. If, however, $P^m * X \supset P$ is valid we get $X \supseteq P^m(P^m * X) = P^m$, according to (G). Hence condition (S) is satisfied, too. □

8.4 The left Divisor Case

8. 4. 1 Proposition. *Let $\mathfrak{A}$ be an LD-AML. Then $\mathfrak{A}$ is a multiplication AML iff it satisfies the conditions* (B) *and* (N*) *.*

PROOF. First recall: $(*)\quad A \supset P \supseteq B \Longrightarrow AB = B\ = BA$, which was shown in the proof of 8.3.1.

We now show that the required conditions imply condition (S):

By condition (N*) we are in the position to infer

$$a \ = \ a\,(a * b + b * a)$$

To this end suppose

$$a \neq a\,(a * b + b * a)\,.$$

Then there exists some prime element P with

$$aP \subset a \;\&\; P \supseteq a * b + b * a \supseteq a + b \supseteq a, b\ ,$$

and some $k \in \mathbf{N}$ with

$$P \not\supseteq P^k * a \;\;\&\;\; P^k \supseteq a \;\; (\forall\, n \in \mathbf{N})\,.$$

But, on the grounds of $P^k \supseteq a * b + b * a \supseteq b$ this would lead to the contradiction

$$P \supseteq b * a \supseteq P^k * a \not\subseteq P\,.$$

Next, by $a(a * b + b * a) = a$ the sum $a + b$ proves to be a left divisor of a (and b), because

$$\begin{aligned} a &= a(a * b + b * a) \\ &= a(a * b) + a(b * a) \\ &= b(b * a) + a(b * a) \\ &= (b + a) \cdot (b * a)\,. \end{aligned}$$

Let us assume now $P^m \supset X \supset P^{m+1}$. Then there exist elements a, b satisfying

$$a \subseteq P^m \;\;\&\;\; a \not\subseteq X \;\;\&\;\; b \subseteq X \;\;\&\;\; b \not\subseteq P^{m+1}\,.$$

Hence, because $a * b = (a + b) * b \not\subseteq P$, including $P + a * b \supset P$, we get:

$$\begin{aligned} P^{m+1} + a + b &= (P^{m+1} + (a + b)) \cdot (P + a * b) && (\text{by } (*)) \\ &= P^{m+1}(P + a * b) + (a + b)P + (a + b) \cdot (a * b) \\ &= P^{m+1} + b\,, && (\text{by } \; P^{m+1} \supseteq (a + b)P) \end{aligned}$$

opposite to $a \not\subseteq P^{m+1} + b$. Consequently condition (S) is satisfied, too. $\square$

8. 4. 2 Proposition. *Let $\mathfrak{A}$ be an LD-AML. Then $\mathfrak{A}$ is a multiplication AML iff it satisfies the conditions* (A) *and* (J) *.*

PROOF. First of all we verify $A \supset P \Longrightarrow AP = P = PA$ that is condition (I). To this end we recall duality and suppose that some prime element P

would satisfy the inclusion $A \supset P \supset AP$. Then according to (A^ℓ) there would exist some $n \in \mathbf{N}$ with $A^n \supseteq P$ and $A^{n+1} \not\supseteq P$, and, because

$$P * A^{n+1} \ \supseteq \ A^n * A^{n+1} \supseteq A \supseteq P$$

we would get

$$\begin{aligned} P * A^{n+1} &= P + P * A^{n+1} \\ &= A^{n+1} * P + P * A^{n+1} \end{aligned}$$

that is – by (J^*) –

$$P * A^{n+1} \ = \ (P * A^{n+1})^2 ,$$

and therefore, according to (A^r), furthermore

$$A^{n+1} \ \supseteq \ P \cdot (P * A^{n+1}) = P ,$$

a contradiction!

We now verify condition (B), starting from $P \supseteq P^n * B$ $(\forall n \in \mathbf{N})$, in particular $P \supseteq B$. If then each P^n contains B, we are through by condition (A). In the opposite case there exists some $P^m \not\supseteq B$, leading to $P^m \supseteq B(B * P^m) \supseteq B(B * P)^m$ that is $P \supseteq B * P$, since otherwise (I) would imply $P(B * P)^n = P$ which then by (A) would lead to $B(B * P)^m = B$ that is $P^m \supseteq B$, a contradiction. Hence we get $P \supseteq P^m * B + B * P \supseteq P^m * B + B * P^m \supseteq B$, and thereby – according to (J) – $P^n \supseteq B$ $(\forall n \in \mathbf{N})$, whence by condition by (A) we get $PB = B = BP$. □

The characterization of the preceding proposition reflects the characterization of Dedekind domains in an optimal manner. Apart from other characterizations Larsen/McCarthy, for instance, give as one central description of Dedekind domains the Noether property together with the equation $(a) : (b) + (b) : (a) = (1)$. But as is easily seen the archimedean property (A) results from the Noether property and $(a) : (b) + (b) : (a) = (1)$ leads to $A : B + B : A = (1)$ for finitely generated ideals – here for all ideals, consult the proof of 7.2.1. Thus (A) & (J) is formally weaker than the description of Dedekind domains above, but still strong enough in the most general case of an LD-AML in order to imply condition (M).

8.5 The Divisor Case

8. 5. 1 Proposition. *Let $\mathfrak{A}$ be an AML, generated by compact divisors. Then $\mathfrak{A}$ is a multiplication AML iff $\mathfrak{A}$ satisfies the conditions* (J) *and* (T) *.*

PROOF. We show that all prime elements P are divisors.

First of all – by (J) and (T) – we get $a(a*b+b*a) = a$ and $a+b\,|_\ell\, b$ – consult the proof of 8.4.1 This leads to condition (I), since from $A \supseteq a$ & $P \not\supseteq a$ & $P \supseteq p$ we get $(a+p)(a*p) = p$ with $P \supseteq a*p$, and thereby $AP \supseteq A(a*p) \supseteq p$ which leads to $AP = P$, and thereby to (I) – by duality, and to (G) by (I) and (T).

Next it results condition (S), consult the proof of 8.4.1

Assume now that P is an idempotent prime element. Then P is a divisor by condition (T).

Otherwise, let P be a not idempotent prime element. Then we continue as follows:

Condition (J) implies $(C^{*\prime})$ that is in particular $P^m \supseteq B$ & $P^{m+1} \not\supseteq B \Longrightarrow P \not\supseteq P^m * B$, since

$$\begin{array}{rcl}
P \supseteq P^m * B & = & (P^{m+1} + B) * B \\
\text{leads to} \quad P & \supseteq & P^{m+1} * B + P \\
 & = & P^{m+1} * B + P^m * P^{m+1} \\
 & = & P^{m+1} * B + (B + P^{m+1}) * P^{m+1} \\
 & = & P^{m+1} * B + B * P^{m+1} \\
 & \supseteq & P
\end{array}$$

from which by (J) would follow $P^2 = P$. Hence by (S) we get (X) along the proof of 8.3.1 And this leads to commutativity – again along that proof.

Finally suppose $a \subseteq P$ and $a \not\subseteq P^2$. Then for all $p \subseteq P$ it follows $a+p \subseteq P$. We consider such an $a+p =: B$. It holds $P \supseteq B$. So we get first $BX \subseteq P^2 \Longrightarrow P^2 = P^2 + (P^2+B)X = P^2 + PX = P(P+X)$ leading to $B*P^2 = P$, whence we get further $P^2*B+B*P^2 = (P^2+B)*B+B*P^2 = (P*B+P)^2$. But this means either $P \supseteq P*B$ and thereby $P^2 = P$, a contradiction, or $P + P * B \supset P$. Consequently we get – recall commutativity:

$$\begin{array}{rcl} B & \supseteq & P(P * B) \\ & \supseteq & (P \cap (P * B)) \cdot (P + (P * B)) \\ & \supseteq & P \cap (P * B)(\text{ by (I)}, \text{(T)}) \\ & \supseteq & B \\ \text{and thereby} \qquad P \mid B & = & a + p \mid p\,. \end{array}$$

This completes the proof □

A Hint. The assumption might arise that in ideal semigroup condition (M) results already from condition (B) (without any further requirement).

That this is not the case, even though $\mathfrak{A}$ should be lattice distributive, is shown by the example of a zero-monoid ($a \neq 1 \neq b \Longrightarrow ab = 0$) with respect to its Rees ideals.

8.6 Further Criteria

8. 6. 1 Proposition. *An arbitrary AML $\mathfrak{A}$ is a multiplication AML iff it satisfies the conditions* (B) *and* (S) *.*

PROOF. Let P be prime and assume $A \supset P$. Then $P \supseteq AX \Longrightarrow P \supseteq X$, meaning $A * P = P$. Hence we are led to:

$$\begin{array}{rcl} A \supset P \supseteq B & \Longrightarrow & A \supset P = A^n * P \\ & \supseteq & A^n * B \ \ (\forall\, n \in \mathbf{N}) \\ & \Longrightarrow & AB = B\,, \end{array}$$

that is – by duality – condition (G).

Next recall

(S) $$P^n \ \succeq \ P^{n+1}$$

Let now $P^s \supseteq B$ & $P^{s+1} \not\supseteq B$ be satisfied. Then we get $P \not\supseteq P^s * B$, since it holds

$$\begin{array}{lrcl} & P^s \supseteq B & \& & P^{s+1} \not\supseteq B\,, \\ \text{leading to} & P*(P^s*B) & = & P^{s+1}*B \\ & & = & (P^{s+1}+B)*B \\ & & = & P^s*B \\ \text{leading to} & P^k*(P^s*B) & = & P^{k+s}*B \ \ (\forall k\in\mathbf{N}) \\ & & = & P^s*B \\ \text{leading to} & (\star) \qquad P & \not\supseteq & P^s*B\,, \end{array}$$

the final conclusion since otherwise (B) would imply $P(P^s*B)=P^s*B$ and thereby $P^{s+1}\supseteq P^s*B\supseteq B$. This proves the assertion.

Next we get

$$A \ = \ \bigcap P_i^{\,e_i} \quad (P_i^{\,e_i}\supseteq A)\,.$$

To this end suppose $\bigcap P_i^{\,e_i}\ \ (P_i^{\,e_i}\supseteq A)=: B\supset A$. Then there would exist at least one $b\subseteq B$ satisfying $b\,(B*A)\subset b$ which by 5.4.8 would provide a prime element $P\supseteq B*A$ with $b\cdot P\subset b$, and by (B) it must exist some $m\in\mathbf{N}$ with $P\not\supseteq P^m*A$. But this leads to the contradiction

$$P\not\supseteq P^m*A \ \subseteq \ B*A\subseteq P\,.$$

Thus – on the grounds of (S) – it results furthermore

$$\text{(X)} \qquad P\supseteq X\supseteq P^n \implies X=P^\ell \ \ (\exists \ell\in\mathbf{N})\,,$$

observe that in case of $P^e\supseteq X$ & $P^{e+1}\not\supseteq X$ it follows:

$$X\supseteq P^e\cdot(P^e*X)=P^e\cdot(P^e*X+P^{n-e})\supseteq P^e\cdot(P^e*X+P)^e \overset{(\star)}{=} P^e\,.$$

Hence each $U,V\in\mathcal{A}$ commutes, observe that in case of $P^e\supseteq UV$ we get

$$P^e=P^e+UV=P^e+(P^e+U)\cdot(P^e+V)=P^e+VU\,.$$

Now we are in the position to show that any prime element is even a prime divisor. To this end we suppose first $P^n\supseteq B\ \ (\forall n\in\mathbf{N})$ and assume $P\supseteq P^n*B\ \ (\forall n\in\mathbf{N})$. Then we are through by condition (B).

Otherwise there is some $m \in \mathbf{N}$ satisfying $P^m \supseteq B \;\&\; P \not\supseteq P^m * B$. In this case we get – according to commutativity –

$$\begin{array}{rll} B & \supseteq & P^m(P^m * B) \\ & \supseteq & (P^m \cap (P^m * B)) \cdot (P^m + (P^m * B)) \\ & \supseteq & (P^m \cap (P^m * B)) \cdot (P + (P^m * B))^m \\ & \supseteq & P^m \cap (P^m * B) \qquad\qquad\qquad (\mathrm{G}) \\ & \supseteq & B \end{array}$$

that is $\quad P^m \;\Big|\; B$.

This completes the proof by the prime criterion. □
We finish this section by some implications.

8. 6. 2 Proposition. *Any AML $\mathfrak{A}$ satisfies the implication:*

$$(\mathrm{H}) \implies (\mathrm{I})\,.$$

PROOF. It holds in general $(A \supset P \;\&\; Q\ P\text{-primary}) \implies (AQ = Q)$, since one infers $Q \supset AQ \;\&\; AQ\ P$-primary & $\operatorname{Rad} AQ = P \not\supseteq A$ implies $AQ \supseteq Q$. □

8. 6. 3 Proposition. *Any AML $\mathfrak{A}$ satisfies the implication:*

$$(\mathrm{F}) \;\&\; (\mathrm{H}) \implies (\mathrm{A})\,.$$

PROOF. By condition (H) all prime powers P^m are primary. Hence we get:

$$P^m \supseteq AB \;\&\; P \not\supseteq A \implies P^m \supseteq B\,.$$

We continue similarly to the proof of 8.1.6: To this end suppose again $A^n \supseteq B$ $(\forall\, n \in \mathbf{N})$. Then for prime elements P_i we get

$$\begin{array}{ll} & {P_i}^{e_i} \supseteq BA \\ \implies & (P_i \supseteq A \rightsquigarrow {P_i}^{e_i} \supseteq B) \vee (P_i \not\supseteq A \rightsquigarrow {P_i}^{e_i} \supseteq B)\,. \end{array}$$

But this would lead to $BA = B$, according to condition (F).

The rest follows by duality. □

8.7 Left Prüfer Cases

We start with

8. 7. 1 Lemma. *Let $\mathfrak{A}$ be a left Prüfer structure and let P be prime. Then $P \not\supseteq A$ implies $AP \supseteq PA$.*

PROOF. By $P \not\supseteq A$ there exists some $a \subseteq A$ with $P \not\supseteq a$ and hence with $P \not\supseteq a + a_i$ for all $a_i \subseteq A, a_i \in \mathcal{A}_c$. So, we get $P \cdot (a + a_i) = (a + a_i) \cdot X_i \rightsquigarrow P \supseteq X_i \rightsquigarrow P \cdot A \subseteq A \cdot P$. □

8. 7. 2 Proposition. *A left Prüfer monoid* [3] $\mathfrak{A}$ *is an M-monoid iff* $\mathfrak{A}$ *satisfies*

$$\text{(B)} \qquad \begin{aligned} & A \supseteq A^n * B \ \ (\forall\, n \in \mathbf{N}) \Longrightarrow AB = B \\ \& \quad & A \supseteq B : A^n \ \ (\forall\, n \in \mathbf{N}) \Longrightarrow BA = B\,. \end{aligned}$$

PROOF. Sufficiency. First of all we get

$$\text{(G)} \qquad A \supset P \supseteq C \ \Longrightarrow\ AC = C = CA$$

applying $A \supset P \supseteq C \Longrightarrow A \supseteq P = A * P = A^n * P \supseteq A^n * C$ and its dual.

Assume now $P^m \supseteq X \supset P^{m+1}$ and $P^m \supseteq a \ \&\ X \supseteq b \not\subseteq P^{m+1}$. Then $(a + b)(a * b) = b$ leads to $P \not\supseteq a * b$ and hence to

$$\begin{aligned} P^{m+1} + (a + b) &= (P^{m+1} + (a + b)) \cdot (P + a * b) \\ &= P^{m+1}(P + (a * b)) + (a + b)P + (a + b)(a * b) \\ &= P^{m+1} + b\,. \end{aligned}$$

In particular, by (5.26) this means that there are only powers of P between $1 \neq P$ and $P^m \neq 1$.

Next we prove

$$\text{(LA)} \qquad P^n \supseteq b \ \ (\forall\, n \in \mathbf{N}) \ \Longrightarrow\ bP = b\,.$$

Case 1: If $P^n \succ P^{n+1}$ $(\forall\, n \in \mathbf{N})$ then $Q = \bigcap P^n$ is prime, since (G) implies (I). Hence we get $bP = b$ by (G), observe $P \supset Q \supseteq b$.

Case 2: If $P^e = P^{e+1}$ and $P \supseteq b : P^n$ $(\forall\, n \in \mathbf{N})$ then $bP = b$ by (B).

[3] The reader will easily verify that we will apply only $(a + b)(a * b) = b$.

Case 3: If $P^e = P^{e+1}$ and $P \not\supseteq b : P^m$ $(\exists\, m \in \mathbf{N})$ then it holds all the more $P \not\supseteq b : P^e$ leading by 8.7.1 to $(b : P^e)P^e \supseteq P^e(b : P^e)$. This implies

$$\begin{aligned} b &\supseteq (b : P^e)P^e \\ &\supseteq (b : P^e + P^e)(b : P^e \cap P^e) \\ &\supseteq (b : P^e + P)^e(b : P^e \cap P^e) \\ &\supseteq (b : P^e \cap P^e) \\ &\supseteq b \end{aligned}$$

that is $b = (b : P^e)P^e = (b : P^e)P^e \cdot P = bP$.

Now we are in the position to show that $\mathfrak{A}$ is commutative.

To this end suppose $\bigcap P_i{}^{e_i}$ $(P_i{}^{e_i} \supseteq A) =: B \supset A$. Then there exists at least one $b \subseteq B$ satisfying $b\,(B * A) \subset b$, and by 5.4.8 this provides a prime element $P \supseteq B * A$ with $b \cdot P \subset b$.

We verify that both, $P \supseteq P^n * A$ $(\forall\, n \in \mathbf{N})$ and $P \not\supseteq P^m * A$ $(\exists\, m \in \mathbf{N})$ are impossible.

Case A. Assume first $P \supseteq P^n * A$ $(\forall\, n \in \mathbf{N})$. Then by (LA) it results

$$\begin{aligned} AP = A &\leadsto P^n \supseteq A \ \ (\forall\, n \in \mathbf{N}) \\ &\leadsto P^n \supseteq B \ \ (\forall\, n \in \mathbf{N}) \\ &\leadsto P^n \supseteq b \ \ (\forall\, n \in \mathbf{N}) \\ &\leadsto bP = b\,. \end{aligned}$$

Thus the assumption $P \supseteq P^n * A$ $(\forall\, n \in \mathbf{N})$ leads to a contradiction.

Case B. Assume now $P \not\supseteq P^m * A$ $(m \in \mathbf{N})$. This implies $P \supseteq B * A \supseteq P^m * A \not\subseteq P$, again a contradiction.

Hence it must hold $A = B$.

Next, by (G) and (5.26) we get $P^1 \supseteq B \supseteq P^n \Longrightarrow B = P^\ell$. So each $U, V \in \mathcal{A}$ commutes since – compare above –

$$\begin{aligned} P^e \supseteq UV &\Longrightarrow P^e = P^e + UV \\ &\overset{(5.8)}{=} P^e + (P^e + U) \cdot (P^e + V) = P^e + VU\,. \end{aligned}$$

Finally assume $P^n \supseteq B$ & $P^{n+1} \not\supseteq B = \bigcap_{i \in I} P_i^{e_i}$. Then by (G) we may suppose that P and all prime elements P_i are minimal over B, since $P_i \supset P_j$ implies $P_j{}^n \cap P_i = P_i$ $(\forall\, n \in \mathbf{N})$ and $P * P_i^{e_i} = (P + P^{e_i}) * P_i^{e_i} = P_i^{e_i}$. So we get $P^n * (P^n * B) = P^n * \bigcap_{P_i \neq P} P_i^{e_i} = \bigcap_{P_i \neq P} P_i^{e_i}$, that is by (G) the implication $Q \supseteq B \Longrightarrow Q \,|\, B$ – for arbitrary prime elements Q.

Thus we are finished by the **prime criterion** 8.1.7, which in the commutative case – as it is given here – will turn out as a consequence of the **divisor lemma**, presented in the next section. However, also another calculation is possible, as will be shown in the next proof. □

We now turn to Prüfer cases.

8. 7. 3 Proposition. *A Prüfer monoid* $\mathfrak{A}$ *is an M-monoid iff satisfies*

$$\text{(PE)} \qquad a \;=\; a\cdot(a*B+B*a)$$

$$\text{(PS)} \qquad P\supset P^2 \;\Longrightarrow\; P\succ P^2$$

$$\text{(PU)} \qquad P=P^2\supseteq p \;\Longrightarrow\; P\,|\,p\,.$$

PROOF. Clearly conditions (PE) and (PU) are necessary and we get (PS) *via* $P\supseteq X\supset P^2 \Longrightarrow X=PY=P(Y+P)\supset P^2 \Longrightarrow P+Y\supset P$ which under (M) leads to $X=P$.

Let now (PE), (PU), and (PS) be satisfied. We show that all prime elements P are divisors:

If P is idempotent, this is clear by (PU).

If P is not idempotent assume $P\supseteq p$ and $P\supseteq a$ & $P^2\not\supseteq a$. We shall show $P\,|\,a+p=:b$ which implies $P\,|\,p$.

First assume $P\supseteq P*a$. Then it holds $a=a\cdot(a*P^2+P^2*a)=a((a+P^2)*P^2+(P^2+a)*a)=a\cdot(P*P^2+P*a)\subseteq aP\subseteq P^2$, a contradiction to $a\not\subseteq P^2$.

So P cannot contain $P*a$ whence we get $P\not\supseteq P*(p+a)$. Put $B:=p+a$. Then by 8.7.1 and 7.3.9 we obtain:

$$\begin{aligned} P\cdot(P*B) &\supseteq (P\cup P*B)\cdot(P+P*B)\\ &= P\cup P*B\supseteq B \rightsquigarrow P\cdot(P*B)=B\,. \end{aligned}$$

Therefore – by duality – all prime elements are prime divisors.

Suppose now $A\supseteq b$ and $b\supset A(A*b)=b\cdot(b*A(A*b))$. Then by 5.4.8 there exists a prime element P containing $b*A(A*b)\supseteq A\cdot(A*b)$, which leads to $P\supseteq A \vee P\supseteq A*b \rightsquigarrow P\,|\,b$ and satisfying $bP\neq b$.

Next assume $P^e \,|_\ell\, b$ but $P^{e+1} \nmid b$. Then it results:

$$\begin{aligned} P^e \cdot P &\supseteq b \cdot P \supseteq A(A * b) \\ &\supseteq A(P^e * b) \\ &\supseteq P^e \cdot (P^e * b) \\ &= P^e \cdot (P + P^e * b)) = b\,. \end{aligned}$$

This means $P^n \supseteq b \ \ (\forall\, n \in \mathbf{N})$.

We consider first $P^n \succ P^{n+1}$ $(\forall\, n \in \mathbf{N})$. Here – by 7.3.5 – the element $Q := \bigcap P^n \ \ (n \in \mathbf{N})$ would be a prime divisor of b implying $bP = b$.

Next we consider $P^m = P^{m+1}$ $(\exists\, m \in \mathbf{N})$. In this case we get – by (U) – $Y \cdot P^m = b = bP \ \ (\exists\, Y)$, since $P^k \neq P^{k+1}$ & $X \cdot P^k = b$ & $P^{k+1} \supseteq b \Longrightarrow P^{k+1} = (P + X)P^k \Longrightarrow P \,|\, X \Longrightarrow P^{k+1} \,|\, b$.

Thus the proof is complete. □

8.8 The commutative Case

Mori AMLs are always commutative. Hence it doesn't mean a real restriction to start with commutativity. Right- left- interpretations then usually are of success also in the non commutative case. But it seems to the author that the characterizing conditions don't become simpler.

On the other hand, certain notions of commutative algebra are based on commutativity. So we add some systems, not only implying but even containing commutativity.

First of all we recall 6.2.5, that is (G)$\Longleftrightarrow \ker A = A \ \ (\forall\, A \in \mathcal{A})$.

Next we take up 8.4.1 and get in particular

8. 8. 1 Corollary. *A commutative ring with identity* 1 *is a multiplication ring iff it satisfies condition* (B) *and if in addition its ideal lattice is distributive.*

Furthermore we remark:

8. 8. 2 Lemma. *Every commutative ideal semigroup* $\mathfrak{A}$ *satisfies the implication*

$$\text{(G) \& (H}^0) \ \Longrightarrow\ \text{(F) \& (A)}\,.$$

PROOF. Since $\mathfrak{A}$ is commutative, according to (H^0) each primary element of $\mathfrak{A}$ is a prime power, since the generators are assumed to be compact divisors. Consequently by condition (G) also condition (F) is satisfied, and furthermore it results condition (H), since on the grounds of the given circumstances every prime power P^n is the intersection of all its isolated primary components, each of which is of type P^e. Consequently condition (A) is valid, according to 8.6.3 □

By 8.4.2 the preceding lemma provides

8. 8. 3 Corollary. *A commutative ideal semigroup is a Mori AML iff it satisfies the conditions* (G), (H^0), *and* (J).

We finish this section by an alternate proof of a result due to MOTT, [304]:

8. 8. 4 Proposition. *Let $\mathfrak{R}$ be a commutative ring with identity and $\mathfrak{A}$ be its ideal semigroup. Then $\mathfrak{R}$ is a multiplication ring iff it satisfies:*

(*i*) *If* $\operatorname{Rad} Q = P$ *is prime, then* $Q = P^n$ $(\exists n \in \mathbf{N})$.

(*ii*) *Each ideal is equal to its kernel.*

(*iii*) *If Q_i is an isolated P-primary component of A then P does not contain the intersection of the remaining isolated primary components of A.* [4)]

PROOF. As is easily seen, this characterization is equivalent to the combined conditions (H^o) & (F) & (E). Let now these conditions be satisfied.

Then it follows first in case of some prime element P with $A \supseteq P$ that $AP =: Q$ is P-primary with $\operatorname{Rad} Q = P \not\supseteq A$, leading to $Q \supseteq P$, leading to $AP = P$, i. e. condition (I).

Next, by evidence, exactly all prime powers are primary whence (H) and (H^o) coincide. But this implies condition (A) by 8.6.3.

Finally (E) implies (C) for prime elements P since

$$\begin{aligned} & P^n = B : c \;\&\; P \supseteq P^n * B \\ \Longrightarrow\;& P \supseteq P^n * (B : c)c = P^n * P^n \cdot c \supseteq c\,. \end{aligned}$$

[4)] This result is true also for arbitrary commutative ideal semigroups. However, since we did not develop the notion of a kernel, we have to restrict our assertion here to the ring case.

This completes the proof. □

Recall again: The proofs of this chapter do not depend on compactness of the identity. This means in the case of a ring $\mathfrak{R}$ without identity that we may change to the ideal semigroup $\mathfrak{R}$ enlarged by an element 1. Maybe that this adjoined identity is not compact in the extended ideal semigroup, but nevertheless by replacing (J) through (C) we get the ring theoretical results of Mott, [304], and Gilmer/Mott, [163].

Chapter 9

Classical Ideal Structures

9.1 Preface

Again, all multiplicative structures of this chapter are supposed to be commutative. We consider a commutative ring with identity 1 and a *lattice group cone.*

In both cases we are faced with lattice modular ideal semigroups, the d-ideal-semigroup on the one hand, and the filter semigroup on the other hand. In each of these cases any $\mathfrak{A}/P =: \overline{\mathfrak{A}}$ with prime element P is cancellative with 0, for short, each of these ideal semigroups is P-cancellative.

Moreover, recall that 5.5.5 entails that any ringlike Prüfer DV-IDM is P-cancellative, because $ax = ay \Longrightarrow a(x \wedge y)x' = a(x \wedge y) \Longrightarrow x' = 1$.

In this chapter we give some examples showing how modularity and the P-cancellation property work together, but no theory in general is attempted – much more should be possible. So, after general definitions, we will restrict ourselves to studying modular P-cancellative commutative DV-IDMs, even though much material could be carried over to weaker situations.

9. 1. 1 Definition. Let $\mathfrak{A}$ be an AMV. We call $\mathfrak{A}$ *P-cancellative* if for all prime elements P the homomorphic image $\mathfrak{A}/P =: \overline{\mathfrak{A}}$ satifies the condition

$$\overline{a} \cdot \overline{X} = \overline{a} \cdot \overline{Y} \Longrightarrow \overline{a} = \overline{0} \vee \overline{X} = \overline{Y}\,.$$

Furthermore we call $\mathfrak{A}$ *classical* if it is P-cancellative and lattice modular.

In particular – according to 5.5.2 and 5.5.3 – in the classical case $\mathfrak{A}/P$ is generated by cancellable generators.

Classical are, as shown above, all ringlike Prüfer AMLs and, as will be shown below, every modular AML which is generated by a semigroup of cancellable elements. Classical is as well the semigroup of ideals of a commutative ring without identity, extended by an identity.

9.2 Modular Divisor Ideal Monoids

First of all recall 5.5.4, that is:

9. 2. 1 Lemma. *Let $\mathfrak{A}$ be modular and as $\sum$-ideal semigroup generated by a set $\mathcal{A}_0$ of compact divisors.*

Then in case that the elements $a \neq 0$ of $\mathcal{A}_0$ are cancellable in $\mathfrak{A}$ and that P is prime, $\mathfrak{A}_0/P =: \overline{\mathfrak{A}}_0$ is integral w.r.t. $(\overline{\mathcal{A}}_0)$.

9. 2. 2 Lemma. *Let $\mathfrak{A}$ be a modular Noether DV-IDM. Then every $\cap$-irreducible Q is primary.*

PROOF. Let Q be $\cap$-irreducible and $ax \subseteq Q$, but $x \not\subseteq Q$. Then, for some $n \in \mathbf{N}$, it follows from the ascending chain condition

$$a * Q \subseteq a^2 * Q \subseteq a^3 * Q \subseteq \ldots \subseteq a^n * Q = a^{n+1} * Q$$

and furthermore with $Z := (Q + a^n) \cap (Q + x) \supseteq Q$ it holds the equation:

$$(Q + a^n) \cap Z = Z = (Q + x) \cap Z\,.$$

And this leads to:

$$\begin{aligned} Z &= Q + (a^n \cap Z) \\ &= Q + (x \cap Z) \\ &\rightsquigarrow \\ Z &= Q + a^n \cdot (a^n * Z) \quad (*) \\ &= Q + x \cdot (x * Z) \end{aligned}$$

$$
\begin{array}{rcl}
& \rightsquigarrow & \\
aZ & = & aQ + a^{n+1}(a^n * Z) \\
& = & aQ + ax \cdot (x * Z) \subseteq Q \\
& \rightsquigarrow & \\
a^{n+1} \cdot (a^n * Z) & \subseteq & aZ \\
& \rightsquigarrow & \\
a^n * Z & \subseteq & a^{n+1} * aZ \\
& \subseteq & a^{n+1} * Q = a^n * Q \\
& \rightsquigarrow & \\
Z & \overset{(*)}{=} & Q = Q + a^n \vee Q \\
& = & Q + x \\
& \rightsquigarrow & \\
a^n & \subseteq & Q\,,
\end{array}
$$

which had to be shown. □

The proof, presented here, is based on EMMY NOETHER's crucial idea of applying chain condition in algebraic number theory.

Another proof of 9.2.2, based on $r * A \supset A \Longrightarrow r^n * A = r^{n+1} * A \ \ (\exists n \in \mathbf{N})$ as well, was given by HOLZAPFEL in [193].

On the grounds of 9.2.2 in a modular Noether DV-IDM each $A \in \mathcal{A}$ is an intersection of primary elements. This means, see below, that the Noether property implies the archimedean property.

9. 2. 3 Definition. An AML is called *hyper-archimedean* if

(H-A) $\qquad \forall\, A, B\ \exists\, m \in \mathbf{N}: \quad A \cap B^m \subseteq A \cdot B$

As is easily seen the hyper-archimedean property implies the archimedean property. Moreover it is immediately seen that homomorphic images of hyper-archimedean AMLs are again hyper-archimedean. Hence, $\cdot\,, \cap$-homomorphic images of any hyper-archimedean AML are archimedean.

9. 2. 4 Proposition. *Let $\mathfrak{A}$ be a not necessarily lattice modular. Noether DV-IDM whose elements are intersections of primary elements. Then $\mathfrak{A}$ is hyper-archimedean .*

PROOF. Suppose $Q \supseteq AB$ but $Q \not\supseteq A$. It follows $\operatorname{Rad} Q \supseteq B$, and hence, because of the Noether property, $Q \supseteq B^n \ \ (\exists n \in \mathbf{N})$. Thus we get

$A \cdot B \supseteq A \cap B^m \ (\exists m \in \mathbf{N})$, i. e. (H-A). □

In integral domains $\mathfrak{R}$ the archimedean property implies that nonunits r satisfy

(ar) $$\bigcap \langle r \rangle^n = \langle 0 \rangle .$$

On the other hand, if (ar) is satisfied, then principal ideals have the archimedean property in the sense of this paper.

(ar) seems to be introduced by SHELDON in [389]. But the stronger archimedean property in our sense seems to be unsettled up till now. However, it should be stressed that the archimedean property of commutative Noether rings with identity 1 is an immediate consequence of ARTIN-REES.

Finally, by 8.6.2, 9.2.2, 9.2.4 we get:

9. 2. 5 Proposition. *Let $\mathfrak{A}$ be a modular Noether DV-IDM. Then the following are equivalent:*

(*i*) $\ker A = A$

(*ii*) $\operatorname{Rad} Q$ *prime implies* Q *primary*.

PROOF. $(i) \Longrightarrow (ii)$ follows by definition.
$(ii) \Longrightarrow (i)$. Because of the Noether property every A is intersection of $\cap$-irreducible and hence by modularity an intersection of primary elements. Furthermore condition (I) is satisfied on the grounds of (ii), i. e. condition (H), according to 8.6.2. Consequently, by the Noether property, primary elements Q satisfy the inclusion $Q \supseteq (\operatorname{Rad} Q)^n$ for some suitable n and by (ii) it follows

($\star$) $$\operatorname{Rad} Q_1 = P_1 \supset P_2 = \operatorname{Rad} Q_2 \Longrightarrow Q_1 \cdot Q_2 = Q_2 .$$

Furthermore we may assume that different elements $Q_i \ (1 \leq i \leq n)$ have different radicals P_i, since the meet of two P-primary elements is again P-primary.

Therefore primary decompositions $Q_1 \cap \ldots \cap Q_n$ are equal to their associated product $Q_1 \cdot \ldots \cdot Q_n$, which is shown as follows:

Let $Q_1 \cdot \ldots \cdot Q_n$ be associated with the primary decomposition $Q_1 \cap \ldots \cap Q_n$. We denote $\operatorname{Rad} Q_i$ by P_i. Then, if $i \neq j$ we obtain first $P_i \not\supseteq P_j$ & $P_j \not\supseteq P_i$ and thereby according to ($\star$) furthermore $(Q_i + Q_j) \cdot Q_j = Q_j$, since every prime element P containing both, Q_i and Q_j, contains P_j even properly. And this provides by induction, if the assumption is proven already for all k with $1 \leq k \leq n$:

$$\begin{array}{rcl} Q_1 \cdot (Q_2 \cdot \ldots \cdot Q_n) & \supseteq & (Q_1 + \prod Q_i) \cdot (Q_1 \cap \prod Q_i) \;\; (2 \leq i \leq n) \\ & = & (Q_1 + \prod Q_i) \cdot (Q_1 \cap \bigcap Q_i) \\ & \supseteq & (\prod (Q_1 + Q_i)) \cdot (Q_1 \cap \bigcap Q_i) \\ & = & Q_1 \cap \bigcap Q_i \\ & \rightsquigarrow & \\ Q_1 \cdot \ldots \cdot Q_n & = & Q_1 \cap \ldots \cap Q_n \,. \end{array}$$

So it remains to show that the P_i under consideration are minimal over A. To this end assume the opposite. Then it follows $P_i \supset P \supseteq P_j$ for some prime P, minimal over A, and at least one i, j with $1 \leq i, j \leq n$. But this leads to $P_i \supset Pj$ for at least one pair P_i, P_j, a contradiction! □

9.3 Classical Divisor Ideal Monoids

In a commutative Noetherian multiplication ring $\mathfrak{R}$ with identity, for short a Noetherian M-ring, any $\mathfrak{a}$ is a product of prime ideals $\mathfrak{p}_\mathfrak{i}$.

Coincidentally classical DV-IDMs satisfy:

9. 3. 1 Proposition. *Let $\mathfrak{A}$ be a classical DV-IDM. Then the following are equivalent:*

- (i) *Each A of $\mathfrak{A}$ is a product of primes.*
- (ii) *$\mathfrak{A}$ is a Mori AML with Noether property.*

PROOF. We succeed along classical lines, cf. [268].

$(ii) \Longrightarrow (i)$: Consult the proof of 12.1.1

$(i) \Longrightarrow (ii)$. First of all we show that condition (I) ($A \supset P \Longrightarrow AP = P$) is satisfied. According to (i) this will imply that $\mathfrak{A}$ is a Mori AML.

On this we choose and fix for some given prime element P some $a \not\subseteq P$ and consider the elements $P + a^2$ and $(P+a)^2$ with prime factorizations

$$P + a^2 = P_1 \cdot \ldots \cdot P_m \;\text{ and }\; (P+a)^2 = Q_1 \cdot \ldots \cdot Q_n \,.$$

Then all P_i $(1 \leq i \leq m)$ and all Q_j $(1 \leq j \leq n)$ are sup-elements of P satisfying thereby w.r.t. $\overline{X} := P + X$

$$\overline{P}_i \supseteq \overline{Q}_j \supseteq \overline{P}_k \iff P_i \supseteq Q_j \supseteq P_k \ .$$

But by assumption the elements $\overline{a}$ und $\overline{a}^2 = \overline{a^2}$ are cancellable in $\overline{\mathfrak{A}}$.

Consequently, as divisors of $\overline{a^2}$, the elements $\overline{P}_i$ and $\overline{Q}_j$ are cancellable in $\overline{\mathfrak{A}}$, too.

We now show that in $\overline{\mathfrak{A}}$ condition (I) is satisfied at least for prime factors of $\overline{a^2}$ and infer then that $\mathfrak{A}$ satisfies condition (I) in general.

To this end we consider $\overline{P}_i \supset \overline{P}_k$. Here we get first $\overline{S} \cdot \overline{P}_i = \overline{a}^2 \supseteq \overline{S} \cdot \overline{P}_k \quad (\exists S)$ and thereby furthermore

$$\begin{aligned}
\overline{S} \cdot \overline{P}_k &= \overline{S} \cdot \overline{P}_i \cdot (\overline{S} \cdot \overline{P}_i \star \overline{S} \cdot \overline{P}_k) \\
&= \overline{S} \cdot \overline{P}_i \cdot (\overline{P}_i \star (\overline{S} \star \overline{S} \cdot \overline{P}_k)) \\
&= \overline{S} \cdot \overline{P}_i \cdot (\overline{P}_i \star \overline{P}_k) \\
&= \overline{S} \cdot \overline{P}_i \, \overline{P}_k \, .
\end{aligned}$$

So, by cancellation, it results:

$$\overline{P}_k = \overline{P}_i \cdot \overline{P}_k \ .$$

We go back to the prime factorizations above. Because of $\overline{a}^2 = \overline{a^2}$ and the prime property we get immediately that there exists for each $\overline{P}_i$ some $\overline{Q}_j$ with $\overline{P}_i \supseteq \overline{Q}_j$ and for each $\overline{Q}_j$ some $\overline{P}_k$ with $\overline{Q}_j \supseteq \overline{P}_k$. But according to condition (I) and the cancellation property this means that each $\overline{P}_i$ is a $\overline{Q}_j$ and each $\overline{Q}_j$ is a $\overline{P}_i$, because of irredundancy.

Hence the overlined prime factor products and thereby the corresponding original products coincide up to permutation. But this provides

$$P + a^2 = (P + a)^2 \, ,$$

and thereby

$$\begin{aligned}
P &\subseteq P^2 + Pa + a^2 \\
&\leadsto \\
P &= P \cap ((P^2 + Pa) + a^2) \\
&= (P^2 + Pa) + (P \cap a^2) \\
&= P^2 + Pa + a^2 \cdot (a^2 * P) \\
&= P^2 + Pa + Pa^2 \\
&= P(P + a) \, .
\end{aligned}$$

Consequently, if $A \supset P$, we get $P = P(P + A)$ *a fortiori.*

Thus condition (I) is verified and thereby condition (M) as well, since all elements are prime factor products.

We now show that $\mathfrak{A}$ has the Noether property.

Since each prime element is even completely prime, irredundant prime factor decompositions of the same A coincide up to permutation. Consequently $A \supset B$ implies that the irredundant prime decomposition of A admits a decomposition into a proper sub-product of the irredundant prime product of B, 1 included as a formal prime product, and a product of primes dividing at least one of the factors of the irredundant prime factor decomposition of B, 1 again included as a formal prime product.

But: any ascending chain, starting with a prime element, is finite.

For, if P and Q are prime with $P \supset Q$ then P is maximal and hence irreducible, since $1 \neq A \supset P$ would imply in $\mathfrak{A}/Q$ the contradiction $\overline{p}\cdot\overline{A} = \overline{p}$ for some $p \in P$, $p \notin Q$.

Consequently $\mathfrak{A}$ satisfies ACC or equivalently the Noether property. □

9. 3. 2 Proposition. *Let $\mathfrak{A}$ be a classical DV-IDM. Then the following are equivalent:*

- (*ii*) *$\mathfrak{A}$ is a Mori AML with Noether property.*
- (*iii*) *$\mathfrak{A}$ has the Noether property and each maximal element M of $\mathfrak{A}$ satisfies $M \succeq M^2$.* [1)]

PROOF. $(ii) \Longrightarrow (iii)$ follows from condition (X). It remains to show $(iii) \Longrightarrow (ii)$. According to 9.3.1 it suffices to prove $(iii) \Longrightarrow (i)$.

To this end we verify first condition (I). So, assume $M \supset P$. $\mathfrak{A}/P$ has the Noether property and thereby also the archimedean property, because of modularity according to 9.2.4. But this leads to $\bigcap M^n = P$, consult the proof of 10.2.10.

Hence, each prime element of $\mathfrak{A}$ is maximal or minimal and each pair P, Q of primes is *comparable* or *co-maximal* $(P+Q = 1)$. In particular different minimal primes are co-maximal .

1) Recall: this is Sono's condition, c.f. [400], [401].

Furthermore $M \supset P \Longrightarrow MP = P$ is satisfied by the archimedean property, and from this follows condition (I):

For $A \supset P \supset AP$ would imply the existence of some $M \supseteq A \supset P \supseteq p$ with maximal M and $p \supset p \cdot M$, a contradiction! Recall: $\mathfrak{A}$ is archimedean and $M \cdot P = P \supseteq p$.

We now turn to the Mori condition.

According to 9.2.2 and by the Noether property for any A there exists a primary decomposition $Q_1 \cap \ldots \cap Q_s$. Moreover, each primary element Q of $\mathfrak{A}$ satisfies $P = \operatorname{Rad} Q \supseteq Q \supseteq P^n$ $(\exists\, n \in \mathbf{N})$ – again by the Noether property.

Hence all primary elements whose radical is maximal are prime powers, according to (iii) and 7.3.1.

But, also the other primary elements are prime powers. To realize this, recall first that primes are maximal or minimal.

Let now $0 = Q_1 \cap \ldots \cap Q_m$ be a primary decomposition of 0 with P_i-primary Q_i $(1 \leq j \leq m)$. If then $m = 1$ it follows $Q_1 = 0 = P_1^n$ for some $n \in \mathbf{N}$, because of the Noether property. Otherwise we may start from two different isolated primary components Q_1, Q_2 with minimal co-maximal prime elements P_1, P_2 as radicals.

But then Q_1, Q_2 are co-maximal, too, since otherwise, the radicals of Q_1, Q_2 could not be co-maximal because

$$M \text{ maximal } \& \ Q \text{ primary } \& \ M \supseteq Q \Longrightarrow M \supseteq \operatorname{Rad} Q\,.$$

In particular each of both radicals is co-maximal to each power of the other one.

Hence for isolated primary components Q of 0 and minimal P we get by $P \supseteq Q \supseteq P^n$ that the prime power P^n must contain the primary component Q, since it contains 0 and since P is co-maximal to all primary components, different from Q. Thus we arrive at $Q = P^n$.

Let now $A = Q_1 \cap \ldots \cap Q_n$ be a primary decomposition with pairwise co-maximal components. Then, according to (5.8), it follows $A = Q_1 \cdot \ldots \cdot Q_n$ by the inclusion $X \cdot Y \supseteq (X \cap Y) \cdot (X + Y)$.

Thus it is proven that (ii) implies (i) and thereby (iii).

This completes the proof. $\square$

Chapter 10

Ringlike Ideal Structures

In this section all AMLs are assumed to be commutative.

The most essential problem of abstract ideal theory is an adequate description of what is called in concrete situations a principal ideal. This is impossible in general. For, consider the ideal structure of some Dedekind domain, it acts like the principal ideal structure of a principal ideal domain.

Nevertheless, in [103], ROBERT P. DILWORTH succeeded in characterizing the principal ideals of the polynomial rings over fields by defining principal elements T *via*:

$$\textbf{(MP)} \qquad T \cdot (A \cap T * B) \;=\; T \cdot A \,\cap\, B \qquad (\forall\, A, B)$$

$$\textbf{(JP)} \qquad T * (A + T \cdot B) \;=\; T * A + B \qquad (\forall\, A, B)\,,$$

where (MP) stands for meet principle ($\cap$- principle) and (JP) stands for join principle ($+$- principle).

Thus in [103] DILWORTH got into the position of completing his investigations on abstract commutative ideal theory, initiated by MORGAN WARD in [154] and afterwards continued by WARD and DILWORTH himself, compare the references. As one main result he presented an abstract proof of the celebrated THEOREM OF LASKER [1)].

It is not difficult to see that the principal ideals of commutative rings with identity are principal elements in the sense above. Furthermore it is easily checked that products of $+$- principal elements and products of $\cap$- principal elements, respectively, are again $+$- principal and $\cap$- principal,

[1)] to say it fair, the importance of LASKER's contribution results above all from its constructive methods.

respectively. Moreover, putting $A = 1$ in (MP) we get

$$\text{(PD)} \qquad T(T * B) \;=\; T \cap B\,.$$

Elements satisfying (PD) are called *weak meet principle* in *multiplicative lattice theory,* here they are called divisors, as usual in algebra.

Principal elements remain principal with respect to localization and residue class building, which is shown in [103], and will be shown for join principal elements under 10.2.5 and 10.2.2.

DILWORTH's principal elements and generalizations of it led to a tremendous renaissance of abstract ideal theory, initiated by D. D. ANDERSON in [4], and afterwards developed essentially under his leadership by himself and "his group". Roughly speaking it led to a branch of abstract ideal theory in its own right, closely along concrete ideal theory of commutative rings.

In this chapter we are concerned with ideal monoids, generated by compact join principle divisors, below the level of DILWORTH.

It will turn out that in the modular case the conditions (PD) and (JP) are stable w.r.t. residue class building and localization.

10.1 Starting ab ovo

Let $\mathfrak{R}$ be a commutative ring with identity 1 and $\mathfrak{A}$ its d-ideal semigroup. Then

$$\begin{aligned}
\langle a\rangle \subseteq B + \langle a\rangle C \;\Longrightarrow\; && a &= b + acx \;\; (\exists\, cx \in C)\\
\Longrightarrow\; && a\,(1 - cx) &= b\\
\Longrightarrow\; && \langle a\rangle * B &\perp C\,,
\end{aligned}$$

that is

$$\textbf{(RL)} \qquad \langle a\rangle \subseteq B + \langle a\rangle C \;\Longrightarrow\; (\langle a\rangle * B) \perp C\,.$$

Similarly in *cancellative* semi-rings – like *lattice group cones* – d-ideals, as defined above, satisfy (RL) since by suitable elements $x_i\,, y_i$ $(1 \leq i \leq n)$

one infers

$$\begin{aligned} \langle a\rangle \subseteq B + \langle a\rangle C \implies & \quad a &=& \ b_1x_1 + \ldots + b_nx_n + ac \\ \implies & \quad a\cdot 1 &=& \ a\cdot(y_1 + \ldots + y_n + c) \\ \implies & \quad 1 &=& \ y_1 + \ldots + y_n + c \\ \implies & \ \langle a\rangle * B &\perp& \ C\,, \end{aligned}$$

the final implication because $\langle a\rangle * B \supseteq \langle a\rangle * \langle y_1 + \ldots + y_n\rangle$. In particular for $B = 0$ condition (RL) leads to

(HN) $$\langle a\rangle U = \langle a\rangle \implies \langle a\rangle U^* = 0 \ \ (\exists\, U^* \perp U)\,.$$

10. 1. 1 Definition. An ideal structure is called *hyper-normal* if at least one basis $\mathcal{A}_c$ of compact divisors satisfies condition (HN) .

Condition (HN) is obviously satisfied by definition if every element of $\mathcal{A}_0$ is even $+$- *principal*, see above. But in this section we are concentrated in the hyper-normal situation.

Let $\mathfrak{A}$ be a hyper-normal *lattice modular* ideal structure. Then condition (HN) is even equivalent to condition (RL),

SINCE: $$\begin{aligned} a \subseteq B + aC \implies & \ a\cdot 1 = (a\cap B) + aC \\ \implies & \ a\cdot 1 = a\cdot(a*B + C) \\ \implies & \ \exists\, U^* : U^* \perp a*B + C \ \ \& \ \ a\cdot U^* = 0 \\ \implies & \ a*B = U^* + a*B \ \perp \ C\,. \end{aligned}$$

As an example we consider a commutative ring with identity 1. Choosing as basis the semigroup of principal ideals, here condition (HN) [2] is satisfied by the semigroup of d-ideals, but – it is also satisfied in *principal ideal rings,* what sort of ideals ever [3].

The notion hyper-normal suggests that the underlying structure is "at least" normal, compare 7.2.1. But this need not be true, even in the distributive case. To check this, the reader may study the r-ideal semigroup $\mathfrak{S}$ of

[2] Observe: In commutative monoids (HN) can be deduced from

(HN*) $\quad I + \langle a\rangle\cdot\langle x\rangle = I + \langle a\rangle\cdot\langle y\rangle \Longrightarrow \exists\, z:\ \langle a\rangle\cdot\langle z\rangle = \langle 0\rangle \ \ \&\ \ \langle x,z\rangle = \langle x,y\rangle = \langle z,y\rangle\,,$

a condition which like (RL) is always satisfied by d-ideals in commutative rings with identity.

[3] Recall $\langle a\rangle\cdot\langle b\rangle = \langle a\rangle \Longrightarrow ab \,\big|\, a \Longrightarrow a(bx-1) = 0$ with $\langle bx\rangle \perp \langle bx-1\rangle \rightsquigarrow \langle b\rangle \perp \langle bx-1\rangle$.

10. 1. 2 Example. *Define on* $\{1, x, y, z, 0\}$ *a commutative multiplication by* $xx = xy = yy = z$ *and* $zx = zz = zy = 0$ *and consider the ideal lattice. Then it holds* $(x)*(0+(x)(y)) = (x)+(y) \neq (y) = (z)+(y) = (x)*(0)+(y)$.

Condition (HN) implies always that $a(U^* + a * b) = a \cap b \rightsquigarrow a * b = U^*+a*b \ \ (\exists\, U^*)$ whence it results (HN) $\Longrightarrow$ (jn) if condition (e) is satisfied.

However, in general (HN) $\Longrightarrow$ (jn) does not hold, as is verified by

10. 1. 3 Example. *Let* $p \in \mathbf{N}$ *be prime and* $\{p^n\} \cup \{0\}$ *be the set* P *of its powers, extended by 0 and considered* w.r.t. *multiplication.*

Adjoin an element u *with* $1 \cdot u := u =: u \cdot 1$ *and* $ux := 0 =: xu \ \ (x \neq 1)$. *Here each principal ideal is even a* $+$ *- principal element, whence* $\mathfrak{S}$ *is hyper-normal. But in spite of this it holds:*

$$\langle u \rangle * \langle a \rangle + \langle a \rangle * \langle u \rangle \neq \langle 1 \rangle \,.$$

Under 5.5.1 it was shown that the mapping

$$\phi_A : X \longmapsto A + X =: \overline{X}\text{w.r.t.}\overline{X} \circ \overline{Y} := A + XY$$

provides a $\sum$- respecting homomorphism with algebraic image, satisfying

$$A_i \supseteq A \ \ (\forall\, i \in I) \ \Longrightarrow \ \phi_x(\textstyle\bigcap_{i\in I} A_i \ ) = \bigcap_{i\in I} \phi_x A_i \ .$$

Furthermore it was pointed out that in the modular case divisors are sent to divisors. We continue by studying the hyper-normal situation.

10. 1. 4 Proposition. *Let* $\mathfrak{A}$ *be a hyper-normal and (lattice) modular ideal structure and suppose* $A \in \mathcal{A}$ *. Then* $\mathfrak{A}/A =: \overline{\mathfrak{A}}$ *is hyper-normal (and modular) again.*

PROOF. By modularity condition (HN) is equivalent to condition (RL). Let now $\circ$ denote the multiplication of $\overline{\mathfrak{A}}$. Then it results:

$$\begin{aligned} \overline{b} \circ \overline{U} = \overline{b} \ &\Longrightarrow \ bU + A = b + A \\ &\Longrightarrow \ b \subseteq A + bU \\ &\Longrightarrow \ b * A \perp U \\ &\Longrightarrow \ \overline{b * A} \perp \overline{U} \end{aligned}$$

□

If $\mathfrak{A}$ is distributive, then – by 5.3.5 – condition (HN) is satisfied even for all compact elements $A := a_1 + \ldots + a_n \ \ (a_i \in \mathcal{A}_0)$. This follows by 5.3.5 *via*

$$A \cdot U = A \ \Longrightarrow \ a_i \cdot U = a_i \ \ (1 \leq i \leq n),$$

which by (5.7) leads to $U \perp a_i * 0 \ (1 \leq i \leq n)$ and thereby to the equality $U \perp U^* := \prod_1^n (a_i * 0)$ with $a_i \cdot U^* = 0 \rightsquigarrow A \cdot U^* = 0$.

10.2 Nearer to Dilworth

Henceforth, let $\mathfrak{A}$ always be an AML, generated by compact divisors, (but) not necessarily closed under multiplication.

10. 2. 1 Definition. By a *ringlike AML* we mean an AML, that is generated by an $\mathcal{A}_c$ of compact $+$-principle divisors.

This means in the language of DILWORTH, that $\mathfrak{A}$ is generated by a subset of $+$-principal weak $\cap$-principal elements.

Moreover recall that $\mathfrak{A}$ is said to be hyper-normal if (HN) holds w.r.t. at least one generating system $\mathcal{A}_c$.

(HN) does not imply (RL), not even in the distributive case, as was shown by example 10.1.2. But if $\mathfrak{A}$ is a *Prüfer monoid* – or merely satisfying

$$(\mathbf{k}\cap) \qquad a(B \cap C) = aB \cap aC$$

then $\mathfrak{A}$ satisfies (RL) if only (HN) is satisfied – which is shown next:

To this end recall again that in the lattice modular case hyper-normality implies condition (RL). And applying (RL) and (k$\cap$) we obtain:

$$\begin{aligned} x \subseteq a * (B + aC) &\implies ax \subseteq B + aC \\ &\implies ax \subseteq B + (ax \cap aC) \\ &\implies ax \subseteq B + ax(x * C) && (\mathrm{k}\cap) \\ &\implies ax * B + x * C = 1 && (\mathrm{RL}) \\ &\implies (x * (a * B)) + x * C = 1 \\ &\implies x * (a * B + C) = 1 \\ &\implies x \subseteq (a * B) + C\,. \end{aligned}$$

So we may state $a * (B + aC) \subseteq (a * B) + C \subseteq a * (B + aC)$, that is (RL).

Finally we show

10. 2. 2 Proposition. *Let* $\mathfrak{A}$ *satisfy* (JP) & (RL). *Then* $\mathfrak{A}/D$ *satisfies* (JP) & (RL), *too,* w.r.t. $\overline{A} \star \overline{B} := (D + A) * (D + B)$.

PROOF. Suppose that (JP) is satisfied. We calculate:

$$\begin{aligned}\overline{a}\circ\overline{X}\subseteq\overline{B}+\overline{a}\circ\overline{C} &\Longrightarrow aX\subseteq(D+B)+aC\\ &\Longrightarrow X\subseteq(a*(D+B))+C\\ &\Longrightarrow D+X\subseteq((D+a)*(D+B))+(D+C)\\ &\Longrightarrow \overline{X}\subseteq\overline{a}\star\overline{B}+\overline{C}\,.\end{aligned}$$

The proof for (RL) is done by putting $X=1$. □

10. 2. 3 Proposition. *Let $\mathfrak{A}$ satisfy* (JP)*, let a be a generator of $\mathfrak{A}$ and let P be prime in $\mathfrak{A}$. Then in $\mathfrak{A}/P=:\overline{\mathfrak{A}}$ it holds*

$$\overline{a}\circ\overline{X}=\overline{a}\circ\overline{Y}\neq\overline{0}=\overline{P}\Longrightarrow\overline{X}=\overline{Y}.$$

PROOF. It holds $\overline{a}\circ\overline{X}=\overline{a}\circ\overline{Y}\neq\overline{0}\Longrightarrow P+aX=P+aY\neq P\Longrightarrow aX\subseteq P+aY\Longrightarrow X\subseteq a*P+Y=P+Y\Longrightarrow\overline{X}\subseteq\overline{Y}$. The rest follows by symmetry. □

Next we present:

10. 2. 4 Proposition. *Let $\mathfrak{A}$ satisfy* (HN) *and moreover $a(b\cap c)=ab\cap ac$. Then any $\mathfrak{A}_P$ satisfies* (HN) *again.*

PROOF. Assume $a_S\circ U_S=(aU)_S=a_S\neq 0_S$. Then there exists a compact u satisfying $a_S\circ u_S=a_S$ that is with $aus=at=at(t*us)$ $(s,t\not\subseteq P)$. Hence there exists some $(t*us)^*\perp(t*us)$ with $(at)\cdot(t*us)^*=0$ and thereby with $u_P=us_P=(t*us)_P$ that is with

$$a_P\circ((t*us)^*)_P=0_P\ \&\ ((t*us)^*)_P\perp u_P\,.$$

But $u_P\perp X_P\Longrightarrow U_P\perp X_P$. This completes the proof. □

10. 2. 5 Proposition. *Let $\mathfrak{A}$ satisfy* (JP)*. Then any $\mathfrak{A}_P$ satisfies* (JP) *again.*

PROOF.
$$\begin{aligned}a_S\circ x_S\subseteq B_S\oplus a\circ Y &\Longrightarrow ax\subseteq(B+aY)_S\\ &\Longrightarrow a(xs)\subseteq B+aY\\ &\Longrightarrow xs\subseteq a*B+Y\\ &\Longrightarrow x\subseteq(a*B+Y)_S\\ &\Longrightarrow x_S\subseteq a_S*B_S\oplus Y_S\,.\end{aligned}$$
□

Recall: An AML is said to be *normal* if it satisfies

$$\text{(n)} \qquad a * b + b * a \ = \ 1 \ \ (a, b \in \mathcal{A}_c)\,.$$

If $\mathfrak{A}$ is normal and A, B are finitely generated. Then

$$\text{(N)} \qquad A * B + B * A \ = \ 1\,.$$

Any normal AML is lattice-distributive, that is satisfies

$$\text{(D)} \qquad A \cap (B + C) \ = \ (A \cap B) + (A \cap C)\,.$$

Studying normality it turned out that normal IDMs have the Prüfer property. For the sake of completeness we give next a short proof of this fact, in addition, based on the normality of the substructure of all compact elements.

10. 2. 6 Lemma. *Let $\mathfrak{A}$ be a normal ideal monoid. Then $\mathfrak{A}$ is a Prüfer ideal monoid.*

PROOF. By assumption all 1-generated elements, that is all generators are divisors. Suppose now that all at most n-generated elements are divisors and assume that A, B are at most n-generated. Then it results

$$\begin{aligned} (A + B)(A * B) &= A(A * B) + B(A * B) \\ &= B(B * A) + B(A * B) \\ &= B(A * B + B * A) \\ &= B\,. \end{aligned}$$

Thus, by induction, all finitely generated elements are divisors. □

Clearly, a ringlike AML need not be normal, observe: otherwise any commutative ring with identity would be *arithmetical* that is have a distributive ideal lattice, consult f. i. Larsen/McCarthy.

But the question arises wether a lattice distributive ringlike ideal $\mathfrak{A}$ is a Prüfer monoid. That this is not the case was shown by example 10.1.3.

Here each principal Rees ideal is even a $+$-principal element, whence $\mathfrak{S}$ is hyper-normal. But in spite of this it holds:

$$\langle u \rangle * \langle a \rangle + \langle a \rangle * \langle u \rangle \neq \langle 1 \rangle\,.$$

However, condition (HN) implies

$$\begin{aligned} a\cdot U = a &\implies a\cdot U^* = 0 \;\; (\exists\, U^*\perp U)\\ &\implies a\cdot(U^* + a*b) = a\cap b\\ &\rightsquigarrow \;\; a*b = U^* + a*b \;\; (\exists\, U^*). \end{aligned}$$

Hence under assumption of (HN) condition (j_n) holds, if only condition $a\cdot(a*b+b*a) = a$ is guaranteed. Therefore

10. 2. 7 Proposition. *A ringlike ideal monoid is a Prüfer monoid if and only if it is normal.*

Finally we remark that in a lattice distributive $\mathfrak{A}$ condition (HN) is carried over to all compact elements $A := a_1 + \ldots + a_n \;\; (a_i \in \mathcal{A}_c)$, since

$$A\cdot U = A \overset{5.3.5}{\Longrightarrow} a_i\cdot U = a_i \;\; (1\le i\le n)$$

leads to $U \perp a_i * 0 \;\; (1\le i\le n)$ from which by (5.8) follows the equation $U\perp U^* := \prod\limits_1^n (a_i * 0)$ with $A\cdot U^* = 0\,.$

Next we give some remarks concerning special structures.

10. 2. 8 Lemma. *Ringlike AP-ideal-monoids satisfy*

$$1\neq A\supset P,Q \;\; (P,Q \text{ prime}) \implies P = Q\,.$$

PROOF. By (I) and (A) we get $A\supset P\supseteq c \rightsquigarrow cA = c \rightsquigarrow cA^* = 0$ with some $A^*\perp A$, whence it follows $Q\supseteq c$, observe $A\not\supseteq A^*$. □

10. 2. 9 Proposition. *Let $\mathfrak{A}$ be a ringlike Prüfer ideal monoid generated by $\mathcal{A}_c$ and let P be prime. Then $\mathfrak{A}/P$ is a Prüfer ideal monoid whose compact elements are* 0-cancellable, *that is (recall) satisfy the implication* $\overline{\mathrm{a}}\circ\overline{X} = \overline{\mathrm{a}}\circ\overline{Y}\neq\overline{0} = \overline{P}\Longrightarrow \overline{X} = \overline{Y}$ *,*

If moreover $\mathfrak{A}$ has even the multiplication property (M) then $\mathfrak{A}/P$ again satisfies (M) and is moreover cancellative with 0*.*

PROOF. By distributivity, divisors are sent to divisors. Hence all $\overline{a}_1 + \ldots + \overline{a}_n$ are divisors in $\mathfrak{A}/P$. Consequently $\mathfrak{A}/P$ has the Prüfer property (M-property), if $\mathfrak{A}$ has the Prüfer property (M-property).

Moreover, all generator images $\overline{a}$ are 0-cancellable, recall 10.2.3. But this means that in the Prüfer case all $\overline{a}_1 + \ldots + \overline{a}_n$ are cancellable, since they are divisors of – for instance – $\overline{a}_1$, and by analogy (M) implies that all elements $\overline{A}$ are 0-cancellable divisors. $\square$

10. 2. 10 Lemma. *Let $\mathfrak{A}$ be an archimedean ideal-monoid. Then each prime element P satisfies the implication*

$$1 \neq M \supset P \Longrightarrow P = \bigcap M^n \ \ (n \in \mathbf{N})\,.$$

PROOF. Otherwise we would get $\mathfrak{A}/P = \overline{\mathfrak{A}}$ with $\bigcap \overline{M}^n \supseteq \overline{S} \supset \overline{0} = \overline{P}$ for some prime P and thereby some $\overline{c} \neq \overline{0}$ with $\overline{c} \circ \overline{M} = \overline{c} \circ \overline{1} \rightsquigarrow \overline{M} = \overline{1}$, a contradiction! $\square$

10.3 The Kernel

Throughout this section $\mathfrak{A}$ is assumed to be an AML with respect to some fixed submonoid of compact generators, not necessarily divisors.

We study the *kernel of an element,* introduced by Krull, see also [163]. To this end we need lemmata, basically due to Krull, whose proofs remain valid even in general since paper [244] is of purely multiplicative character.

We exhibit some equivalents of $\ker A = A$, valid in arbitrary AMLs of the above type, partly along the lines of Mori, [300], partly along the lines of Gilmer/Mott, [163].

First of all recall 6.2.4, that is

Krull's Kernel Lemma. *Let $\mathfrak{A}$ be a compactly generated AML. Then the following are equivalent:*

(*i*) $\ker A = A \ \ (\forall\, A \in \mathcal{A})\,.$

(*ii*) $X \supset P \supseteq p \Longrightarrow pX = p\,.$

We now turn to the ringlike case.

10. 3. 1 Proposition. *Let $\mathfrak{A}$ be an AML compactly generated by a submonoid and ringlike with respect to this submonoid. Then the following are equivalent:*

(*i*) $\ker A = A \ (\forall A \in \mathcal{A})$.

(*iii*) *Non maximal primes are idempotent divisors.*

PROOF. Obviously by 6.2.5 condition (*iii*) implies condition (*i*).

So, it remains to prove $(i) \Longrightarrow (iii)$. We suppose $1 \neq A \supset P \supseteq p$. Then (*ii*) implies $pA = p \rightsquigarrow pA^* = 0 \ (\exists A^* \bot A)$, that is $pP = p(P + A^*) = p$ by $P + A^* = P \Longrightarrow A \supseteq P \supseteq A^*$, so non maximal primes are divisors. □

10. 3. 2 Lemma. *Let $\mathfrak{A}$ be an AML that is compactly generated by a submonoid and ringlike with respect to this submonoid. Suppose furthermore $1 \neq A \supset P$. Then any P-primary element Q is equal to P.*

PROOF. Assume $a \subseteq A \ \& \ a \not\subseteq P$ and $p \subseteq P \ \& \ p \not\subseteq Q$. Then it follows:

$$ab \subseteq Q + ap \ \& \ a \not\subseteq P \Longrightarrow p \subseteq Q + ap \Longrightarrow pa^* \subseteq Q \text{ with } a^* \bot a.$$

But it holds $a^* \not\subseteq P$, since otherwise it would follow $A \supseteq a + a^* = 1$. Hence no power of a^* is contained in P. So we get $Q \supseteq p$ and thereby in general $Q \supseteq P$, that is $Q = P$. □

10. 3. 3 Proposition. *Let $\mathfrak{A}$ be an AML that is compactly generated by a submonoid and ringlike with respect to this submonoid. Then the following are equivalent:*

(*i*) $\ker A = A \ (\forall A \in \mathcal{A})$.

(*iv*) $\mathrm{Rad}\, A$ *prime* $\Longrightarrow A$ *is primary.*

PROOF. Suppose (*iv*) and $M \supseteq P$ with minimal P and $P \supseteq p$. Then by 10.3.2 we get $0_M = P$. Hence there exists some $s \not\subseteq M$ with $ps = 0$ leading to $pM = p(M + s) = p$ since M is maximal. Thus it results (*ii*).

Let now $\mathrm{Rad} A = P$ be prime and $\ker A = A$. Then P is the only minimal prime over A whence A is primary. □

10.4 Idempotency

We start with a lemma, which was proven for rings by Mori, [300] and [302], respectively: [4)]

[4)] In this section slanted letters will denote compact elements.

10. 4. 1 Lemma. *Let $\mathfrak{A}$ be a multiplication AML, not necessarily with compact identity. Put $N := \text{Rad } 0$. Then to each compact c there exists a compact $u \subseteq (c * N) * N$ with $c \subseteq N + cu$.*

PROOF. First by

$$y \subseteq c * N \cap (c * N) * N \implies y^2 \subseteq N \Longrightarrow y \subseteq N \tag{10.10}$$

it follows

$$N \;=\; c * N \cap (c * N) * N\,. \tag{10.11}$$

Next by (M) there exists some divisor D with

$$(c + c * N)D \;=\; c \;=\; cD + (c * N)D\,. \tag{10.12}$$

This implies in particular – recall (10.11) –

$$\begin{array}{rcl} (c * N)D & \subseteq & c \cap c * N \\ & \subseteq & (c * N) * N \cap c * N = N \\ \rightsquigarrow \quad D & \subseteq & (c * N) * N\,. \end{array}$$

Thus by (10.12) we get

$$c \;\subseteq\; c \cdot ((c * N) * N) + N \tag{10.13}$$

which leads to some compact $u \in (c * N) * N$ with

$$c \;\subseteq\; N + cu\,. \tag{10.14}$$

This completes the proof. □

Applying (10.14) we get in particular:

10. 4. 2 Corollary. *Any ringlike multiplication AML satisfies:*

$$c * N + (c * N) * N \;=\; 1\,. \tag{$\mathbf{N}^c$}$$

PROOF. Suppose $c \subseteq N + cu$ with $u \subseteq (c * N) * N$. This entails

$$\begin{array}{rl} c \subseteq N + cu & \Longrightarrow\;\; c * N + u = 1 \\ & \Longrightarrow\;\; c * N + (c * N) * N = 1\,. \end{array}$$ □

Now we are in the position to prove a result which was exhibited for commutative rings by Gilmer/Mott in [163]:

10. 4. 3 Proposition. *Let $\mathfrak{A}$ be a ringlike multiplication ideal monoid. Then any idempotent element is a sum of idempotent compact elements.*

PROOF. Let U be idempotent, and let A be the subelement that is generated by the set of all compact idempotents contained in U. This set is not empty because 0 is idempotent. We prove:

$$U = U^2 \supset A \implies \exists\, e : U \supseteq e = e^2 \not\subseteq A\,.$$

To this end suppose $A \subset U$ and $c \subseteq U$ but $c \not\subseteq A$. By property (M) we get $U \cdot c = c$, whence there exists some $f \subseteq U$ with $fc = c$ and thereby with $f^n c = c$. So we may assume that already c satisfies $c^n \not\subseteq A$, in particular that c is not contained in N. Then by ($\mathbf{N}^c$) and $U \cdot c = c$ we get

$$c = c \cdot (c * N) + c \cdot U \cdot ((c * N) * N)$$

whence we find some $u \subseteq U$ with

$$c \subseteq N + cu \ \ (u \subseteq (c * N) * N)\,.$$

This leads in $\mathfrak{A}$ to some $u^* \subseteq c * N$ with $u^* \perp u$ and $uu^* \subseteq N$ and hence to some power $(uu^*)^k = 0 \ \ (\exists\, k \in \mathbf{N})$. Therefore by (5.9) we get next

$$\begin{aligned} u^k &= u^k(u^k + u^{*k}) \\ &= (u^k)^2 + (uu^*)^k \\ &= (u^k)^2\,. \end{aligned}$$

But by $c \subseteq N + cu \rightsquigarrow cu \subseteq Nu + cu^2$ we get $c \subseteq N + cu^k$. Hence, the element u of lemma 10.4.1 may be assumed to be idempotent.

It remains to show that $u^k =: e$ is not contained in A. But it holds $c \subseteq N + ce$ and hence $c \subseteq n + ce \ \ (\exists\, n \subseteq N)$. So there exists some $m \in \mathbf{N}$ with

$$c^m \subseteq (n + ce)^m \;=\; n^m + c^m e = c^m e \rightsquigarrow c^m = c^m e\,. \tag{10.16}$$

Therefore e cannot belong to A, since c^m is not contained in A. □

As is easily checked, the proof that idempotent elements are sums of idempotent compact elements does not depend on compactness of the identity but merely on the existence of some u^*, for every compact u, satisfying $u \cdot u^* = 0$ and $u = u \cdot (u + u^*)$. Such elements u^* exist, for instance, in the ideal monoids of (commutative) M-rings with *fixing elements,* that is elements e_a with $a \cdot e_a = a$.

Moreover: commutative rings with fixing elements, monoids or d-monoids have ideal structures in which the product of any principal ideal with an arbitrary ideal is equal to the *complex product.* In those cases the proof above works even for principal ideals instead of compact ones, that is finitely generated ideals, as is easily verified by the reader.

In particular: property (M) guarantees fixing elements whence in analogy to the element $\langle c\rangle$ of (RL) one finds some $\langle c\rangle^*$ satisfying $\langle c\rangle \cdot \langle c\rangle^* = \langle 0\rangle$ and $\langle c\rangle = \langle c\rangle\,(\langle c\rangle + \langle c\rangle^*)$. This means that M-rings and thereby also idempotent ideals of M-rings are generated idempotently, on the grounds of $a^2x = a \Longrightarrow (ax)^2 = ax$.

10.5 Decomposition Theorems

First a ring theoretical result. Here we denote the *radical* N from above by $\mathfrak{n}$ and prime ideals by $\mathfrak{p}$.

10. 5. 1 A Decomposition Theorem for Rings. *Every M-ring with identity* 1 *has a subdirect decomposition into components which are cancellative with* 0 *or primary.*

PROOF. Let $\mathfrak{R}$ be an M-ring with identity 1. Then the subdirect irreducible images of $\mathfrak{R}$ are again M-rings containing in particular no idempotents different from $\overline{0}$ and $\overline{1}$. But this means that the corresponding ideal monoids are *nilpotent* or otherwise that in 10.4.3 we get first $\langle e\rangle = \langle 1\rangle$ and thereby furthermore $(\,\langle c\rangle * \mathfrak{n}\,) * \mathfrak{n} = \langle 1\rangle$, recall $\langle e\rangle \subseteq (\,\langle c\rangle * \mathfrak{n}\,) * \mathfrak{n}$.

So, in the non nilpotent components we get $\langle c\rangle * \mathfrak{n} = \mathfrak{n}$, as is easily checked, and thereby $\langle c\rangle * \langle 0\rangle = \langle 0\rangle$, which results as follows:

Suppose in the proof of 10.4.3 the equation $(\langle c\rangle * \mathfrak{n}) * \mathfrak{n} = \langle 1\rangle$. Then from $\langle c\rangle * \mathfrak{n} = \mathfrak{n}$ it follows $\langle c\rangle^n * \mathfrak{n} = \mathfrak{n}$ $(\forall\, n \in \mathbf{N})$. So, if $c \cdot y = 0$, it follows $y \in \mathfrak{n}$ and thereby $y^n = 0$ for some $n \in \mathbf{N}$. Consequently every minimal prime element $\mathfrak{p}$ contains y.

We show that not only each minimal prime $\mathfrak{p}$ contains y but also all its powers $\mathfrak{p}^n$. From this, by $\ker 0 = 0$, it then results $y = 0$ (and thereby $\langle c\rangle * \langle 0\rangle = \langle 0\rangle$).

Observe: It holds $\mathfrak{p} \supseteq \mathfrak{n}$ and if $y \notin \mathfrak{p}^{m+1}$ we get $\mathfrak{p} \not\supseteq \mathfrak{p}^m * \langle y \rangle$ and thereby $c \notin \mathfrak{p}$, because $0 = c \cdot y \notin \mathfrak{p}^{m+1}$. But this leads to the contradiction

$$\mathfrak{p} \supseteq \mathfrak{n} = \langle c \rangle^m * \mathfrak{n} \supseteq \mathfrak{p}^m * \mathfrak{n} \supseteq \mathfrak{p}^m * \langle y \rangle \not\subseteq \mathfrak{p}\,.$$

Thus the proof is complete. □

As an immediate consequence we obtain:

10. 5. 2 Corollary. *Any ringlike multiplication AML admits a subdirect decomposition into factors satisfying* $\langle c \rangle * \langle 0 \rangle = \langle 0 \rangle$ *or* $\mathfrak{m}^n = 0$ *for all and thereby for exactly one maximal element.*

Next recall condition (F), that is

10. 5. 3 Proposition. *Any multiplication AML satisfies:*

(DC) $$A = \bigcap {P_i}^{e_i} \qquad (P \textit{ prime and } {P_i}^{e_i} \supseteq A)\,.$$

Obviously by 10.5.3 and 10.2.3 we obtain again 10.5.2, since in the M-case any $\mathfrak{A}/P$ is again a multiplication AML and thereby 0-cancellative.

10. 5. 4 Proposition. *A ringlike M-ideal-monoid* $\mathfrak{A}$ *is a direct product in the sense of 10.5.2 if and only if for each family of idempotent elements* B_i $(i \in I)$ *the equation holds:*

($\mathbf{D}_\cap$) $$A + \bigcap B_i \;=\; \bigcap (A + B_i) \quad (i \in I)\,.$$

PROOF. ($\mathrm{D}_\cap$) is obviously necessary. Let now $\bigcap {P_i}^{e_i} = 0$ be the representation of 0 by minimal prime powers. Then each factor ${P_i}^{e_i} =: U_i$ is idempotent and each $A \in \mathcal{A}$ can be decomposed into

$$A = A + 0 = A + \bigcap U_i \;=\; \bigcap (A + U_i)\ (=: \bigcap A_i)\ (i \in I)\,.$$

Now, by 10.2.8 we get $P_i \neq P_j \Longrightarrow P_i \perp P_j$. But by ($\mathrm{D}_\cap$) this leads to $U_i \perp \bigcap U_j$ $(j \neq i)$. Hereby the proof is complete. □

The most natural question arises, when a ringlike multiplication AML has the Noether property. There is an abundance of necessary and sufficient conditions. In particular, since multiplication AMLs are archimedean ideal monoids, the reader may consult the corresponding section. Moreover, since components $\mathfrak{A}/P$ with idempotent minimal P may by JAFFARD, [208], be considered as the ideal structure of some integral domain, and since any component of type $\mathfrak{A}/P^n$ with $P^{n-1} \neq P^n = P^{n+1}$ may be considered as ideal structure of some residue class ring $\mathbf{Z}/p^n$ we are arrived at MOTT, [306].

For the sake of completeness only one characterization, which will not be mentioned in the chapter on archimedean Prüfer structures.

10. 5. 5 Proposition. *A ringlike M-ideal-monoid $\mathfrak{A}$ with compact identity 1 is a finite direct product in the sense of 10. 5. 1 if and only if:*

$$(\mathrm{D}^*) \qquad U = U^2 \implies U + U * 0 = 1\,.$$

PROOF. By assumption it follows immediately that idempotent elements are finitely generated since

$$U + U * 0 = 1 \Longrightarrow u + u^* = 1 \ \ (\exists\, u \subseteq U, u^* \subseteq U * 0)\,.$$

Observe $U \cdot u^* = 0 \Longrightarrow u \supseteq U$, apply (5.8).

Hence the set of idempotent elements satisfies the ascending chain condition. So, since all kernel components of 0 are idempotent, the set of kernel components of 0 is finite. □

Finally, a ring theoretical result, due to D. D. ANDERSON, compare [3], is proved in an alternate manner.

10. 5. 6 Proposition. *Let $\mathfrak{R}$ be a ring with identity* 1*. Then $\mathfrak{R}[\,x\,]$ is a multiplication ring if and only if $\mathfrak{R}$ is a direct product of fields.*

PROOF. The one direction is clear. So let $\mathfrak{R}[\,x\,]$ be a multiplication ring. Then $\mathfrak{R}$ is (von Neumann) regular, since by distributivity of the ideal lattice every $a \in R$ satisfies

$$\langle a\rangle \supseteq \langle x-a\rangle + \langle x\rangle \implies (\langle a\rangle \cap \langle x-a\rangle) + (\langle a\rangle \cap \langle x\rangle\,,$$

which implies
$$\begin{aligned} a &= (x-a)\cdot f(x) + x\cdot g(x) \\ &\quad\ \text{with } a \,|\, x\cdot g(x) \rightsquigarrow a \,|\, g(x) \\ &\rightsquigarrow a \,|\, (x-a)\cdot f(x) \\ &\rightsquigarrow a \,|\, xf(x) \rightsquigarrow a \,|\, f(x) \\ &\rightsquigarrow a^2 \,|\, af(x) = x(\,f(x)+g(x)\,) - a \\ &\rightsquigarrow a^2 \,|\, a\,. \end{aligned}$$

Thus the principal ideals form a boolean algebra, whence in particular all finitely generated ideals are principal ideals, which results by $u = u^2$ & $v = v^2 \Longrightarrow \langle u, v\rangle = \langle u - uv + v\rangle$.

We now show that $\mathfrak{R}$ has the Noether property. From this it will follow that $\mathfrak{R}$ is indeed a direct product of fields. To this end let $A = \langle a_i\rangle$ $(a_i^2 = a_i)$ be an ideal of $\mathfrak{R}$ and suppose $\langle A, x\rangle \cdot B = \langle x\rangle$ in $\mathfrak{R}[\,x\,]$. Then we obtain $\langle A, x\rangle \cdot B = \langle x\rangle = \langle a_1, \ldots, a_n, x\rangle \cdot B$ $(\exists\, a_i \in A, 1 \leq i \leq n) \supseteq \langle x\rangle \rightsquigarrow \langle a_1, \ldots, a_n, x\rangle \cdot B = \langle x\rangle$.

Now, by $B \mid \langle x\rangle$, B is cancellable since $\langle x\rangle$ is cancellable. Hence we obtain: $\langle A, x\rangle = \langle a_1, \ldots, a_n, x\rangle = \langle a, x\rangle$ with $\langle a\rangle = \langle a_1, \ldots, a_n\rangle$ and hence for all $a_i \in A$ some $a \cdot u(x) + x \cdot v(x) = a_i$ that is, by the rules of polynomial arithmetic, $a_i = as$ with $s \in R$. Thus it is – even – shown $A = \langle a\rangle$. □

10.6 M-characterizations

Throughout this section we are concerned with ringlike AMLs. In this case we may hope for M-characterizations based on ringlike particularities shedding some special light.

10. 6. 1 Lemma. *In a ringlike ideal monoid $\mathfrak{A}$ satisfying*

(M1) $$a * B + B * a = 1$$

(RP) $$P \succeq P^2 \qquad (\forall\, P \textit{ prime})$$

any prime power satisfies $P^n \supseteq AB \,\&\, P \not\supseteq B \Longrightarrow P^n \supseteq A$. Evidently this means in particular that any prime power is primary.

PROOF. [5] First of all observe that $\mathfrak{A}$ has the Prüfer property. Suppose now $P^n \supseteq AB \,\&\, P \not\supseteq B$, then $P^n \supseteq (P^n{+}A)(P{+}B)^n$. We put $P{+}B =: D$ and shall show in general $D \supset P \supseteq p \Longrightarrow Dp = p$.

To this end suppose $p \subseteq P$ & $p \not\subseteq P^2$. Then

$$PX \subseteq P^2 \Longrightarrow P(P + X) = P^2 \Longrightarrow P + X = P\,,$$

that is – by (I) – $P \supseteq P * P^2$ and thereby $P = P * P^2$.

[5] This proof avoids the Prime Criterion, but for the sake of plurality and in order to write in a more self-contained manner we decided for this alternative method of proof.

This leads next to $p * P^2 = (p + P^2) * P^2 = P * P^2 = P$ and $P^2 * p = (P^2 + p) * p = P * p$. Consequently it holds $P \perp P * p$, that is by (5.11) $P \,|\, p$. Hence we get

$$D \supset P \supseteq p \Longrightarrow D \cdot p = D \cdot P \cdot (P * p) = P \cdot (P * p) = p\,. \qquad \square$$

As a first characterization we present:

10. 6. 2 Proposition. *A ringlike ideal monoid* $\mathfrak{A}$ *has property* (*M*) *if and only if it satisfies the conditions:* [6)]

(M1) $$a * B + B * a \;=\; 1$$

(M2) $$U = U^2 \;\Longrightarrow\; U = \sum u_i \;\; (u_i = u_i{}^2)$$

(M3) $$P \textit{ prime } \& \; P \supset X \supseteq P^2 \;\Longrightarrow\; X \textit{ is } P\textit{-primary}$$

PROOF. Necessity: Condition (M1) follows by (HN) and the equation $a(a * B + B * a) = a$, recall $a * B = a * B + a * 0$.

Next, condition (M2) was proven in the preceding section.

Finally let's turn to condition (M3). Obviously, under our assumption above we get $X = PY = P(P + Y)$. So – by condition (I) – X must be equal to P^2. But P^2 is primary because

$$P^2 \supseteq ab \;\&\; P \not\supseteq a \Longrightarrow P^2 \supseteq (P + a)^2(P^2 + b) = P^2 + b\,.$$

Sufficiency: By (M1) the underlying ideal monoid has the Prüfer property. So, any idempotent U is a divisor because it is a sum of compact idempotents.

Furthermore by condition (M3) prime elements are maximal or idempotent, recall 10.3.2. This means in particular (M3) & (M2) $\Longrightarrow \ker A = A$.

Next, by (M1), we get $(x + y) * B + B * (x + y) = 1$, because

$$\begin{aligned} & (x + y) * B + B * (x + y) \\ = \;& ((x * B) \cap (y * B)) + B * (x + y) \\ = \;& ((x * B) + B * (x + y)) \cap ((y * B) + B * (x + y)) \\ \supseteq \;& (x * B + B * x) \cap (y * B) + (B * y) = 1\,. \end{aligned}$$

6) Evidently condition (M3) results from $\ker A = A$ as well as from $\mathrm{Rad} A$ prime $\Longrightarrow A$ primary.

Consider now some $x \subseteq M$ with $x \not\subseteq M^2$. Then by $M \succ M^2$ for each $m \subseteq M$, defining $b := x + m$, it follows

$$M^2 * b + b * M^2 = (M^2 + b) * b + (M^2 + b) * M^2 = M * b + M = 1\,.$$

But by (5.11) this leads to $M \cdot (M * b) = M \cap (M * b) \supseteq b$, that is $M \mid b$.

So, given some $b \subseteq M$ we find some $x \subseteq M$ with $x \not\subseteq M^2$ implying $M \mid b + x \mid b$ and thereby $M \supseteq B \Longrightarrow M \mid B$.

Summarizing: By (M1),(M2),(M3) any prime element is even a prime divisor. This completes the proof by the prime criterion. □

10. 6. 3 Proposition. *A ringlike ideal monoid $\mathfrak{A}$ is a multiplication AML iff it satisfies*

(M1) $$a * B + B * a \;=\; 1$$

(DC) $$A = \bigcap {P_i}^{e_i} \qquad (P \textit{ prime and } {P_i}^{e_i} \supseteq A)\,.$$

PROOF. By the results above it suffices to verify

SUFFICIENCY: By (DC) $\mathfrak{A}$ satisfies condition (S) whence according to lemma 10.6.1 any prime power is primary. Conversely by (DC) any primary element is a prime power.

Assume now $P^n \supseteq B$ $(\forall\, n \in \mathbf{N})$ but $B \neq PB$. Then any prime power Q^m with $Q^m \supseteq PB$ either satisfies $Q \supseteq P \Longrightarrow Q^m \supseteq B$ or we get $Q \not\supseteq P \Longrightarrow Q^m \supseteq B$, since Q^m is primary. Hence $\mathfrak{A}$ has the archimedean property, leading to $U^2 = U \supseteq B \rightsquigarrow UB = B$. Therefore the rest is done along the proof lines of 10.6.2 by applying the Prüfer property. □

Recall: 8.8.4 provides

10. 6. 4 Proposition. *In an arbitrary commutative ideal monoid $\mathfrak{A}$ the following are equivalent:*

- (i) *$\mathfrak{A}$ is a multiplication AML.*
- (ii) *$\mathfrak{A}$ is a weak multiplication AML, that is for each prime element P $\mathfrak{A}$ satisfies the implication $P \supseteq B \Longrightarrow P \mid B$.*
- (iii) *$\mathfrak{A}$ satisfies:*
- (a) *Every element is equal to its kernel.*

(b) *Every primary element is a power of its radical.*

(c) *If P is minimal prime over A, if n is the least positive integer such that P^n is the isolated P-primary component of A and if $P^n \neq P^{n+1}$, then P does not contain the meet of the remaining isolated primary components.*

For the ideal structure of commutative rings with identity 1 this result is due to Mott, [304]. It was carried over to ringlike AMLs in a joint paper of Alarcon/Anderson/Jayaram in [2]. Here we add:

10. 6. 5 Proposition. *A ringlike ideal monoid $\mathfrak{A}$ is a multiplication AML iff it satisfies*

(M1) $$a * B + B * a = 1$$

(RP) $$\operatorname{Rad} A = P \textit{ prime} \implies A = P^n \ \ (\exists\, n \in \mathbf{N}).$$

PROOF. Let $\operatorname{Rad} A$ be prime. Then by (RP) A is equal to some P^n. Hence by (DC) of 10.6.3 it suffices to show $\ker A = A$, which by 10.3.3 is equivalent to $\operatorname{Rad} B$ is prime $\Longrightarrow B$ is primary. But, by (RP) it holds $P \succeq P^2$ whence B is primary by 10.6.1. □

Chapter 11

Archimedean Prüfer Ideal Monoids

11.1 Preliminaries

Throughout this chapter multiplication where ever, is assumed to be commutative. However in the considered situations this will not mean a real restriction, since archimedean Prüfer monoids are always commutative, as was shown by the author, cf. consult [69], [70], [77].

So, let $\mathfrak{A}$ be a commutative AML, generated by a monoid of compact divisors. This applies for instance to Rees ideals in monoids or to Dedekind ideals in rings with identity, but also, of course to t-ideals in monoids and rings.

If in addition any $a_1 + a_2 + ... + a_n$ is a divisor $\mathfrak{A}$ is called a Prüfer IDM. In this case the set of all $a_1 + a_2 + ... + a_n$ forms a monoid of compact divisors which is closed under $\cdot$, $+$, $\cap$, and $|$, that is – briefly – generated by a Prüfer monoid and denoted as a Prüfer ideal monoid, briefly a Prüfer IDM or a P-IDM.

11. 1. 1 Example. *Consider an arithmetical ring with identity. Here the set of principal ideals may be considered as a monoid of compact divisors, whereas the set of all finitely generated ideals may be considered as a Prüfer basis, that is a generating submonoid of compact divisors, closed under $+$, $\cap$, and $|$.*

For the sake of convenience the reader may read this chapter w.r.t. Püfer ideal monoids. The interested insider however is invited to check each situation also w.r.t. DV-IDMs, again these are AMLs generated by a monoid of compact divisors, not necessarily closed under $+$.

Main subject will be the *archimedean Prüfer IDM*, briefly AP-IDM. By definition in any AP-IDM the set A_C of compact elements is closed under $\cdot$, $+$, and $\cap$. From this point of view – again – the reader may presume that Prüfer IDMs are always considered w.r.t. their subset C of compact elements as distinguished basis of divisors. Nevertheless in some proofs we will employ slanted letters for compact elements, not necessarily a generator, having in mind the situation of monoids or rings with identity, for instance.

Recall, AP-IDMs satisfy $\ker A = A$, by 6.2.5 and property (I*).

$A \neq 0$ is called a *zero divisor* if A satisfies $A * 0 \neq 0$. This reflects the situation in rings. $\mathfrak{A}$ is called an AML without zero divisors if there are no zero divisors, which means if there are no compact zero divisors, since $AX = 0 \Longrightarrow aX = 0 \ (\forall a \subseteq A)$.

Recall, $\mathfrak{A}$ is said to be hyper-normal, if at least one system of compact generators a satisfies

$$\text{(HN)} \qquad aU = a \implies \exists U^* : U \perp U^* \ \&\ aU^* = 0\,.$$

Let $\mathfrak{A}$ be a commutative hyper-normal AP-IDM. Then $\mathfrak{A}$ has no zero divisors iff 0 is prime. And this is the case iff $ax = ay \neq 0 \Longrightarrow x = y$ is satisfied, because

$$\begin{aligned} ax = ay &\implies a(x+y)x' = a(x+y) \\ &\implies \exists u \perp x' : a(x+y)u = 0 \\ &\implies u = 0 \leadsto x' = 1\,. \end{aligned}$$

In particular by 10.1.4 hyper-normal Prüfer monoids are P-cancellative.

11.2 Arithmetics

11. 2. 1 Definition. Let $\mathfrak{A}$ be an archimedean Prüfer-structure (-ideal monoid). Then we call $\mathfrak{A}$ briefly an AP-structure (AP-IDM).

Next recall 10.2.8, that is: Any hyper-normal AP-monoid $\mathfrak{A}$ satisfies:

$$1 \neq A \supset P, Q \ \ (P, Q \text{ prim}) \implies P = Q\,.$$

11. 2. 2 Lemma. *In any hyper-normal Prüfer monoid each idempotent prime element P is minimal.*

PROOF. Suppose $P \supset Q$ where Q is prime. Then by 5.3.5 there exists an element p and $P \supseteq p \not\subseteq Q$ and $p \cdot P = p$, $p \cdot P^* = 0$ with $(P^* \perp P)$. But by $P \not\supseteq P^*$ this would lead to $Q \not\supseteq P^*$ that is to $Q \supseteq p$, that is a contradiction. $\square$

11. 2. 3 Lemma. *In any hyper-normal AP-IDM $\mathfrak{A}$ each prime element is irreducible or an idempotent divisor, whence by 7.3.3 and 7.3.1 it holds in particular* $P^n \succeq P^{n+1}$ $(\forall n \in \mathbf{N})$ *.*

PROOF. Recall 10.3.1 $\square$

11.3 Localizations of $AP-$ideal-monoids

11. 3. 1 Proposition. *Let $\mathfrak{A}$ be a commutative Prüfer IDM and let P be prime in $\mathfrak{A}$. Then P is idempotent or P is compact in $\mathfrak{A}_P$. Moreover the following are pairwise equivalent:*

- (i) *$\mathfrak{A}$ is an AP-IDM.*
- (ii) *Each $\mathfrak{A}_M$ (M maximal) is an AP-IDM.*
- (iii) *Each $\mathfrak{A}_P$ (P prime) is an AP-IDM.*

PROOF. Consider first P in $\mathfrak{A}_P$ and suppose $a \subseteq P$ & $a \not\subseteq P^2$ and $b \subseteq P$. Then by the Prüfer property we get $(a+b)(b*a) = a$ and hence $P \not\supseteq b*a$. So it results $(b*a)_P = 1_P$ and thereby $a_P \supseteq b_P$. This leads to $P_P = a_P$.

Next, let M be a maximal element and S the set of generators $\{s \mid s \not\subseteq M\}$. We denote the elements of $\mathfrak{A}_M$ by A_S, $B_S, \ldots$

$(i) \Longrightarrow (ii)$. By assumption each $\mathfrak{A}_M$ has the Prüfer property. Recall that (D) and (e) are transferred.

Furthermore each $\mathfrak{A}_M$ satisfies condition (A). To show this we may restrict our considerations to prime elements P_S. Recall that P_S is prime in $\mathfrak{A}_M$ if and only if P_S is prime in $\mathfrak{A}$.

By (A) and according to 7.3.4 each prime element P of $\mathfrak{A}$ is even completely prime, that is, see above, each prime element P of $\mathfrak{A}$ satisfies $P^n \supseteq AB$ & $P \not\supseteq B \Longrightarrow P^n \supseteq A$. Hence, in case of $P_S \neq 1_S$, that is if $s \not\subseteq P$ $(\forall\, s \not\subseteq M)$, then it results $(P_S)^n = (P^n)_S = P^n$. This provides next $(P_S)^n \supseteq B_S \Longrightarrow P^n \supseteq B$, implying:

$$(P_S)^n \supseteq B_S \ (\forall\, n \in \mathbf{N}) \implies P_S \circ B_S = (P \cdot B)_S = B_S\,.$$

Thus condition (A) is proven for prime elements and thereby also for arbitrary elements.

$(ii) \Longrightarrow (i)$. First of all by the rules of localization it holds

$$a_S(a_S * b_S \oplus b_S * a_S) = a_S = (a(a * b + b * a))_S\,.$$

Hence applying the localization theorem we obtain condition (e) for $\mathfrak{A}$ – and in a similar manner we get condition (D).

Finally it results

$$\begin{aligned} P^n \supseteq A \ (\forall n \in \mathbf{N}) \Longrightarrow {P^n}_S &\supseteq A_S \ (\forall n \in \mathbf{N}, \forall \text{maximal } M) \\ &\Rightarrow P_S A_S = A_S = (PA)_S \end{aligned}$$

leading to condition (A) for $\mathfrak{A}$, again by the localization theorem.

$(i) \Longleftrightarrow (iii)$. Consult $(i) \Longleftrightarrow (ii)$.

This completes the proof. □

The conjecture might come up that each $\mathfrak{A}_M$ would need to be even a multiplication AML. That this is wrong is easily seen. Assume that an AML satisfies condition (AP) but not condition (M). Then we could add a new identity. This way the original identity would turn to the unique maximal element of this extension but the extension would not satisfy condition (M).

However, observe for instance the ideal structure of a commutative ring may be extended by a new identity in the above sense, to a new AML. But this new AML will in general not be isomorphic to the ideal structure of some commutative ring with identity.

11. 3. 2 Definition. By a *lattice cube* we mean a *lattice ordered* monoid $(S\,, \wedge\,, \vee\,, \cdot\,)$ *admitting a subdirect decomposition whose factors are of type* $\mathfrak{S}_n := (\{0, 1, \ldots, n\}, \circ, \wedge)$ *where*

$$a \circ b := \min\,(n, a + b) \quad \textit{and} \quad a \wedge b := \min\,(a, b)\,.$$

By 7.1.6 the set $\mathcal{C}$ of all compact elements forms a $d-$semigroup under $\cdot, +, \cap$ denoted here by $\mathfrak{C}$. The elements of $\mathfrak{C}$ are exactly all $\sum_1^n a_i$. For the sake of convenience they will be denoted by lower case slanted letters here. That is, for instance a is a sum $a_1 + ... + a_n$ of generators a_i.

The focus of the subsequent considerations will be the 0-monoid of all compact elements, again denoted by lower case slanted letters.

We shall say that there are *enough* prime elements P of a certain property if the corresponding structures $\mathfrak{A}_P$ separate each pair of different compact elements a, b, that is guarantee at least one prime element P satisfying the inequality $a_S \neq b_S \ \ (S = \{s \mid s \not\subseteq P\})$.

Now we are in the position to present:

11. 3. 3 Proposition. *Let $\mathfrak{A}$ be a commutative IDM* [1] *and let C be the set of its compact elements. Then the following are pairwise equivalent:*

(*i*) *$\mathfrak{A}$ is an AP-IDM.*

(*ii*) *$\mathfrak{C}$ is a lattice cube, satisfying*
(j) $(\mathrm{a} * \mathrm{b} + \mathrm{b} * \mathrm{a})^2 = \mathrm{a} * \mathrm{b} + \mathrm{b} * \mathrm{a}$.

(*iii*) *Any $\mathfrak{C}/c$ is a lattice cube, satisfying condition* (j).

PROOF. Let P be a prime element and put $S := \{x \,|\, x \not\subseteq P\}$. Then, obviously we obtain:

$$\begin{array}{rrcl}
 & (a_1 + ... + a_n)_S & = & (b_1 + ... + b_m)_S \\
 & & \Rightarrow & \\
 & a_1 + ... + a_n & \supseteq & b_1 \cdot e_1 + ... + b_m \cdot e_m \\
 & & \supseteq & b_1 \cdot e_1, ..., b_m \cdot e_m \\
 & & \Rightarrow & \\
 & a_1 + ... + a_n & \supseteq & b_1 \cdot (e_1 e_2 \cdot ... \cdot e_m), \ldots\ldots b_m \cdot (e_1 e_2 \cdot ... \cdot e_m) \\
 & & \Rightarrow & \\
 & a_1 + ... + a_n & \supseteq & (b_1 + ... + b_m) \cdot u \ \ (\exists u \in S) \\
\& & b_1 + ... + b_m & \supseteq & (a_1 + ... + a_n) \cdot v \ \ (\exists v \in S(\text{ (by symmetry)},
\end{array}$$

that is in general

$$a_S = b_S \Longleftrightarrow \mathrm{a} \cdot w = b \cdot w \quad (\exists w \in S) \tag{11.2}$$

[1] recall again: that is an AML generated by a monoid of compact divisors. In particular the sets $\{x|x \not\subseteq P\}$ are multiplicatively closed.

Furthermore by lattice distributivity $X \neq Y$ are separated iff $X+Y$ and $X \cap Y$ are separated.

$(i) \Longrightarrow (ii)$.

By the preceding remark we may start from $a \supset b$.

Then there exists a maximal chain of *convex* multiplicatively closed sets $S_i \ni 1$ $(i \in I)$ of compact elements, that is subsets of C, such that no S_i contains an element u satisfying $b \subseteq au$. It follows that the union S of these S_i is again such a set, satisfying moreover

$$x + y \subseteq S \implies x \in S \vee y \in S .$$

In order to verify this, we suppose $x, y \notin S$ but $x + y \in S \ni (x+y)^n$.

Then the set of all $z \supseteq x^n \cdot s$ $(s \in S)$ is a convex and multiplicatively closed proper subset of S . Hence there exists an element $e \in S$ with $a \cdot x^k \cdot e \subseteq b$ and – by symmetry – an element $f \in S$ with $a \cdot y^\ell \cdot f \subseteq b$, respectively. Consequently, putting $n := \max(k, \ell)$, $u := ef$ we get

$$a \cdot x^{2n} \cdot u \subseteq b \quad \text{and} \quad a \cdot y^{2n} u \subseteq b .$$

But $x^{2n} + y^{2n} = (x+y)^{2n}$, whence [2] we obtain $a \cdot ((x+y)^{2n} \cdot u) \subseteq b$ with $(x+y)^{2n} \cdot u \in S$, a contradiction. In particular $P := \sum x$ $(x \notin S)$ is prime, whence we obtain $\mathfrak{A}_S = \mathfrak{A}_P$.

Now we get in any case

$$(a_S \oplus x_S) \circ u_S = a_S \oplus x_S \supset b_S \implies u_S = 1_S \Longrightarrow u \in S ,$$

since otherwise $u \notin S$ would imply $a_S (u^n) e_S = a_S (u^n)_S = a_S \subseteq b_S$ for some exponent $n \in \mathbf{N}$.

Hence a_S is comparable with each x_S since $(a+x)a' = a$ & $(a+x)x' = x$ leads to

$$\begin{aligned} (a+x)(a'+x') = a+x &\rightsquigarrow a_S(a'+x')_S = a_S \\ &\rightsquigarrow (a'+x')_S = 1_S . \end{aligned}$$

Hence $a' + x' \in S$ and thereby $a' \in S \vee x' \in S$ that is $x_S \supseteq a_S \vee a_S \supseteq x_S$.

[2] We choose the way along condition (Q) which is more convenient here. But it should be mentioned that the prime property does not depend on commutativity.

Next we show that in any case the elements x_S above a_S are powers of some compact prime p_S, in particular that $a_S = {p_S}^n$ $(\exists n \in \mathbf{N})$ is satisfied, and that moreover a_S properly contains at least one of these powers.

(a) First let a and thereby b as well be contained in P.

Recall ${P_S}^n = P^n$. Suppose now $P^n \supseteq a_S$ and thereby $P^n \supseteq a$ $(\forall n \in \mathbf{N})$. Then, according to the archimedean property, we get $aP = a$. This leads to some $p \subseteq P$ satisfying $ap = a$, and thereby to $p \in S$ & $p \subseteq P$, a contradiction w.r.t. the definition of P.

Consequently there exists an exponent $m \in \mathbf{N}$ with $P^m \not\supseteq a$ whence by comparability of a_S with all p_S it follows $a_S \supseteq {P_S}^m$, and thereby $a_S \supseteq {x_S}^m$ $(\forall\, x_S$ with $P \supseteq x)$.

But, in a local Prüfer monoid the uniquely determined maximal element M satisfies the implication $M \supset M^2 \Longrightarrow M = \sum(p + x_i)$ $(i \in I)$ with $p, x_i \subseteq M$. So, if M properly contains M^2 then in particular M contains some $p \not\subseteq M^2$, and each element of this type satisfies $x_S \neq 1_S \Longrightarrow p_S \supseteq x_S$, since $x * p \in M$ would imply $(x + p)(x * p) = p \subseteq M^2$. Hence we get $M_S = M = p_S$ and thereby:

$$ {p_S}^\ell({p_S}^\ell * A_S) = A_S \implies {p_S}^\ell * A_S = 1 \vee {p_S}^\ell * A_S \subseteq M = p_S \,, $$

that is $$x_S = {p_S}^\ell \ \ (\exists \ell \in \mathbf{N}) \quad \vee \quad {p_S}^n \,\Big|\, x_S \ \ (\forall n \in \mathbf{N})\,.$$

Thus in case (a) it is shown $x_S \supseteq a_S \Longrightarrow x_S = {p_S}^\ell$ $(\exists \ell \in \mathbf{N})$.

(b) Suppose now $a \not\subseteq P$ but $b \subseteq P$ or equivalently $a \in S$ and $b \subseteq P$. If there is some c_S properly between 1_S and b_S then, of course, S is maximal with respect to c and b, and we may continue as above.

Otherwise it holds $1_S \succeq b_S$ and $1_S \neq P_S \supseteq b_S \leadsto P = P_S = b_S$, and again, we may continue as above.

NEXT send all $x_S \subset a_S$ to 0. This provides a homomorphic $\mathfrak{S}_m$ since together with $u_S, v_S \subset a_S$ we have $u_S \oplus v_S \subset a_S$.

Observe that by construction $a_S = 1_S$ or $a_S = {p_S}^k \subset {p_S}^{k+1}$.

Hence, $\mathfrak{C}$ is a lattice satisfying condition (j), since this condition is satisfied by the localization theorem.

$(ii) \Longrightarrow (iii)$ and $(iii) \Longrightarrow (iv)$ follow nearly immediately.

$(iv) \Longrightarrow (i)$. Since all components are 0-cancellative, that is satisfy the implication $ax = ay \neq 0 \Longrightarrow x = y$, any lattice cube satisfies condition (K) of 7.1.4. Hence, by condition (j) any lattice cube has the Prüfer property, recall 7.1.4. Finally lattice cubes are archimedean by evidence, whence there filter-monoid is archimedean, too, recall any homomorphism of a Prüfer monoid $\mathcal{P}$ generates – in a canonical manner – a homomorphism of its filter monoid, whence any subdirect decomposition of $\mathcal{P}$ leads to a subdirect decomposition of its filter extension of $\mathcal{P}$. $\square$

In [71] it was shown that a divisibility monoid admits a cube extension $\mathfrak{E}^\omega$ with $E := [0,1]$ and

$$a \circ b := \min(1, a+b) \quad , \quad a \wedge b := \min(a,b)$$
$$\text{iff} \qquad A^n \supseteq b \;\; (\forall \in \mathbf{N}) \;\Longrightarrow\; \mathfrak{a} \cdot b = b\,,$$

where A is a filter, $\mathfrak{a}$ is the $v-$ideal, generated by A, and b is the $v-$ideal, generated by b.

But the question remained unsettled what an archimedean filter monoid might yield. By the preceding theorem this question is answered *via* ideal theory.

11.4 P-cancellative AP-ideal-monoids

In this section we study 11.3.1 with respect to P-cancellative DV-IDMs.

11. 4. 1 Proposition. *Let $\mathfrak{A}$ be a commutative P-cancellative DV-IDM. Then the following are pairwise equivalent:*

- (i) *$\mathfrak{A}$ is an AP-IDM.*
- (ii) *All elements of each $\mathfrak{A}_M$ are compact divisors.*
- (iii) *Each $\mathfrak{A}_M$ is a normal archimedean valuation structure.*
- (iv) *$\mathfrak{A}$ is normal and archimedean.*

PROOF. Recall the denotations under 11.3.1

$(i) \Longrightarrow (ii)$. We know that each $\mathfrak{A}_M$ is an AP-IDM. We show that furthermore each $A_S \in \mathfrak{A}_M$ is a power of some compact prime element. According to 11.3.1 the element A_S is prime in $\mathfrak{A}_M$ only if A_S is prime in $\mathfrak{A}$.

Let now P be prime, satisfying $M \supset P$. It follows $Q := \bigcap M^n = P$, since $\mathfrak{A}$ is P-cancellative, whence $\mathfrak{A}/P =: \overline{\mathfrak{A}}$ has no idempotent elements except for $\overline{0}$. Hence each maximal M contains at most one (necessarily minimal) prime element $P \neq M$.

Suppose next $P = P^2$. Then according to the archimedean property all $a \subseteq P$ satisfy $ap = a$ $(p \subseteq P)$ and thereby $a_S \circ p_S = a_S$. But, the set of private units of a_S in $\mathfrak{A}_M$ is closed w. r. t. multiplication.

Hence, by the separation lemma, it follows $a_S = 0_S$ and thereby $P_S = 0_S$, since otherwise there would exist some prime element Q_S different from $M_S = M$ and P_S.

If, however, it holds $P \neq P^2$ and $a, b \subseteq P$ but $a, b \not\subseteq P^2$, then it follows $a + b \subseteq P$ but $a * b \notin P$. Hence in this case we get $(a * b)_S = 1_S$ and thus

$$a_S \oplus b_S = (a_S \oplus b_S) \circ 1_S = (a_S \oplus b_S) \circ (a_S * b_S) = b_S .$$

Consequently it holds $a_S \oplus b_S = b_S = a_S$ and thereby $P_S = p_S$ for any $P \supseteq p \not\subseteq P^2$. In particular, this provides $M_S = m_S$. Hence each A_S is a power of m_S or of p_S.

Thus $\mathfrak{A}_M$ is normal and totally ordered.

$(ii) \Longrightarrow (iii)$. By (ii) each $\mathfrak{A}_M$ is a Mori structure. Hence, according to 11.3.1, $\mathfrak{A}$ is an AP-IDM. Therefore each $\mathfrak{A}_M$ is normal and totally ordered as shown below $(i) \Longrightarrow (ii)$.

$(iii) \Longrightarrow (iv)$. If each $\mathfrak{A}_M$ is a normal valuation structure then each $\mathfrak{A}_M$ and thereby, according to the localization theorem, $\mathfrak{A}$ is normal, too. And if each $\mathfrak{A}_M$ is archimedean then $\mathfrak{A}$ is archimedean, too.

$(iv) \Longrightarrow (i)$ Normality implies the Prüfer property. □

Gilmer had tried, compare [148], to characterize Dedekind domains as domains whose DV-IDMs are cancellative with 0, before he discovered that these structures are weaker then originally expected. This will be demonstrated now.

11. 4. 2 Proposition. *Let $\mathfrak{A}$ be a commutative P-cancellative DV-IDM without zero divisors. Then the following are pairwise equivalent:*

(i) *$\mathfrak{A}$ is an AP-IDM.*

(*ii*) $\mathfrak{A}$ *is distributive and cancellative with* 0 .

(*iii*) $\mathfrak{A}$ *is normal and satisfies* $A \neq 1 \Longrightarrow \bigcap A^n = 0$.

PROOF. First of all: Since $\mathfrak{A}$ is P-cancellative without zero divisors the generators a satisfy: $aX = aY \neq 0 \Longrightarrow X = Y$.

$(i) \Longrightarrow (ii)$. Suppose now $AX = AY \neq 0$. Then in all $\mathfrak{A}_M$ it follows $A_S \circ X_S = A_S \circ Y_S$ whence for $a \subseteq A$ we get $a_S \circ X_S = a_S \circ Y_S$, since – according to 11.4.1 – each A_S is some c_S .

So by localization we get in $\mathfrak{A}$ $a \cdot X = a \cdot Y$ $(\exists a \neq 0)$ and thereby $X = Y$.

$(ii) \Longrightarrow (iii)$. We infer by cancellation

$$\begin{array}{rcl} (A+B)(A+B)^2 & = & (A+B)(A^2+B^2) \\ & \rightsquigarrow & \\ (A+B)^2 & = & A^2+B^2 \, . \end{array}$$

This leads to the Prüfer property, according to 7.2.6, which implies in particular normality, and furthermore, according to 7.3.8,

$$\begin{array}{rcl} x \not\subseteq P \neq 0 & \rightsquigarrow & P(P+x) = P \\ & \rightsquigarrow & P + x = 1 \, . \end{array}$$

Thus every prime element is equal to 0 or maximal and consequently, according to 7.3.3, every $\bigcap M^n$ with maximal M is prime and hence equal to 0. But this yields *a fortiori* $A \subseteq M \rightsquigarrow \bigcap A^n = 0$, that is in particular the archimedean property.

$(iii) \Longrightarrow (i)$. The Prüfer property is certified by 7.2.3 and the archimedean property is certified by $A \neq 1 \Longrightarrow \bigcap A^n = 0$. $\square$

11.5 Ringlike AP-ideal monoids

11. 5. 1 Proposition. *Let* $\mathfrak{A}$ *be a ringlike DV-IDM. Then* $\mathfrak{A}$ *is an AP-IDM if and only if it satisfies:*

(P) $$a_1 + \ldots + a_n \supseteq b \ \Longrightarrow \ a_1 + \ldots + a_n \, \Big| \, b$$

(U) $$U = U^2 \supseteq A \ \Longrightarrow \ UA = A = AU$$

$$\text{(Z)} \qquad P \textit{ prime} \implies P \succeq P^2$$

PROOF. SUFFICIENCY. In any ringlike Prüfer IDM prime elements are idempotent or maximal. Therefore assume that M is maximal satisfying $M^n \neq M^{n+1}$ & $M^n \supseteq b$ $(\forall n \in \mathbf{N})$. Then $\bigcap M^n$ is an idempotent prime element, cf. 7.3.6. So in any case $M^n \supseteq b$ $(\forall n \in \mathbf{N}) \Longrightarrow Mb = b$. Hence $\mathfrak{A}$ is archimedean.

NECESSITY. By the Prüfer property it holds (I), and by the archimedean property any AP-IDM satisfies $\ker A = A$, according to Krull's kernel lemma. In the ringlike case this means that $M \supset X \supseteq M^2$ implies that X is primary, according to proposition 10.3.3.

Assume now $M \supset X \supset M^2$ and $M \supseteq a$ & $X \not\supseteq a$ & $X \supseteq b$ & $M \not\supseteq b$ for a maximal M. Then

$$X \supseteq b = (a+b)(a*b) \ \& \ X \not\supseteq a+b \rightsquigarrow \operatorname{Rad} X = M \supseteq a*b$$

But this leads to $M^2 \supseteq (a+b)(a*b) = b$, a contradiction. □

Next we get

11. 5. 2 Lemma. *Let $\mathfrak{A}$ be a commutative ringlike AP-IDM. Then zero divisors of $\mathfrak{A}$ are exactly the elements A which are contained in some minimal prime P.*

PROOF. First of all recall $\ker A = A$, see above.

Let now A be contained in no minimal prime P_i. Then – by 5.4.6 – for the corresponding primary components Q_i it follows $Q_i \supseteq A * 0$, which leads to $A * 0 = 0$. Hence all zero divisors are contained in some minimal prime element P_i.

Next let P be minimal prime. Then there exists some $e \in \mathbf{N}$ with $(P^e)^2 = P^e =: U$, since otherwise, according to 11.2.3 and 7.3.5, P was not minimal prime. Consequently each compact $\mathrm{x} \subseteq P$ satisfies $\mathrm{x}^e \cdot U = \mathrm{x}^e$ for some suitable exponent $e$and thereby $x^e U^* = 0$ for some $U^* \perp U$ with $U^* \neq 0$, because $U \neq 1$. Therefore there exists for each $0 \neq \mathrm{x} \subseteq P$ a first $\mathrm{x}^m U^* \neq 0$ with $x \cdot \mathrm{x}^m U^* = 0$, may be $x^o U^*$ and this entails $\mathrm{x} * 0 \neq 0$. □

Provided I is even finite, the second part of the preceding proof admits the abbreviation: $\mathrm{x} \subseteq P_i \Longrightarrow \mathrm{x} * 0 \supseteq \bigcap\limits_{j \neq i} Q_j \neq 0 \Longrightarrow \mathrm{x} * 0 \neq 0$.

Apart from the AP-IDMs without zero divisors in the subsequent theorem *special primary* DV-IDMs will play a crucial role. Recall: These are those DV-IDMs, whose elements are powers of a fixed prime element p. More precisely: Motivated by the ring theoretic result of D. D. Anderson, [3], we show:

11. 5. 3 Proposition. *Let $\mathfrak{A}$ be a commutative ringlike AP-IDM. Then the following are pairwise equivalent:*

- (i) *$\mathfrak{A}$ is a finite direct product of components which are primary or don't contain any zero divisors.*
- (ii) *Minimal primes of $\mathfrak{A}$ are compact.*
- (iii) *$\mathfrak{A}$ has only finitely many minimal primes.*
- (iv) *There are finitely many minimal primes P_i $(1 \le i \le n)$, such that each zero divisor of $\mathfrak{A}$ is contained in one of these P_i.*

PROOF. $(i) \Longrightarrow (ii)$. First of all, each component contains exactly one minimal prime element, namely the generating p in the primary case and *0* in the zero divisor free case.

So there are only finitely many elements $(1_1, \dots, P_i, \dots, 1_n)$, that is with components 1_j, except for one component P_i, minimal prime in $\mathfrak{A}_i$, and these are prime in $\mathfrak{A} = \bigotimes\limits_1^n \mathfrak{A}_i$. Consequently exactly elements of this type are minimal prime in $\mathfrak{A}$. Hence the minimal primes P of $\mathfrak{A}$ are compact.

$(ii) \Longrightarrow (iii)$. Let p be a minimal, and by assumption compact prime element, and let Q_i $(i \in I)$ be the family of isolated primary components of 0, satisfying the radical condition $\mathrm{Rad}\ Q_i =: p_i \ne p$. Then p is co-maximal w.r.t. $\bigcap Q_i$, which results as follows:

First we get $(p^e)^2 = p^e =: u$ $(\exists e \in \mathbf{N})$ since otherwise $dis \cap p^n$ would be prime but different from p. So $u \cdot u^* = 0$ $(\exists u^* \perp u)$. Consequently all isolated primary components Q_i of 0 with $\mathrm{Rad}\, Q_i = p_i \ne p$ satisfy $\mathrm{Rad}\, Q_i \not\supseteq u \leadsto Q_i \supseteq u^*$. Hence we get $\bigcap Q_i$ $(p_i \ne p) \supseteq u^*$ and thereby $p \perp \bigcap Q_i$ $(p_i \ne p)$.

Let now Q be the isolated P-component of 0. Then $\mathrm{Rad}\, Q = p \not\supseteq u^*$ leads to $Q \supseteq p^e$. On the other hand we have $p^e \supseteq Q$, since p^e is completely prime and $Q \cdot u^* = 0$. But this means $Q = p^e$. Hence, choosing p_i instead of p and e_i instead of e, we obtain

$$p_i^{e_i} \perp \bigcap_{j\neq i} p_j^{e_j}\,, \tag{11.6}$$

and in addition u^* and u_i^* are idempotent, by $(u^*)^2 \supseteq u\cdot u^*$ and $u \perp u^*$.

Next, let Q be an arbitrary P-primary element. Then P contains at least one p_i and, according to (11.6) it does not contain $p_i^{e_i} * 0$. So, if $J \subseteq I$, this means for minimal p_j $(j \in J)$

$$P \supseteq \bigcap p_j^{f_j} \ (1 \leq f_j \leq e_j\,,\ p_j \text{ min}) \implies P \supseteq p_{j^*} \ (\exists j^* \in J)\,.$$

Hence – by 7.3.4 the elements $p_i^{f_i}$ $(1 \leq f_i \leq e_i)$ are exactly all isolated primary components of $\bigcap p_i^{f_i}$ $(0 \leq f_i \leq e_i)$.

Therefore, according to 10.2.8, if a maximal element M contains elements of type $\bigcap p_i^{f_i}$ in common then these elements have a common minimal prime divisor p_{i^*}. So by ker $A = A$, *products*, *residues* and *sums* on the set

$$\{x \,|\, x = \bigcap p_i^{f_i} \ (0 \leq f_i \leq e_i)\}$$

are built componentwise. This is clear w.r.t. $+$ and $\cap$, and follows w.r.t. $*$ by

$$\bigcap p_i^{k_i} = p_i^{k_i} \cap \bigcap_{j\neq i} p_j^{k_j} = p_i^{k_i} \cdot \bigcap_{j\neq i} p_j^{k_j} \tag{11.7}$$

which in case of $f_i \leq g_i$ $(\forall i \in I)$ entails – recall the powers of any p_i are completely prime:

$$\Big(p_i^{f_i} \cdot \bigcap_{j\neq i} p_j^{f_j}\Big) \cdot X \subseteq p_i^{g_i} \cdot \bigcap_{j\neq i} p_j^{g_j} \Longrightarrow p_i^{g_i - f_i} \supseteq X \Longrightarrow \bigcap_{i\in I} p_i^{g_i - f_i} \supseteq X\,.$$

$$\text{and} \qquad \Big(\bigcap_{i\in I} p_i^{f_i}\Big) \cdot \Big(\bigcap_{i\in I} p_i^{g_i - f_i}\Big) \subseteq \bigcap_{i\in I} p_i^{g_i}$$

that is

$$\Big(\bigcap_{i\in I} p_j^{f_j}\Big) * \Big(\bigcap_{i\in I} p_j^{g_j}\Big) = \Big(\bigcap_{i\in I} p_i^{g_i - f_i}\Big) \tag{11.8}$$

Finally (11.8) implies:

$$(\bigcap p_i^{f_i} * \bigcap p_i^{g_i}) * \bigcap p_i^{g_i} = (\bigcap p_i^{g_i} * \bigcap p_i^{f_i}) * \bigcap p_i^{f_i}\,.$$

Consequently the considered substructure is closed under Σ, $\cap$ and $\cdot$, and in addition, according to 12.4.1, it satisfies $A * \Sigma B_i = \Sigma(A * B_i)$. But this means that along the lines of the proof of 12.1.1 $\mathfrak{A}$ satisfies ACC for elements of type $\bigcap p_j^{e_j}$ $(j \in J \subseteq I)$. Hence 0 has only finitely many isolated primary components whereby $\mathfrak{A}$ has only finitely many minimal primes.

$(iii) \Longrightarrow (iv)$. Consult 11.5.2

$(iv) \Longrightarrow (i)$. To begin with, according to 11.5.2 there are only finitely many minimal prime elements P_i , and, according to 10.2.8, each pair of different elements P_i and thereby also each pair of the corresponding isolated primary components Q_i of 0 is co-maximal where Q_i is of type $P^{e_i} = (P^{e_i})^2$.

Hence $\mathfrak{A} = \bigotimes\limits_1^n (\mathfrak{A}/Q_i)$ provides a direct decomposition with each of the components $\mathfrak{A}_i := \mathfrak{A}/Q_i$ $(1 \le i \le n)$ having exact one minimal prime element $\overline{P}_i$.

Suppose now $\overline{P}_i = \overline{0}_i$. Then $\overline{\mathfrak{A}}_i$ has no zero divisors.

But if $\overline{P}_i$ differs from $\overline{0}_i$ then it follows $P_i^2 \neq P_i$. Hence, in this case, P_i is not only minimal in $\mathfrak{A}$, according to 11.2.3, but at the same time it is maximal. From this, by $P_i^{e_i} = 0_i$ $(\exists e_i \in \mathbf{N})$ and $P_i \succ {P_i}^2$, observing the archimedean property we get from 7.3.1 the compactness of $\overline{P_i}$, i. e. $\overline{P}_i = \overline{p}_i$ for any p_i with $P_i \supseteq p_i \not\subseteq P_i^2$. Thus, in this case $\overline{\mathfrak{A}}_i$ turns out to be primary. $\square$

11. 5. 4 Corollary. *A ringlike Mori-IDM has the Noether property iff it has only finitely many minimal prime elements iff* $\ker 0$ *has only finitely many components.*

Chapter 12

Factorial Structures

A classical problem of commutative ring theory is whether each ideal is a product of prime ideals. If so, then in addition it holds $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \,|\, \mathfrak{b}$. In analogy we ask under which conditions the elements of an AML are products of primes.

Usually such prime factorizations are studied in Noether structures.

In this section we present conditions yielding prime factorization even in arbitrary, not necessarily Noether DV-IDMs. Provided the underlying DV-IDM is even hyper-normal, these conditions are not only sufficient but even necessary.

12.1 UF-Structures

In the following we will call UFS (U̲nique F̲actorization S̲tructure) each AML, whose elements are unique products of primes.

12. 1. 1 Proposition. *Let $\mathfrak{A}$ be a commutative DV-IDM. Then each of the two subsequent conditions is sufficient in order that $A \supseteq B \Longrightarrow A \Big| B$ be satisfied and that each $A \in \mathcal{A}$ is a product of primes:*

(a) $$A * \sum_{i \in I} B_i \;=\; \sum_{i \in I} (A * B_i)$$

(b) $$(\bigcap_{i \in I} A_i) * B \;=\; \sum_{i \in I} (A_i * B),$$

and in addition (a)*, and* (b) *as well, yield that irredundant prime decompositions of the same element coincide up to permutation.*

PROOF. As is easily checked it holds $a(a*b) = b(b*a)$ and each condition implies $a*b+b*a = 1$, replace the first components by $a+b$ and apply (a) – replace the second components by $a \cap b$ and apply (b). Thus we get

$$\begin{aligned}(a+b)(a*b) &= a(a*b)+b(a*b) \\ &= b(b*a)+b(a*b) \\ &= b(a*b+b*a) \\ &= b\,.\end{aligned} \tag{12.3}$$

In order to verify afterwards the UF-property, We now show that both, (a) and (b), imply condition (M) $A \supseteq B \Longrightarrow A \,\big|\, B$.

Ad (a): By (a) $\mathfrak{A}$ is a Prüfer AML. Let $a_1 \subset a_1 + a_2 \subset a_1 + a_2 + a_3 \subset \ldots$ be an infinite chain of finitely generated elements $A_n = a_1 + \ldots + a_n$. Then it results $(\sum\limits_{n \in N} A_n) \supset A_m$ $(\forall m \in \mathbf{N})$ and thereby $(\sum\limits_{n \in N} A_n) * A_m \neq 1$. But, because of 1-compactness this leads to the contradiction

$$\begin{aligned}1 &= (\sum_{n \in N} A_n) * (\sum_{m \in N} A_n) \\ &= \sum_{m \in N} ((\sum_{n \in N} A_n) * A_m) \\ &\neq 1\,.\end{aligned}$$

Hence $\mathfrak{A}$ has the Prüfer and the Noether property.

Ad (b): By (b) $\mathfrak{A}$ is a Prüfer AML, according to (12.3). Hence it holds $(a+c) \cdot (a*c) = c$. Furthermore we get:

$$x \cdot \bigcap_{i \in I} a_i = \bigcap_{i \in I} (x \cdot a_i) \quad (i \in I),$$

SINCE

$$\begin{aligned}(\bigcap x a_i) * (x \cdot \bigcap a_i) &= \sum (x a_j * x \cdot \bigcap a_i) \quad (j, i \in I) \\ &= \sum_{j \in J} (a_j * (x * x \cdot \bigcap a_i)) \\ &\supseteq \sum_{j \in J} (a_j * \bigcap a_i) \\ &= (\bigcap a_i) * (\bigcap a_i) \\ &= 1 \quad \text{(by (b))}.\end{aligned}$$

So, distributing alternatively we are led to

$$\begin{aligned} \sum (a_i + c) \cdot \bigcap (a_i * c) &= A \cdot \bigcap (a_i * c) \\ &= c\,. \end{aligned}$$

But this means $A \supseteq B = \sum\limits_{j \in J} b_j \Longrightarrow A(A * b_j) = b_j \ (\forall\, j \in J)$, from which follows $A \supseteq B \Longrightarrow A \Big| B$.

We now start from some $\subset^*$-chain

$$A \subset^* A_1 \subset^* A_2 \subset^* \dots$$

satisfying $A_{i+1} = X_i * A_i \ (\exists\, X_i)$. Here each A_i is a right residuum of A, recall $X * (Y * Z) = YX * Z$, and thereby equal to $(A_i * A) * A$. We consider

$$1 \supseteq B_1 \supseteq B_2 \supseteq \dots$$

with $B_i = A_i * A$, and form $B := \bigcap B_i$. Since A is a divisor it follows $B \supseteq A \rightsquigarrow B(B * A) = A$, and by $A_i = (A_i * A) * A$ all A_i are of type

$$A_i = B_i * A = (B_i * B) \cdot (B * A)\,.$$

FOR: suppose $X \supseteq Y \supseteq Z$. Then it follows

$$\begin{aligned} X * Z &= (X * Y)U \ \ (\exists\, U) \\ &\rightsquigarrow \\ Z &= YU \\ &\rightsquigarrow \\ (Y * Z)V &= U \ \ (\exists\, V) \\ &\rightsquigarrow \\ (X * Y) \cdot (Y * Z)V &= X * Z\,.) \end{aligned}$$

But this means that $A_i \neq A_j$ implies $B_i * B \neq B_j * B$ whence the chain

$$B_1 * B \subset B_2 * B \subset \dots$$

would not finish if the chain A_i would be infinite. But the ascending chain

$$B_1 * B \subset B_2 * B \subset \dots$$

cannot be infinite, since this would imply the contradiction

$$\begin{aligned} 1 &= B * B = (\bigcap B_i) * B \\ &= \sum (B_i * B) \\ &\neq 1 \quad (i \in I) \end{aligned}$$

So in both cases each $\subset^*$-chain is finite.

We now verify the UF-property by combining the divisor property and $\subset^*$-chain condition.

First of all P is prime iff $P = AB \Longrightarrow P = A \vee P = B$:

By the divisor property we get $X \supset P$ & $Y \supset P \Longrightarrow XY \supset P$ which by the assumption above yields:

$$\begin{aligned} P \supseteq UV &\Longrightarrow P \supseteq (P+U)\cdot(P+V) \\ &\Longrightarrow P = U + P \vee P = V + P \\ &\Longrightarrow P \supseteq U \vee P \supseteq V\,. \end{aligned}$$

Suppose now that there would exist some X different from all prime factor products. Then the set of *indecomposable* elements would not be empty and hence would contain some $\subset^*$-maximal element A. So, by the divisor property we would get $A = BC$ and thereby $A = (B*A)\cdot((B*A)*A)$ with $B \supset A \subset C$. But this would imply $A \subset^* B*A$ and $A \subset^* (B*A)*A$ whence $B*A$ and $(B*A)*A$ would be prime factor products, a contradiction!

It remains to show that irredundant prime factor decompositions of the same element coincide up to permutation. To this end we take into account that each irredundant prime factor product $P_1 \cdot \ldots \cdot P_n$ satisfies $P_i \supseteq P_j \Longrightarrow P_i = P_j$, recall the implication $A \supset P \Longrightarrow P = AX = AP$. This completes the proof on the grounds of 8.1.4 ($P^m \supseteq P^n B \Longrightarrow P^m \supseteq P^n \vee P \supseteq B$). □

12.2 Special cases

We now study some situations, close to classical ring theory.

12. 2. 1 Proposition. *Let $\mathfrak{A}$ be a hyper-normal DV-IDM. Then the following are equivalent:*

(*i*) $\mathfrak{A}$ *is a Noether Mori AML.*

(*ii*) $\mathfrak{A}$ *satisfies* (a) $A * \sum\limits_{i\in I} B_i = \sum\limits_{i\in I} (A * B_i)\,.$

PROOF. Let (i) be satisfied. Then $\mathfrak{A}$ is normal, since from (Y) and $a\,(a*b+b*a) = a$ it results $(a*0+a*b)+b*a = 1$ with $a*0+a*b = a*b$. Furthermore we get (a). To this end consider some $\sum B_i$. Then by the Noether property there exists a finite chain

$$B_1 \subset B_1 + B_2 \subset B_1 + B_2 + B_3 \subset \ldots \subset B_1 + \ldots + B_n\,,$$

whose final element is equal to $\sum\limits_{i\in I} B_i$. But putting $B_1 + \ldots + B_k =: C_k$ this provides:

$$\sum_1^n (A * B_i) = \sum_1^n (A * C_i) = A * \sum_1^n B_i\,.$$

Consequently $\mathfrak{A}$ satisfies condition (ii) .

Let now condition (ii) be satisfied. Then condition (i) follows along the lines in the proof of 12.1.1. □

12. 2. 2 Proposition. *Let $\mathfrak{A}$ be a hyper-normal DV-IDM. Then the following are equivalent:*

(i) *Each $A \in \mathcal{A}$ is a product of maximal elements.*

(ii) *$\mathfrak{A}$ satisfies* (b) $(\bigcap\limits_{i\in I} A_i) * B = \sum\limits_{i\in I} (A_i * B)\,.$

PROOF. $(i) \Longrightarrow (ii)$. From condition (i) it follows that $\mathfrak{A}$ is an atomic Mori structure. In particular this means that $\mathfrak{A}$ is finite since 0 has only finitely many divisors. Hence $\mathfrak{A}$ satisfies condition (ii).

$(ii) \Longrightarrow (i)$. Suppose (ii). Then $\mathfrak{A}$ is a hyper-normal Noether Mori structure. It remains to verify that any prime is maximal.

To this end let P be prime and $1 \neq M \supset P$ with maximal M. Then it follows

$$\textstyle\bigcap_{n\in N} M^n =: U = U^2\,,$$

since either some power of M is idempotent or otherwise $\bigcap_{n\in N} M^n$ is a prime element which must be idempotent, too, according to 11.2.3

Hence we get $U = U^2 \supseteq P$. But $U \supset P$ is impossible since $U \neq P$ would lead to $U \supset P \supseteq U^*$. So it holds $U = P$. But this leads to

$$1 = P * P = U * P = (\bigcap_{n\in N} M^n) * P = \sum_{n\in N} (M^n * P) = \sum P = P\,.$$

a contradiction! Consequently P is maximal. □

12.3 Mori Criterions in the integral Case

We start with a general proposition not based on the cancellation property
12. 3. 1 Proposition. *Any AMV, whose elements $A \neq 0$ are products of maximal elements has the Mori property (M).*

PROOF. Evidently, under the assumption above any prime element is a prime divisor and starting from $A \supseteq b \neq A(A * b)$ by 5.4.8 we are led to some maximal M satisfying $b * bM = M$ and $M^n \succeq M^{n+1}$ $(\forall\, n \in \mathbf{N})$. So, by the **divisor lemma** we get $Q := \bigcap M^n \,|\, b$ $(n \in \mathbf{N})$ whence Q must be prime by (5.26), that is must be equal to 0, a contradiction. □

One of KRULL's fundamental theorems, apart from those presented above, is a simple but important lemma. This lemma was added in proof by KRULL in [], after he had omitted this fact in his original version. We give an extension and generalization here:

12. 3. 2 The Finiteness Lemma. *Let $\mathfrak{A}$ be a complete lattice and suppose $A(A * B) = B = B(B : A)$ with cancellable divisor B. Then also A is a cancellable divisor.*

If moreover $\mathfrak{A}$ is an AML and B is compact, then also A is compact.

PROOF. Clearly, divisors of cancellable elements are cancellable. Suppose now $A \cdot (A * B) = B$ with cancellable divisor B. Then it results:

$$\begin{aligned} A \supseteq C &\implies B = A \cdot (A * B) \supseteq C \cdot (A * B) \\ &\implies AY \cdot (A * B) = C \cdot (A * B) \\ &\implies A \cdot Y = C \ \ (\exists\, Y)\,. \end{aligned}$$

Let now $\mathfrak{A}$ be algebraic and suppose that B is a cancellable compact divisor. Then it follows:

$$\begin{aligned} A \cdot (A * B) = B &\implies B = (\sum_1^n a_i) \cdot (A * B) \\ &\implies A = \sum_1^n a_i \ \ (\exists\, a_i \ \ (1 \leq i \leq n))\,. \end{aligned}$$

Hence, divisors of cancellable generators are again divisors, compare [245]. □

12. 3. 3 Corollary. (Krull). *If $\mathfrak{A}$ is generated by a cancellable monoid*

$\mathfrak{A}_c$, *then* $\mathfrak{A}$ *is a Mori ideal monoid iff* $\mathfrak{A}$ *has the Noether and the Prüfer property.*

Furthermore it holds:

12. 3. 4 Proposition. *Let* $\mathfrak{A}$ *be an integral ideal monoid. Then* $\mathfrak{A}$ *is an UF-ideal-monoid iff* $\mathfrak{A}$ *is a Mori structure and this is the case iff* $\mathfrak{A}$ *is cancellable with* 0, *satisfying moreover condition* (J) .

PROOF. (a) The conditions above are necessary. This is clear w.r.t. (J) and it results in case of the cancellation property with 0 from the implication $A \supseteq c \Longrightarrow A \cdot B = c \ (\exists B)$.

(b) The stated conditions are sufficient:

SINCE: First of all $A * B + B * A = 1 = A : B + B : A$ is evident, whence $\mathfrak{A}$ has the Prüfer property. And, moreover, condition (S) is fulfilled. To this end observe that any prime element P with $P^s \supset X \supset P^{s+1}$ implies the existence of elements a, b satisfying

$$a \subseteq P^s \quad \& \quad a \not\subseteq X \ \& \ b \subseteq X \quad \& \quad b \not\subseteq P^{s+1} \quad \& \quad P(P + a * b) = P\,.$$

This would imply next $P + a * b = 1$ from which by 7.3.2

$$\begin{aligned} P^{s+1} + (a + b) &= (P^{s+1} + (a + b)) \cdot (P + a * b) \\ &= P^{s+1} + b \end{aligned}$$

would result, a contradiction! Consequently it holds $P^s \succeq P^{s+1}$ – for all exponents s.

But this means, in case of $P^n \supseteq A \ (\forall n \in \mathbf{N})$, that $Q := \bigcap_{n\in N} P^n$ is prime by 7.3.5 satisfying $Q \succeq Q^2$. Consequently, by 7.3.9, we get (A′), that is the archimedean property for all prime elements P, which leads to the general archimedean property (A). □

Next applying 5.3.9 and 8.1.7 we obtain:

12. 3. 5 Proposition. *Any AMV, whose elements* $A \neq 0$ *are products of maximal elements has the Mori property (M).*

PROOF. Evidently, under the assumption above any prime element is a prime divisor and starting from $A \supseteq b \neq A(A * b)$ by 5.4.8 we are led to some maximal M satisfying $b * bM = M$ and $M^n \succeq M^{n+1}$ $(\forall\, n \in \mathbf{N})$. So, by the **divisor lemma** we get $Q := \bigcap M^n \,|\, b$ $(n \in \mathbf{N})$ whence Q must be prime by (5.26), that is must be equal to 0, a contradiction. $\square$

We now turn to laws of distributivity.

12. 3. 6 Proposition. *Let $\mathfrak{A}$ be a commutative AML generated by a cancellative monoid of divisors with zero, say $\mathcal{A}_c$. Then $\mathfrak{A}$ has the multiplication property if and only if $\mathfrak{A}$ is cancellative with zero, satisfying*

$$\text{(D+)} \qquad X_i \supseteq b \neq 0 \;\; (\forall\, i \in I) \implies A + \bigcap X_i = \bigcap (A + X_i) \;\; (i \in I).$$

PROOF. NECESSITY: Obviously the conditions are necessary, recall that property (M) implies the unique factorization property whence any B has only finitely many supelements.

SUFFICIENCY: It holds $(a+b)\cdot(a+b)^2 = (a+b)(a^2+b^2)$ and thereby $ab \subseteq a^2+b^2$ that is $ab = (ab \cap a^2) + (ab \cap b^2) = (ab)(ab * aa + ab * bb) = (ab)(b*a+a*b)$, leading by cancellation to the property $a*b+b*a = 1$. In particular by 7.2.3 and (D+) this means that $\mathfrak{A}$ has the Prüfer property.

Next, if M is maximal and moreover a divisor and if P is prime, then $M \supset P$ would lead to $M \cdot P = P$ and hence by cancellation to $M = 1$. Consequently, if all maximal elements are divisors there cannot exist any non maximal prime elements, except for 0, possibly. Consequently, by the **divisor lemma**, all we have to show is that maximal elements are divisors, since by the Prüfer property $\bigcap\limits_1^\infty M^n$ is prime.

But there are no idempotent maximal elements different from 0 since $\mathfrak{A}$ is cancellative (with zero).

So, let $M := \sum m_i$ $(i \in I)$ be maximal with $c \in M$ and $c \notin M^2$. Consider $(\sum m_i) * c = \bigcap (m_i * c)$. By (n) we get $(m_i + c)\cdot(m_i * c) = c$. Hence M cannot contain any $m_i * c$. Consequently it holds $M + \bigcap (m_i * c) = \bigcap (M + m_i * c) = 1 \overset{(5.11)}{\rightsquigarrow} M \,|\, c$. $\square$

12. 3. 7 Proposition. *An integral commutative DV-IDM $\mathfrak{A}$ is a Mori AML iff it satisfies one of the subsequent distributivity laws:*

$$\text{(D1)} \qquad A \cdot \bigcap B_i \;=\; \bigcap AB_i$$

$$\begin{array}{llcl}
\text{(D2)} & A * \sum B_i & = & \sum (A * B_i) \\
\text{(D3)} & \bigcap A_i & \neq & 0 \\
\Longrightarrow & (\bigcap A_i) * B & = & \sum (A_i * B)\,.
\end{array}$$

PROOF. (a) The conditions above are necessary, since the cancellation law is obvious by (M), whereby we are led to (D1) through (D3) as follows:

(D1) and (D2) are evident for $A = 0$. Therefore we may start from cancellable elements A and $\bigcap A_i$, respectively. We put

$$\sum X_i := \sum_{i\in I} X_i \quad \text{and} \quad \bigcap X_i := \bigcap\nolimits_{i\in I} X_i\,.$$

Then condition (D1) follows by

$$\begin{aligned}
A \cdot \bigcap B_i &= A(\bigcap A * AB_i) \\
&= A \cdot (A * (\bigcap AB_i)) \\
&= \bigcap AB_i\,,
\end{aligned}$$

and condition (D2) follows by

$$\begin{aligned}
A \cdot (A * \sum B_i) &= A \cap \sum B_i \\
&= \sum (A \cap B_i) \\
&= \sum A(A * B_i) \\
&= A \cdot \sum (A * B_i) \\
&\rightsquigarrow \\
(A * \sum B_i) &= \sum (A * B_i)\,.
\end{aligned}$$

Finally we get condition (D3) from

$$\begin{aligned}
\bigcap A_i) \cdot (\sum (A_i * B)) &= \bigcap (A_i \sum (A_i * B)) \quad \text{(by (D1))} \\
&\supseteq \bigcap (A_i \cap B) \\
&= (\bigcap A_i) \cap B \\
&= (\bigcap A_i) \cdot ((\bigcap A_i) * B) \\
&\rightsquigarrow \\
\sum (A_i * B) &\supseteq (\bigcap A_i) * B \supseteq \sum (A_i * B)\,.
\end{aligned}$$

(b) The conditions above are sufficient.

SINCE: (D1) certifies the assertion as shown above below 12.1.1 while (D2) and (D3) worked even as conditions. □

12.4 Factorial Duo structures

We start from a not necessarily commutative ideal structure satisfying the equivalence $(A\,|_\ell\, B \Longleftrightarrow A\,|_r\, B)$, called *duo DV-IDM.*

12. 4. 1 Proposition. *Let $\mathfrak{A}$ be a duo DV-IDM. Then the following are equivalent:*

(i) *Each $A \in \mathcal{A}$ is a product of maximal elements.*

(ii) $(A : B) * A = B : (A * B)$.

PROOF. First of all recall that (ii) is self-dual.

$(i) \Longrightarrow (ii)$. Suppose (i). Then each prime element P of $\mathfrak{A}$ is an atom and a divisor as well. From this commutativity follows because maximal elements $P \neq Q$ satisfy $PQ = AP = QB$. Observe: $Q \supseteq A$ and $P \supseteq B$ implies $PQ \supseteq QP \supseteq PQ$ and thereby $UV = VU$.

Since prime elements are divisors, according to 8.1.3 each prime element is even completely prime.

Consequently in case of $U \supseteq V$ the right quotient $U * V$ is equal to the *rest product* of the *canonical decomposition* of U w. r. t. the canonical decomposition of V. But, this leads to

$$\begin{aligned}(A * B) * B &= ((A + B) * B) * B \\ &= ((A + B) * A) * A = (B * A) * A.\end{aligned}$$

$(ii) \Longrightarrow (i)$. First of all: any prime element is maximal. To this end observe that $1 \supseteq A \supset P \Longrightarrow A = (A : P) * A = P : (A * P) = P : P = 1$.

Next it holds: $\quad A + B \subseteq (A : B) * A$

and it results: $\quad A + B \supseteq (A : B) * A$.

Put $A + B =: C$. Then it follows $A * C = 1 = C : B$ and thereby

$$\begin{aligned}C : ((A : B) * A) &= (C : (A * C)) : ((A : B) * A) \\ &= ((A : C) * A) : ((A : B) * A) \\ &= (A : C) * (A : ((A : B) * A)) \\ &= (A : C) * (A : B) \\ &= ((A : C) * A) : B \\ &= (C : (A * C)) : B \\ &= C : B = 1.\end{aligned}$$

Hence $$A : (B * A) = \ A + B \ = (A : B) * A\,.$$

Choose now some $C \subseteq \bigcap A_i \ \ (i \in I)$. Then it results:

$$\begin{array}{rrcl}
 & x & \subseteq & \sum\,(A_i\, * C)\ \ (i \in I) \\
\Longleftrightarrow & C : x & \supseteq & C : \sum\,(A_i\, * C) \\
\Longleftrightarrow & C : x & \supseteq & \bigcap\,(\,C : (A_i\, * C)\,) = \bigcap\, A_i \\
\Longleftrightarrow & (C : x) * C & \subseteq & \big(\bigcap\, A_i\,\big) * C \\
\Longleftrightarrow & x & \subseteq & \big(\bigcap\, A_i\,\big) * C\,, \\
 & & \rightsquigarrow & \\
 & \big(\bigcap\, A_i\,\big) * C & = & \sum\,(A_i\, * C) \\
\& & C : \big(\bigcap\, A_i\,\big) & = & \sum\,(C : A_i\,)\ ,
\end{array}$$

that is in general:

$$\begin{array}{rcl}
\big(\bigcap\, A_i\,\big) * C & = & \big(\bigcap\, A_i\,\big) * \big(C \cap y \bigcap A_i\big) \\
 & = & \sum\,\big(A_i\, * \big(C \cap \bigcap A_i\big)\big) \\
 & \subseteq & \sum\,(A_i\, * C) \\
\rightsquigarrow \big(\bigcap\, A_i\,\big) * C & = & \sum\,(A_i\, * C)\ .
\end{array}$$

Hence, we could continue along the lines of 12.1.1(b). But (ii) offers the shorter calculation:

$$\begin{array}{rcl}
A \cap B & = & x : (\,(A \cap B) * x\,) \\
 & = & x : (A * x + B * x) \\
 & = & x : (\,(\,(A * x) : (B * x)\,) * (A * x)\,) \\
 & = & x : (\,(\,A * (x : (B * x))\,) * (A * x)\,) \\
 & = & x : (\,(A * B) * (A * x)\,) \\
 & = & x : (\,A\,(A * B) * x\,) \\
 & = & A\,(A * B)\,, \\
 & \rightsquigarrow & \\
A \supseteq B & \Rightarrow & A\,|_\ell\, B\ \ \&\ \ A\,|_r\, B\,.
\end{array}$$

It remains to show that $\mathfrak{A}$ has the Noether property which, according to 12.1.1(a), is done by the calculation:

$$\begin{aligned} C * \sum A_i &= (C*0) : \bigcap (A_i \, * 0) \\ &= \sum (\, (C*0) : (A_i \, * 0)\,) \\ &= \sum (\, C * (0 : (A_i \, * 0)\,)\,) \\ &= \sum (C * A_i\,)\,. \end{aligned}$$

Thus the proof is complete. □

A bit more general we can deduce from the preceding proposition:

12. 4. 2 Corollary. *Let* $\mathfrak{A}$ *be a cancellative DV-IDM with* 0 *. Then, any not vanishing* A *of* $\mathfrak{A}$ *is a product of finitely many maximal elements iff all* $A \neq 0 \neq B$ *satisfy the equation*

$$(A : B) * A = (B : A) * B\,.$$

PROOF. Each pair $A, B \neq 0$ of $\mathfrak{A}$ has a not vanishing intersection C with $[C, 1]$ satisfying (ii) of 12.4.1 □

Chapter 13

v- and t-Ideals

13.1 Preliminaries

By the theorems of chapter 5 various characterizations of algebraic Prüfer AMLs were given, by the theorems of chapter 7 various characterizations of algebraic Mori structures were presented. One crucial assumption of these chapters has been the algebraic property. For instance: Lattice distributivity of Prüfer AMLs was proven by applying the algebraic property, and moreover (MP)$\Longrightarrow$(M) resulted from algebraic property of the underlying structure $\mathfrak{A}$.

In this chapter we are concerned with concrete monoids of ideals, which need not be ideal monoids. Again, it will mean no essential restriction that we start from commutative structures, since condition (M) implies the archimedean property even though $\mathfrak{A}$ fails to be algebraic. Consult [68] and [69].

Mainly we will study monoids of v- and t-ideals, whose importance was pointed out already in former chapters. To this end we start from a commutative monoid $\mathfrak{S}$, considered with respect to some fixed monoid of ideals $\mathfrak{A}$. In order to emphasize that we are concerned with monoids of ideals rather than with ideal monoids, we will denote ideals in general by lower case Gothic letters, and ideals, generated by $A \subseteq S$, by $\langle A \rangle$. Moreover, in the finite case we will freely write $\langle a_1, \ldots, a_n \rangle$ instead of $\langle \{a_1, \ldots, a_n\} \rangle$, and given some $\mathfrak{a}$ and some A the set A should be assumed to be a generating subset of $\mathfrak{a}$.

Furthermore, let us agree, to call $(S, \cdot, 1)$ itself, for instance, a *Prüfer* *monoid* or a *Mori monoid*, without any suffix whenever the monoid of ideals under consideration has the corresponding property and is well fixed.

In detail we will do the following:

After a description of Prüfer structures in general we study the cancellative case. It will turn out that the Prüfer property (P) here is equivalent to the equation $\langle a\rangle * \langle b\rangle + \langle b\rangle * \langle a\rangle = \langle 1\rangle$, whence 7.2.6 will contribute to characterizations of monoids of ideals of cancellative monoids.

Next we will characterize Mori v-monoids by the archimedean property combined with the condition that all $\langle a\rangle * \langle b\rangle$ be divisors.

We then turn to monoids of v- and t-ideals, respectively, of cancellative monoids. Here we will present results on t-ideals, in classical ring theory due to KRULL and on v-ideals due to VAN DER WAERDEN.

13.2 The general Case

13. 2. 1 Proposition. *Let $\mathfrak{S}$ be a monoid and $\mathfrak{A}$ some monoid of ideals of $\mathfrak{S}$. Then $\mathfrak{S}$ is a Prüfer monoid w. r. t. $\mathfrak{A}$ iff $\mathfrak{A}$ for finitely generated $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ satisfies:*

(P1*) $$\langle a\rangle = \langle a\rangle \cdot (\langle a\rangle * \mathfrak{b} + \mathfrak{b} * \langle a\rangle)$$

(P1:) $$\langle a\rangle = (\mathfrak{b} : \langle a\rangle + \langle a\rangle : \mathfrak{b}) \cdot \langle a\rangle$$

(P2) $$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c}).$$

PROOF. Necessity is certified by the proof of 7.1.3

Sufficiency: By definition each $\langle a\rangle$ is a divisor. So, let us assume that all $\langle a_1, \dots, a_k\rangle$ with $(k \le n)$ are (already) divisors. Then we get by assumption

$$\begin{aligned}
\langle a\rangle &= \langle a\rangle \cdot (\langle a\rangle * \langle a_1, \dots, a_n\rangle + \langle a_1, \dots, a_n\rangle * \langle a\rangle) \\
&= \langle a\rangle \cdot (\langle a\rangle * \langle a_1, \dots, a_n\rangle) + \langle a\rangle \cdot (\langle a_1, \dots, a_n\rangle * \langle a\rangle) \\
&= \langle a_1, \dots, a_n\rangle \cdot (\langle a_1, \dots, a_n\rangle * \langle a\rangle) + \langle a\rangle \cdot (\langle a_1, \dots, a_n\rangle * \langle a\rangle) \\
&= \langle a_1, \dots, a_n, a\rangle \cdot (\langle a_1, \dots, a_n\rangle * \langle a\rangle).
\end{aligned}$$

Hence, all $(n+1)$-generated ideals are divisors, too. This completes the proof by induction. $\square$

By 13.2.1 Prüfer monoids are characterized by a weakened distributivity but a stronger absorption law.

If $\mathfrak{A}$ is a left Prüfer AML then a finitely generated A divides a finitely generated B from the left iff there exists a finitely generated X satisfying $A \cdot X = B$. So in algebraic left Prüfer structures compact elements A, B produce a compact $A \cap B$ which thereby is a left divisor. This is different in non algebraic Prüfer structures!

For example: In the additive v-ideal monoid of real numbers $r = a + b\pi$ $(a, b \in \mathbf{N}^0)$ it holds $\langle 2 \rangle \supseteq \langle \pi \rangle$ but, of course, there is no finitely generated v-ideal summand of, for instance, $\langle 2 \rangle$ with respect to $\langle \pi \rangle$. From this point of view it seems desirable to get some more information about Prüfer structures.

13. 2. 2 Proposition. *Let $\mathfrak{S}$ be a Prüfer monoid. Then the meet $\mathfrak{a} \cap \mathfrak{b}$ of compact divisors $\mathfrak{a}$, $\mathfrak{b}$ is again a divisor.*

PROOF. Suppose $\mathfrak{a} \cap \mathfrak{b} \supseteq \langle \mathfrak{x} \rangle$. It follows $\mathfrak{a} \cdot (\, \mathfrak{a} * \langle x \rangle\,) = \langle x \rangle = \mathfrak{b} \cdot (\, \mathfrak{b} * \langle x \rangle\,)$ (already from (P1)). And this implies

$$\begin{aligned} & (\mathfrak{a} \cap \mathfrak{b}) \cdot (\mathfrak{a} * \langle x \rangle + \mathfrak{b} * \langle x \rangle) \\ = \;& \mathfrak{a}\,(\mathfrak{a} * \mathfrak{b})(\,\mathfrak{a} * \langle x \rangle\,) + \mathfrak{b}\,(\mathfrak{b} * \mathfrak{a})(\,\mathfrak{b} * \langle x \rangle\,) \\ = \;& \langle x \rangle \cdot (\mathfrak{a} * \mathfrak{b}) + \langle x \rangle \cdot (\mathfrak{b} * \mathfrak{a}) \\ = \;& \langle x \rangle \cdot (\mathfrak{a} * \mathfrak{b} + \mathfrak{b} * \mathfrak{a}) = \langle x \rangle\,. \end{aligned}$$ $\square$

We now turn to Mori v-monoids. We begin with the general case and then will specialize the results towards the classical theorem that a cancellative monoid is a Mori v-monoid iff it is *completely integrally closed.*

13. 2. 3 Proposition. *A commutative monoid $\mathfrak{S}$ is a Mori v-monoid iff the semigroups $\mathfrak{V}$ of v-ideals $\mathfrak{V}$ satisfies the conditions:*

(A) $\mathfrak{V}$ *has the archimedean property.*

(d) *Every $\langle a \rangle * \langle b \rangle$ is a divisor.*

PROOF. Assume $\mathfrak{b} = b$ and $s \supseteq \mathfrak{a} \circ (\mathfrak{a} * b)$. Then by the **divisor lemma** we get $b \circ (b * s) = b = b \cap s$, that is $s \mid b$.

It remains to show $\mathfrak{a} \circ (\mathfrak{a} * b) \supseteq b$. To this end suppose $s \,|\, \mathfrak{a}(\mathfrak{a} * bt)$. Then it follows $\mathfrak{a} \supseteq bt \supseteq \mathfrak{a} \circ (\mathfrak{a} * bt)$, $s \supseteq \mathfrak{a} \circ (\mathfrak{a} * bt)$, and $bt * s$ is a divisor. Hence, it holds $bt = \mathfrak{a} \circ (\mathfrak{a} * bt)$ or we can apply 13.2.3 by putting $bt := B$ and $s := S$.

This leads – in any case – to $bt \cup s = bt$ and thereby to $s \,|\, b \cdot t$. Thus it results $\mathfrak{a} \circ (\mathfrak{a} * b) = b$.

Consequently, the conditions (A) and (d) are sufficient.

On the other hand, the conditions (A) and (d) are necessary, too.

FOR: Recall $\mathfrak{y} = \mathfrak{x} * \mathfrak{x}\mathfrak{y}$ & $\mathfrak{z} = \mathfrak{x}\mathfrak{y} * (\mathfrak{x}\mathfrak{y})\mathfrak{z} \Longrightarrow \mathfrak{y}\mathfrak{z} = \mathfrak{x} * \mathfrak{x}(\mathfrak{y}\mathfrak{z})$.

Let now $\mathfrak{a}^n \supseteq \mathfrak{b}$ $(\forall n \in \mathbf{N})$ be satisfied. We suppose $\mathfrak{b} \cdot \mathfrak{a} \subset \mathfrak{b}$ that is $\mathfrak{b} * \mathfrak{b}\mathfrak{a} =: \mathfrak{x} \neq \langle 1 \rangle$. Then it holds $\mathfrak{x}^n * \mathfrak{x}^{n+1} = \mathfrak{x}$ and thereby $\bigcap\limits_1^\infty \mathfrak{x}^n \supseteq \mathfrak{x} * \bigcap\limits_1^\infty \mathfrak{x}^n$, implying $\bigcap\limits_1^\infty \mathfrak{x}^n = \mathfrak{x} * \bigcap\limits_1^\infty \mathfrak{x}^n$, that is $\mathfrak{x} \cdot \bigcap\limits_1^\infty \mathfrak{x}^n = \bigcap\limits_1^\infty \mathfrak{x}^n$. But this leads to $\mathfrak{b} \cdot \mathfrak{x} = \mathfrak{b}$, a contradiction. □

There are two aspects which should be taken into account:

As is immediately seen, the preceding proof has shown a bit more than explicitly emphasized. On the one hand we notice

13. 2. 4 Corollary. *If $\mathfrak{S}$ is a complementary monoid, i. e. if each $\langle a \rangle * \langle b \rangle$ is principal then the Mori property is equivalent with the archimedean property for principal ideals.*

On the other hand it should be remarked that the proof of 13.2.3 remains correct by assumption of the (noncommutative) duo-situation if we replace $\mathfrak{z}_n$ by a suitable $\mathfrak{z}'_n$ in the (only) line where $\mathfrak{z}_n$ is commuted.

13.3 Cancellative Monoids

Integral domains with condition (M) and (P), respectively, for v-ideals were investigated by Zafrullah in [432] and since v- and t-ideals don't depend on addition, the conditions of [432] are carried over to cancellative monoids with 0. But apart from this, further characterizations are possible, of course.

First of all we get the most important rule:

13. 3. 1 Lemma. *Let $\mathfrak{S}$ be a duo cancellative monoid. Then each of its principal ideals $\langle a\rangle$ is cancellable, as well in the v-ideal monoid as in the t-ideal monoid.*

PROOF. Suppose $\langle a\rangle \cdot \mathfrak{x} = \langle a\rangle \cdot \mathfrak{y}$. Then it follows

$$\begin{aligned} s \mid u\mathfrak{x}\, v \implies & as \mid \langle a\rangle u\, \mathfrak{x}\, v \\ \implies & as \mid \langle a\rangle u\, \mathfrak{y}\, v \\ \implies & \;\; s \mid u\, \mathfrak{y}\, v \end{aligned}$$

and thereby $\mathfrak{x} = \mathfrak{y}$.

Now we consider the *t-situation.* For each $x \in \mathfrak{x}$ with suitable $y_1, \ldots, y_n \in \mathfrak{y}$ we get

$$\langle a\rangle \cdot \langle x\rangle \;\subseteq\; \langle a\rangle \cdot \langle y_1, \ldots, y_n\rangle_v \,,$$

which leads to $x \in \langle y_1, \ldots, y_n\rangle_v \subseteq \mathfrak{y}$, and thereby to $\mathfrak{x} \subseteq \mathfrak{y}$.

This means $\mathfrak{x} = \mathfrak{y}$, by duality. □

In particular we are led to a theorem, resulting immediately from 7.2.1 and 7.2.6:

13. 3. 2 Proposition. *A commutative cancellative monoid $\mathfrak{S}$ is a Prüfer v-monoid iff its v-ideal monoid satisfies one of the subsequent equations:*

$$(\langle a\rangle + \langle b\rangle)(\langle a\rangle \cap \langle b\rangle) = \langle ab\rangle \tag{13.6}$$

$$\langle a\rangle * \langle b\rangle + \langle b\rangle * \langle a\rangle = \langle 1\rangle \tag{13.7}$$

$$\langle a\rangle \cap (\, \langle b\rangle + \langle c\rangle \,) = (\, \langle a\rangle \cap \langle b\rangle \,) + (\, \langle a\rangle \cap \langle c\rangle \,) \tag{13.8}$$

$$\& \quad (\, \langle a\rangle + \langle b\rangle \,)^2 = \langle a\rangle^2 + \langle b\rangle^2 \,. \tag{13.9}$$

Furthermore, according to 12.4.2, we get

13. 3. 3 Proposition. *A commutative cancellative monoid $\mathfrak{S}$ is a Mori v-monoid iff its semigroup of v-ideals satisfies:*

$$(\mathfrak{a} * \mathfrak{b}) * \mathfrak{b} = (\mathfrak{b} * \mathfrak{a}) * \mathfrak{a} \,. \tag{13.10}$$

PROOF. Recall: the proof of 12.4.2 does not depend on the algebraic property as far as (M) is considered, and in addition cancellative Mori v-monoids always satisfy $(\mathfrak{a} * \mathfrak{b}) * \mathfrak{b} = (\mathfrak{b} * \mathfrak{a}) * \mathfrak{a}$. □

Let $\mathfrak{S}$ be a cancellative Mori monoid w. r. t. an integral monoid $\mathfrak{A}$ of ideals of finite character. Then $\mathfrak{A}$ has the Noether property:

Suppose $\mathfrak{a} \supseteq \langle c \rangle$. According to 7.1.2 it follows $\mathfrak{a} \cdot \mathfrak{b} = \langle c \rangle = \mathfrak{a}' \cdot \mathfrak{b}$ where $\mathfrak{a}'$ is finitely generated which by cancellation leads to $\mathfrak{a} = \mathfrak{a}'$.

But this means that the Noether condition combined with the corresponding condition of 7.2.6 provides criteria for integral Mori semigroups of ideals and that integral Mori t-monoids, for instance, may be considered as cancellative monoids with *divisor theory.*

Remark: A cancellative monoid $\mathfrak{S}$ is called a monoid with divisor theory if the *holoid* $\mathfrak{H}$ of its principle ideals admits an extension $\sum$ respecting divisibility in $\mathfrak{H}$ (and thereby in $\mathfrak{S}$), having the UF-property and satisfying in addition the implication $\alpha \in \sum \Longrightarrow \alpha = \mathrm{GCD}\,(a_1, \ldots, a_n)$ $(\exists\, a_i \in S\,,\, 1 \leq i \leq n)$.

So, the question of an existing divisor theory, discussed for instance in Borewicz/ Šafarevič and actualized by Skula in [392], and recently by Halter-Koch and his co-workers Geroldinger and Lettl is equivalent to the Mori problem for t-ideals, compare the introduction. More precisely:

13. 3. 4 Proposition. *A commutative cancellative monoid $\mathfrak{S}$ is a Mori t-monoid (has a divisor theory) iff the semigroup of t-ideals satisfies:*

$$(\mathfrak{a} * \mathfrak{b}) * \mathfrak{b} = (\mathfrak{b} * \mathfrak{a}) * \mathfrak{a}\,. \tag{13.11}$$

PROOF. Recall: The Mori condition implies the Noether property. □

13.4 Cancellative Mori v-Monoids

Let $\mathfrak{S}$ be a semigroup of ideals of $\mathfrak{S}$ having the Mori property. Then $\mathfrak{S}$ is a Mori v-Monoid, as was shown above. This is interesting above all in the cancellative case, since it will turn out in the next proposition that here condition (M) for v-ideals is equivalent to

$$\left(\frac{s}{t}\right)^n \Big|_S\, c \in S \ \ (\forall n \in \mathbf{N}) \implies \frac{s}{t}\Big|_S\, 1 \Longrightarrow s \,\Big|\, t$$

or, respectively, to

$$\text{(v)} \qquad s^n \,\Big|\, c \cdot t^n \ \ (\forall\, n \in \mathbf{N}) \implies s \,\Big|\, t\,.$$

If (v) is satisfied, $\mathfrak{S}$ is called *completely integrally closed.* Obviously (v) implies the cancellation law.

In particular we may state that (v) depends on divisibility in $\mathfrak{S}$ and not on ideals whatever under consideration. More precisely condition (v) is satisfied whenever there exists a semigroup of ideals, satisfying condition (M).

From this point of view it surprises a bit that condition (v) isn't really present in the rich literature on Dedekind domains, for instance in the monograph of Larsen/ McCarthy, [268] . One reason might be that in these situations one is faced with even integrally closed "structures" . Thus, in Dedekind domains these ring theoretic aspect dominates the semigroup theoretical aspect (v) . In semigroup situations, condition (v) will turn out to be a central, most efficient tool of M-structures, whatever.

Recall 13.2.3. It follows:

13. 4. 1 Proposition. *Let $\mathfrak{S}$ be a commutative cancellative monoid, and let $\mathfrak{V}$ be its monoid of v-ideals. Then the following are pairwise equivalent.*

- (i) $\mathfrak{S}$ *is completely integrally closed.*
- (ii) $\mathfrak{V}$ *satisfies condition* (A) *and condition* (P).
- (iii) $\mathfrak{V}$ *satisfies condition* (A), *and every* $\langle a\rangle \cap \langle b\rangle$ *is a divisor.*
- (iv) $\mathfrak{S}$ *is a Mori v-monoid.*
- (v) $\mathfrak{V}$ *satisfies* (A), *and it holds* $(\,\langle a\rangle \cap \langle b\rangle\,)^2 = \langle a\rangle^2 \cap \langle b\rangle^2$.

PROOF. $(i) \Longrightarrow (ii)$. We put $\langle a\rangle * \langle b\rangle + \langle b\rangle * \langle a\rangle =: \mathfrak{x}$. Then by cancellation it follows for principal ideals $\langle s\rangle$ in a first step $\langle s\rangle \cdot \langle a\rangle \cap \langle s\rangle \cdot \langle b\rangle = \langle s\rangle \cdot (\,\langle a\rangle \cap \langle b\rangle\,)$ and thereby in a second step:

$$\begin{aligned} s \,|\, \mathfrak{x}\, t &\implies sa \,|\, (\,\langle a\rangle \cap \langle b\rangle\,)t \ \&\ sb \,|\, (\,\langle a\rangle \cap \langle b\rangle\,)t \\ &\implies \langle s\rangle(\,\langle a\rangle \cap \langle b\rangle\,) \supseteq (\,\langle a\rangle \cap \langle b\rangle\,)t \end{aligned}$$

$$
\begin{aligned}
&\Longrightarrow\ s^n\,(\,\langle a\rangle\cap\langle b\rangle\,)\supseteq(\,\langle a\rangle\cap\langle b\rangle\,)t^n\\
&\Longrightarrow\ s^n\,|\,c\cdot t^n \qquad (\forall\, c\in\langle a\rangle\cap\langle b\rangle,\forall\, n\in\mathbf{N})\\
&\Longrightarrow\ s\,|\,1\,t\\
&\rightsquigarrow\\
\mathfrak{x}\ &=\ \langle 1\rangle.
\end{aligned}
$$

Hence $\mathfrak{V}$ is normal. Furthermore $\mathfrak{S}$ is archimedean. To verify this, suppose $\mathfrak{a}^n\supseteq\langle b\rangle\ \ (\forall\, n\in\mathbf{N})$. Then it follows $\mathfrak{a}=\langle 1\rangle$, because

$$s\,|\,\mathfrak{a}\cdot t\Longrightarrow s^n\,|\,\mathfrak{a}^n\cdot t^n\Longrightarrow s^n\,|\,b\cdot t^n\Longrightarrow s\,|\,1\cdot t\Longrightarrow\mathfrak{a}=\langle 1\rangle\,.$$

$(ii)\Longrightarrow(iii)$ results from 13.2.2

$(iii)\Longrightarrow(iv)$. If $\langle b\rangle\cap\langle a\rangle$ is a divisor then it follows

$$
\begin{aligned}
\langle b\rangle*\langle a\rangle\supseteq\mathfrak{x}\ &\Longrightarrow\ \langle b\rangle\cdot(\,\langle b\rangle*\langle a\rangle\,)\supseteq\langle b\rangle\cdot\mathfrak{x}\\
&\Longrightarrow\ \langle b\rangle\cdot(\,\langle b\rangle*\langle a\rangle\,)\cdot\mathfrak{y}=\langle b\rangle\cdot\mathfrak{x}\,,
\end{aligned}
$$

whence by cancellation $(\,\langle b\rangle*\langle a\rangle\,)\cdot\mathfrak{y}=\mathfrak{x}$.

$(iv)\Longrightarrow(v)$. According to $\langle a\rangle*\langle b\rangle+\langle b\rangle*\langle a\rangle=\langle 1\rangle$ we get

$$(\,\langle a\rangle^2\cap\langle b\rangle^2\,)*\langle a\rangle\cdot\langle b\rangle=\langle a\rangle*\langle b\rangle+\langle b\rangle*\langle a\rangle=\langle 1\rangle\,,$$

consult the proof of 7.2.1.

$(v)\Longrightarrow(i)$. (v) provides $\langle a\rangle^2*\langle b\rangle^2=(\,\langle a\rangle*\langle b\rangle\,)^2$, which by (A) leads to

$$
\begin{aligned}
s^n\,|\,c\cdot t^n\ \ (\forall\, n\in\mathbf{N})\ &\Longrightarrow\ \langle c\rangle*(\,\langle t\rangle^{2^m}*\langle s\rangle^{2^m}\,)=\langle 1\rangle\ (\forall\, m\in\mathbf{N})\\
&\Longrightarrow\ \langle c\rangle*(\,\langle t\rangle*\langle s\rangle\,)^{2^m}=\langle 1\rangle\quad(\forall\, m\in\mathbf{N})\\
&\Longrightarrow\ \langle t\rangle*\langle s\rangle=\langle 1\rangle\\
&\Longrightarrow\ s\,|\,t\,.
\end{aligned}
$$

This completes the proof. □

Opposite to the algebraic case, where the Prüfer property combined with the archimedean property by no means guarantees the Mori property, in the v-ideal case we get: A commutative cancellative monoid is a Mori v-ideal monoid if and only if it satisfies the properties (A) and (P). However, it has to be taken into account, of course, that the Mori v-quality is significantly weaker than the Mori t-quality is.

The conditions of 13.4.1 may be weakened. As is easily seen, each divisor of a principal v-ideal is cancellable, and because of this each divisor of a principal v-ideal is a divisor in general. Consequently a commutative cancellative monoid is a Mori v-monoid if any $\mathfrak{a}$ is divisor of at least one principal ideal. More precisely:

13. 4. 2 Corollary. *Let $\mathfrak{S}$ be a commutative cancellative monoid and $\mathfrak{V}$ its monoid of v-ideals. Then the following are pairwise equivalent:*

(*i*) *$\mathfrak{S}$ is a Mori v-monoid.*

(*ii*) *$\mathfrak{V}$ satisfies* (A), *and each $\langle a\rangle \cap \langle b\rangle$ of $\mathfrak{V}$ is divisor of some $\langle c\rangle$.*

(*iii*) *$\mathfrak{V}$ satisfies* (A), *and each $\langle a\,,\, b\rangle = \langle a\rangle + \langle b\rangle$ is divisor of some $\langle c\rangle$.*

(*iv*) *$\mathfrak{A}$ satisfies* (A), *and $(\,\langle a\rangle + \langle b\rangle\,)\cdot(\,\langle a\rangle \cap \langle b\rangle\,) = \langle ab\rangle$ for all elements $a\,,\, b\,,$.*

(*v*) *$\mathfrak{A}$ satisfies* (A), *and it holds $\mathfrak{a}\cdot(\mathfrak{b}\cap\mathfrak{c}) = (\mathfrak{a}\cdot\mathfrak{b})\cap(\mathfrak{a}\cdot\mathfrak{c})$.*

(*vi*) *Every v-ideal $\mathfrak{a}$ divides at least one principal ideal $\langle c\rangle$.*

Next we turn to the *v-Gruppensatz* of van der Waerden

Let $\mathfrak{S}$ be a commutative cancellative monoid, $\mathfrak{G}$ its quotient group, and A a subset of G. Then A^{-1} is defined by $\{x \in G \mid Ax \subseteq S\}$, and $\mathfrak{a} \subseteq G$ is called a *v-module* or equivalently a *fractional v-ideal* if $(\mathfrak{a}^{-1})^{-1} = \mathfrak{a}$.

The module definition extends the v-ideal definition, observe

$$\alpha \in (A^{-1})^{-1} \text{ iff } s\Big|_S At \Longrightarrow A\cdot\frac{t}{s} \subseteq S \Longrightarrow \alpha\cdot\frac{t}{s} \in S \Longrightarrow s\Big|_S \alpha\cdot t\,.$$

In particular, by definition v-modules behave like v-ideals, and the monoid of v-ideals is embedded in the monoid of v-modules. Thus we are led to van der Waerden.

13. 4. 3 The v-Gruppensatz. *Let $\mathfrak{S}$ be a commutative cancellative monoid with quotient group $\mathfrak{G}$ and let $\mathfrak{M}$ be the corresponding monoid of v-modules of $\mathfrak{G}$. Then the following are pairwise equivalent:*

(*i*) *$\mathfrak{S}$ is completely integrally closed.*

(*ii*) *$\mathfrak{M}$ is a group with identity S.*

(*iii*) *$\mathfrak{M}$ satisfies $(\mathfrak{a}\cdot\mathfrak{b})^{-1} = \mathfrak{a}^{-1}\cdot\mathfrak{b}^{-1}$.*

(*iv*) *$\mathfrak{S}$ is a Mori v-monoid.*

PROOF. $(i) \Longrightarrow (ii)$. If (i) is satisfied then each $\alpha \in G$ with $\alpha \in (\mathfrak{a}\cdot\mathfrak{a}^{-1})^{-1}$ satisfies $\alpha\cdot\mathfrak{a}\mathfrak{a}^{-1} \subseteq S$ and thereby $\alpha\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$. But this provides furthermore $\alpha^n\cdot\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$ $(\forall n \in \mathbf{N})$, leading to $\alpha^n\cdot\mathfrak{a}\mathfrak{a}^{-1} \subseteq S$. Choose now some $c \in \mathfrak{a}\mathfrak{a}^{-1}$. Then all elements $\alpha^n{\cdot}c$ $(n \in \mathbf{N})$ belong to S. Hence we get $\alpha \in S$ and thereby $(\mathfrak{a}\mathfrak{a}^{-1})^{-1} \subseteq S$. This implies $\mathfrak{a}\mathfrak{a}^{-1} \supseteq S \leadsto \mathfrak{a}\mathfrak{a}^{-1} = S$.

$(ii) \Longrightarrow (iii)$ follows from $\mathfrak{a}\cdot\mathfrak{a}^{-1} \subseteq S = S^{-1} \subseteq \mathfrak{a}^{-1}\cdot\mathfrak{a}$, by $\left(\mathfrak{a}^{-1}\right)^{-1} = \mathfrak{a}$.

$(iii) \Longrightarrow (iv)$. If $\mathfrak{G}$ is a group and if $\mathfrak{a} \supseteq \mathfrak{b}$ then $\mathfrak{a}^{-1}\mathfrak{b}$ is integral and $\mathfrak{a}\cdot(\mathfrak{a}^{-1}\mathfrak{b}) = \mathfrak{b}$.

$(iv) \Longrightarrow (i)$. By the cancellative law we get $\mathfrak{a}\cdot\bigcap\mathfrak{b}_i = \bigcap\mathfrak{a}\mathfrak{b}_i$, which implies the archimedean property. Hence we may continue along the proof of 13.4.1 (v). $\square$

13. 4. 4 Corollary. *Let $\mathfrak{S}$ be a commutative cancellative monoid with quotient group $\mathfrak{G}$ and let $\mathfrak{M}$ be the corresponding monoid of v-modules of $\mathfrak{G}$. Then $\mathfrak{S}$ is a Mori v-monoid iff $\mathfrak{M}$ satisfies:*

$$\text{(V)} \qquad (\mathfrak{a}\cdot\mathfrak{b})^{-1} = \mathfrak{a}^{-1}\cdot\mathfrak{b}^{-1}.$$

For d-ideals the cancellation law

$$\mathfrak{a} \neq \mathfrak{o} \;\&\; \mathfrak{a}\cdot\mathfrak{x} = \mathfrak{a}\cdot\mathfrak{y} \Longrightarrow \mathfrak{x} = \mathfrak{y}$$

does not imply the Mori property. This is quite different in the case of v-ideals.

13. 4. 5 Proposition. *A commutative cancellative monoid is a Mori v-monoid iff its v-ideals satisfy the cancellation law.*

PROOF. First we get $\langle a\rangle * \langle b\rangle + \langle b\rangle * \langle a\rangle = \langle 1\rangle$, since

$$\begin{aligned}
& s \,|\, (\,\langle a\rangle * \langle b\rangle + \langle b\rangle * \langle a\rangle\,)\cdot t \\
\Longrightarrow\;& a\cdot s \supseteq \langle a\rangle(\,\langle a\rangle * \langle b\rangle\,)\cdot t \\
\Longrightarrow\;& a\cdot s \supseteq (\,\langle a\rangle \cap \langle b\rangle\,)\cdot t \\
\&\;\;& b\cdot s \supseteq (\,\langle a\rangle \cap \langle b\rangle\,)\cdot t \\
\Longrightarrow\;& (\,\langle a\rangle \cap \langle b\rangle\,)\cdot s \supseteq (\,\langle a\rangle \cap \langle b\rangle\,)\cdot t \\
\Longrightarrow\;& (\,\langle a\rangle \cap \langle b\rangle\,)\cdot \langle s,t\rangle = (\,\langle a\rangle \cap \langle b\rangle\,)\cdot \langle s\rangle \\
\Longrightarrow\;& s \,|\, 1\cdot t
\end{aligned}$$

leads to $\langle a\rangle * \langle b\rangle + \langle b\rangle * \langle a\rangle = \langle 1\rangle$.

Consequently, each $\langle a\rangle + \langle b\rangle$ divides some principal ideal, for instance $\langle b\rangle$, and hence – according to $(iii) \Longrightarrow (iv)$ in the proof of 13.4.1 – $\langle a\rangle + \langle b\rangle$ is even a cancellable divisor. The same is true for $\langle a\rangle * \langle b\rangle$. This means in particular

$$(\,\langle s\rangle + \langle t\rangle\,)\cdot(\,\langle s\rangle * \langle t\rangle) \;=\; \langle t\rangle\,.$$

Suppose now $s^n \,|\, a\cdot t^n \;\; (\forall n \in \mathbf{N})$. Then, by cancellation property of $\langle s\rangle + \langle t\rangle$, according to (5.7) and (5.6), it results successively

$$(\,\langle t\rangle * \langle s\rangle\,)^n \,\Big|\, \langle a\rangle \;\; (n \in \mathbf{N})\,.$$

But this leads to

$$\begin{aligned}(\,\langle t\rangle * \langle s\rangle\,) * \textstyle\bigcap_{n\in N}(\,\langle t\rangle * \langle s\rangle\,)^n \;&=\; \textstyle\bigcap_{n\in N}(\,\langle t\rangle * \langle s\rangle\,)^{n-1}\\ &=\; \textstyle\bigcap_{n\in N}(\,\langle t\rangle * \langle s\rangle\,)^{n}\;\;,\end{aligned}$$

and hereby to

$$\begin{aligned}\textstyle\bigcap_{n\in N}(\,\langle t\rangle * \langle s\rangle\,)^n \;&=\; (\,\langle t\rangle * \langle s\rangle\,)\cdot\textstyle\bigcap_{n\in N}(\,\langle t\rangle * \langle s\rangle\,)^n\\ &\leadsto\\ \langle t\rangle * \langle s\rangle \;&=\; \langle 1\rangle \leadsto s\,|\,t\,.\end{aligned}$$

Hence $\mathfrak{S}$ is completely integrally closed. □

The proof, presented here, is along the lines of this paper, and will serve as orientation for the proof of 13.5.2 (ii) . But an alternative proof is possible according to ideas of BUTTS, [148], *via* the monoid of v-modules, pointing out the relation between the notions *integrally closed* and *completely integrally closed.*

If an integral domain is completely integrally closed in its quotient field $\mathfrak{K}$ then I contains all quotients α , whose corresponding modules $\mathfrak{a} = (1, \alpha^1, \alpha^2, \ldots, \alpha^n, \ldots)$ can be multiplied into I by a suitable $c \in I$, whereas an integral domain is integrally closed if it contains all quotients whose corresponding modules $(1, \alpha^1, \alpha^2, \ldots, \alpha^n, \ldots)$ are finitely generated and hence *a fortiori* can be multiplied into I by some suitable $c \in I$.

Let now $c\mathfrak{a} =: \mathfrak{b} \subseteq \mathfrak{I}$ be an ideal. Then, according to the cancellation law for non vanishing ideals it follows from $\mathfrak{a}^2 = \mathfrak{a}$ first that $\mathfrak{b}\cdot\mathfrak{b} = \mathfrak{b}\cdot\langle c\rangle$

is valid. Hence, if $\mathfrak{b}$ is a cancellable d- or t- or v-ideal, it follows further $\langle c\rangle = \mathfrak{b} = \mathfrak{a}\langle c\rangle$.

Thus *integrally closed* implies *completely integrally closed.*

13. 4. 6 Corollary. *A commutative cancellative monoid is a Mori v-monoid iff its v-ideals satisfy*

$$\mathfrak{a}\cdot\mathfrak{x} = \mathfrak{a}\cdot\mathfrak{y} \implies (\mathfrak{a}\cap\mathfrak{b})\cdot\mathfrak{x} = (\mathfrak{a}\cap\mathfrak{b})\cdot\mathfrak{y}\,.$$

PROOF. According to 13.3.1 each principal ideal is cancellable. Hence we get $\mathfrak{a}\cdot\mathfrak{x} = \mathfrak{a}\cdot\mathfrak{y} \Longrightarrow \langle a\rangle\mathfrak{x} = \langle\mathfrak{a}\rangle\mathfrak{y} \Longrightarrow \mathfrak{x} = \mathfrak{y}$. □

13.5 Krull Monoids

In [25] it is shown that a commutative cancellative monoid $\mathfrak{S}$ admits a *divisor theory* if and only if the semigroup of v-ideals is a divisor theory. And this is the case, as shown above, if and only if the monoid of v-ideals has the Prüfer and the Noether property, meaning – see above – that $\mathfrak{S}$ be a Mori t-monoid.

On the other hand it is due to Halter-Koch that cancellative monoids with divisor theory may be considered as *divisibility monoids* of some Krull domain, compare [178]. Consequently Mori t-monoids may alternatively be called Krull monoids. This will be done in the following, initiated by a verbal remark of Franz Halter-Koch to the author.

Theory of Krull monoids fills a lecture note by itself. So we refer the reader to the series of papers cited within our historical remarks.

In particular, we will omit divisor class group theory or the interesting results on finitely generated Krull monoids, based on *convex geometry*, c. f. [272].

Since t-ideals are of finite character chapter 7 *a fortiori* applies to Krull monoids. But since Krull monoids are cancellative monoids we may expect characterizations closer to classical characterizations of Dedekind domains.

First of all, because of 7.2.6 we get by t-cancellation

13. 5. 1 Corollary. *A commutative cancellative monoid $\mathfrak{S}$ is a Prüfer t-monoid iff the monoid of t-ideals of $\mathfrak{S}$ satisfies at least one of the conditions below 7.2.6*

Furthermore it holds

13. 5. 2 Proposition. *Let $\mathfrak{S}$ be a commutative cancellative monoid and let $\mathfrak{A}$ be the monoid of its t-ideals $\langle A\rangle$. Then the following are pairwise equivalent:*

(*i*) *The finitely generated t-ideals of $\mathfrak{S}$ are cancellable, and $\mathfrak{A}$ is lattice distributive.*

(*ii*) $\langle a_1,\ldots,a_n\rangle * \langle a_1,\ldots,a_n\rangle\cdot\langle b\rangle = \langle b\rangle$, *and all $\langle a\rangle\cap\langle b\rangle$ are finitely generated.*

(*iii*) *$\mathfrak{S}$ is a Prüfer t-monoid.*

PROOF. Suppose (i). Then finitely generated ideals $\mathfrak{a},\mathfrak{b}$ satisfy

$$(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}+\mathfrak{b})^2 = (\mathfrak{a}+\mathfrak{b})(\mathfrak{a}^2+\mathfrak{b}^2) \rightsquigarrow (\mathfrak{a}+\mathfrak{b})^2 = \mathfrak{a}^2+\mathfrak{b}^2$$

and hereby the Prüfer condition, according to 7.2.6

Let now (ii) be satisfied. Since $\langle a\rangle\cap\langle b\rangle$ is finitely generated, according to 7.1.2 there exists a finitely generated $\mathfrak{x}$ satisfying $\langle a\rangle\cdot\mathfrak{x} = \langle a\rangle\cdot(\,\langle a\rangle*\langle b\rangle\,)$. Hence $\langle a\rangle*\langle b\rangle$ is equal to $\mathfrak{x}$ and thereby finitely generated. Start now as in the proof of 13.4.5. Then, according to condition (ii) we get

$$(\,\langle a\rangle\cap\langle b\rangle)\cdot\langle t\rangle * (\,\langle a\rangle\cap\langle b\rangle)\cdot\langle s\rangle = \langle t\rangle*\langle s\rangle = \langle 1\rangle\,,$$

implying

$$\langle a\rangle*\langle b\rangle + \langle a\rangle*\langle b\rangle = \langle 1\rangle\,.$$

On the other hand 7.1.3 implies $(iii) \Longrightarrow (i)$ & (ii), by cancellation.

This completes the proof. $\square$

13. 5. 3 Corollary. *Let $\mathfrak{S}$ be a commutative cancellative monoid. Then $\mathfrak{S}$ is a Krull monoid iff any t-ideal is finitely generated and in addition one of the conditions below 7.2.6 is satisfied by the monoid of t-ideals.*

Recall: If $\mathfrak{S}$ is a Krull monoid then $\mathfrak{S}$ is also a Mori v-monoid. Hence Krull monoids are completely integrally closed. This results also by the proof of $(v) \Longrightarrow (i)$ below 13.4.1 – as we shall see. But, under which conditions is a completely integrally closed commutative cancellative monoid, i. e. a Mori v-monoid, even a Mori t-monoid, *alias* a Krull monoid?

13. 5. 4 Proposition. *A commutative cancellative monoid $\mathfrak{S}$ is a Krull monoid iff it satisfies simultaneously for at least one system $\mathfrak{A}$ of ideals of finite character with cancellable principal ideals:*

(v) $\mathfrak{S}$ *is completely integrally closed.*

(w) *Each maximal $\mathfrak{m}$ is of type $\langle a \rangle * \langle b \rangle$.*

PROOF. NECESSITY: Suppose the multiplication property for $\mathfrak{A}$. Then it follows the v-multiplication property, as was pointed out above. Recall at this point, that (v) was developed by applying the cancellation law for principal ideals, the Prüfer property and the property $\mathfrak{a} \cdot \mathfrak{u} = \mathfrak{a} \Longrightarrow (\mathfrak{a} \cap \mathfrak{b}) \cdot \mathfrak{u} = \mathfrak{a} \cap \mathfrak{b}$. So, this part remains valid in general also for arbitrary multiplication monoids with cancellable principal ideals. Consequently, $\mathfrak{S}$ satisfies condition (v) .

It remains to verify condition (w) . So, suppose that $\mathfrak{m}$ is maximal and $\mathfrak{m} \supseteq b$ is satisfied. Then it follows $\mathfrak{m} \cdot (\mathfrak{m} * b) = b$. But because of the cancellation property of b it cannot hold $b = \mathfrak{m} * b$. Hence there exists some a with $a \in \mathfrak{m} * b$ but $a \notin b$. This leads further to $a \cdot \mathfrak{m} \subseteq b$ and consequently to $a * b \supseteq \mathfrak{m}$. So it holds either $a * b = 1$ and thereby $\langle a \rangle \subseteq b$, a contradiction, or, on the grounds of maximality, $\mathfrak{m} = a * b$, q, e. d.

SUFFICIENCY: First of all we show that maximal t-ideals $\mathfrak{m}$ are divisors and thereby *a fortiori* cancellable. We recall that by assumption maximal t-ideals are even v-ideals and that

$$\langle A \rangle \cdot \langle B \rangle = \langle C \rangle \implies \langle A \rangle_v \cdot \langle B \rangle_v = \langle C \rangle_v$$

is satisfied. According to (v), in the monoid of v-ideals each $c \in \mathfrak{m}$ satisfies

$$\mathfrak{m} \cdot (\mathfrak{m} * c) = c \,.$$

Suppose next

$$\mathfrak{m} \cdot (\mathfrak{m} * c) \neq c \,.$$

Then it holds

$$1 \neq c * \mathfrak{m} \cdot (\mathfrak{m} * c) \supseteq \mathfrak{m} \rightsquigarrow c * \mathfrak{m} \cdot (\mathfrak{m} * c) = \mathfrak{m}$$

and thereby

$$\mathfrak{m} \cdot (\mathfrak{m} * c) = \mathfrak{m} \cdot c \,,$$

since in the semigroup of v-ideals this would lead to

$$\mathfrak{m} \cdot c = c \;\rightsquigarrow\; \mathfrak{m} = \langle 1 \rangle\,,$$

a contradiction w.r.t. $b \nmid a$. So, we get $\mathfrak{m} \cdot (\mathfrak{m} * c) = c$ also in $\mathfrak{A}$ Hence each maximal $\mathfrak{m}$ of $\mathfrak{A}$ is a cancellable divisor.

We now prove that $\mathfrak{A}$ satisfies condition (A) for maximal elements $\mathfrak{m}$. First a hint: If $b \cdot \mathfrak{z} \neq b$ then any $\mathfrak{m}$, maximal in the set of all $\mathfrak{y} \supseteq \mathfrak{z}$ with $b\mathfrak{y} \neq b$, is maximal even in $\mathfrak{A}$, because

$$\mathfrak{u} \supset \mathfrak{m} \Longrightarrow b \cdot \mathfrak{u} = b = b \cdot 1 \;\rightsquigarrow\; \mathfrak{u} \supset \mathfrak{m} \Longrightarrow \mathfrak{u} = 1\,.$$

Suppose now $c \cdot \mathfrak{p} \neq c$, in spite of $\mathfrak{p}^n \supseteq c$ $(\forall n \in \mathbf{N})$. Then for each maximal $\mathfrak{m}$ in the sense of our hint we get $\mathfrak{m}^n \supseteq c$ $(\forall n \in \mathbf{N})$ on the one hand and $c \cdot \mathfrak{m} \neq c$ on the other hand. But each maximal $\mathfrak{m}$ is a divisor of type $a * b$ as was shown above. Consequently $\mathfrak{m}^n \supseteq c$ $(\forall n \in \mathbf{N})$ would imply next $b \supseteq a \cdot \mathfrak{m}$ and thereby

$$\begin{aligned} \mathfrak{m}^n \supseteq c \;\; (\forall n \in \mathbf{N}) \;&\rightsquigarrow\; b^n \supseteq \mathfrak{m}^n \cdot a^n && (\forall n \in \mathbf{N}) \\ &\rightsquigarrow\; b^n \,\big|\, c \cdot a^n && (\forall n \in \mathbf{N}) \\ &\rightsquigarrow\; b \,|\, a\,, \end{aligned}$$

a contradiction! Hence $\mathfrak{A}$ satisfies:

(A) $$\mathfrak{p}^n \big| \langle b \rangle \;\; (\forall n \in \mathbf{N}) \;\Longrightarrow\; \mathfrak{p}\langle b \rangle = \langle b \rangle\,.$$

Finally assume:

$$\mathfrak{a} \supseteq b \text{ and } b \supset b \cdot \mathfrak{m} \supseteq \mathfrak{a} \cdot (\,\mathfrak{a} * b\,) \text{ with maximal } \mathfrak{m} \supseteq b * \mathfrak{a}(\,\mathfrak{a} * b\,)\,.$$

Then it results:

$$\mathfrak{m} \supseteq \langle b \rangle * \mathfrak{a} \cdot (\,\mathfrak{a} * b\,) \;\supseteq\; \mathfrak{a} * \mathfrak{a} \cdot (\,\mathfrak{a} * b\,) = \mathfrak{a} * b =: \mathfrak{x}\,.$$

Hence for $\mathfrak{x}$, defined this way, it follows

$$\begin{aligned} \mathfrak{a} \cdot \mathfrak{m} \cdot (\mathfrak{m} * \mathfrak{x}) = \mathfrak{a} \cdot \mathfrak{x} \subseteq b \cdot \mathfrak{m} \;&\rightsquigarrow\; \mathfrak{a} \cdot (\mathfrak{m} * \mathfrak{x}) \subseteq b \\ &\rightsquigarrow\; \mathfrak{x} = \mathfrak{a} * b \supseteq \mathfrak{m} * \mathfrak{x} \\ &\rightsquigarrow\; \mathfrak{x} = \mathfrak{m} * \mathfrak{x} \\ &\rightsquigarrow\; \mathfrak{m} \cdot \mathfrak{x} = \mathfrak{m} \cdot (\mathfrak{m} * \mathfrak{x}) = \mathfrak{x}\,. \end{aligned}$$

This completes the proof, since the final line implies $b \cdot \mathfrak{m} = b \cdot 1$ by condition (A) and thereby $\mathfrak{m} = 1$, a contradiction! $\square$

By the preceding theorem the archimedean property is a most natural substitute of condition (v). For, (A) combined with (jn) is equivalent to (v) combined with (jn), but (A) makes sense in arbitrary situations whereas condition (v) - as shown above - makes sense only in integral structures. Furthermore it seems to be interesting that cancellation property of the monoid of v-ideals certifies the Krull condition up to $\mathfrak{m} = \langle a \rangle * \langle b \rangle$ for maximal t-ideals $\mathfrak{m}$, a condition, which has to be introduced in which form ever.

Observe furthermore, that the proof of 13.5.4 offers a proof line for

13. 5. 5 Proposition. *A commutative cancellative monoid $\mathfrak{S}$ is a Krull monoid iff it satisfies simultaneously for at least one system $\mathfrak{A}$ of ideals of finite character with cancellable principal ideals:*

(B) $\quad \mathfrak{a} \supseteq \mathfrak{a}^n * \mathfrak{b} \ \ (\forall\, n \in \mathbf{N}) \ \Rightarrow \ \mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a}$

(c) *Each maximal $\mathfrak{m}$ is cancellable.*

SINCE: $\mathfrak{m} * \langle c \rangle = \langle c \rangle$ implies $\mathfrak{m} \cdot \langle c \rangle = \langle 1 \rangle \cdot \langle c \rangle$ that is $\mathfrak{m} = \langle 1 \rangle$ and since by analogy we may infer $\mathfrak{m} = \langle 1 \rangle$ from $\mathfrak{m} \supseteq \mathfrak{m} * \mathfrak{x} \Longrightarrow \mathfrak{m} \supseteq \mathfrak{m} * \langle x \rangle \ \ (\forall x \in \mathfrak{x})$ – without proving condition (A)! $\square$

As a further result it follows from 13.5.4

13. 5. 6 Proposition. *Let $\mathfrak{S}$ be a commutative cancellative monoid and $\mathfrak{A}$ be some monoid of ideals of $\mathfrak{S}$ of finite character. Then $\mathfrak{A}$ is a Mori structure iff it satisfies:*

(ve) $\quad \langle s_1, \ldots, s_m \rangle^n \,\Big|\, \langle c \rangle \cdot \langle t \rangle^n \ \ (\forall\, n \in \mathbf{N}) \Longrightarrow \langle s_1, \ldots, s_m \rangle \mid \langle t \rangle\,.$

(w) *Each maximal $\mathfrak{m}$ is a v-ideal.*

PROOF. As is easily seen, it suffices to show that principal ideals $\mathfrak{a}$ satisfy

$$\langle a \rangle \cdot \mathfrak{x} = \langle a \rangle \cdot \mathfrak{y} \ \Longrightarrow \ \mathfrak{x} = \mathfrak{y}\,.$$

To this end we start from the premise and choose some $x \in \mathfrak{x}$. It follows for suitable $y_i \ \ (1 \leq i \leq m)$

$$\langle a \rangle \cdot \langle x, y_1, \ldots, y_m \rangle \ = \ \langle a \rangle \cdot \langle y_1, \ldots, y_m \rangle$$

and thereby $\langle a\rangle \cdot \langle x, y_1, \ldots, y_m\rangle^n \ = \ \langle a\rangle \cdot \langle y_1, \ldots, y_m\rangle^n \,,$

which implies $\qquad \langle y_1, \ldots, y_m\rangle^n \ \Big| \ \langle a\rangle \cdot \langle x, y_1, \ldots, y_m\rangle^n \,,$

that is by (ve)

$$\begin{array}{rcl} \langle y_1, \ldots, y_m\rangle & \supseteq & \langle x, y_1, \ldots, y_m\rangle \,, \\ & \rightsquigarrow & \\ \langle y_1, \ldots, y_m\rangle & \supseteq & \langle x\rangle \,. \end{array}$$

Thus it results $\mathfrak{y} \supseteq \mathfrak{x}$, whence by duality it follows $\mathfrak{y} = \mathfrak{x}$. $\square$

The next proposition resembles a classical result due to KRULL, compare [418].

13. 5. 7 Proposition. *Let $\mathfrak{S}$ be a commutative cancellative monoid and let $\mathfrak{A}$ an arbitrary monoid of ideals of finite character. Then $\mathfrak{A}$ is a Mori AML iff it satisfies simultaneously:*

(n) *Each $\mathfrak{a}$ is finitely generated*

(g) $\langle a_1, \ldots, a_n\rangle * \langle a_1, \ldots, a_n\rangle \cdot \langle b\rangle = \langle b\rangle$

(m) *Each prime ideal $\mathfrak{p}$ is maximal.*

PROOF. According to 13.5.7 and 13.5.4 the conditions above are necessary.

So, it remains to verify sufficiency.

First of all (n) certifies that each $\mathfrak{a}$ contains an irredundant t-prime product, since not prime means $\mathfrak{a} \supseteq \mathfrak{b}\mathfrak{c} \ (\exists\, \mathfrak{b}, \mathfrak{c} \,:\, \mathfrak{a} + \mathfrak{b} \supset \mathfrak{a} \ \&\ \mathfrak{a} + \mathfrak{c} \supset \mathfrak{a})$.

Let now $\mathfrak{p}$ be prime and $0 \neq b \in \mathfrak{p}$ and let moreover $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n$ be a shortest prime ideal product, contained in $\langle b\rangle$. Then $\mathfrak{p}$ is equal to one of these $\mathfrak{p}_i \ (1 \leq i \leq n)$, say equal to $\mathfrak{p}_1$, and because of irredundancy there exists at least one element a in $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_n$ which is not divided by b. But this means:

$$\mathfrak{p} \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_n \subseteq \langle b\rangle \ \rightsquigarrow \ \mathfrak{p}\langle a\rangle \subseteq \langle b\rangle \,.$$

Thus we get $\qquad \mathfrak{p} * (\, \langle a\rangle * \langle b\rangle \,) \ = \ \langle 1\rangle \,,$

which, according to $b \nmid a$ and the maximality of $\mathfrak{p}$, leads to

$$\mathfrak{p} \ = \ \langle a\rangle * \langle b\rangle \,.$$

Continuing from here we get further that together with $\mathfrak{p} = \langle a\rangle * \langle b\rangle$ also $\mathfrak{p} \supseteq \langle b\rangle$ and $\mathfrak{p} * \langle b\rangle \supseteq \langle a\rangle$ are satisfied, and that by

$$\begin{aligned}\langle b\rangle * \mathfrak{p}(\,\mathfrak{p} * \langle b\rangle\,) &\supseteq (\,\mathfrak{p} * \langle b\rangle\,) * \mathfrak{p}(\,\mathfrak{p} * \langle b\rangle\,)\\ &\supseteq \mathfrak{p}\end{aligned}$$

that is $$\mathfrak{p}(\,\mathfrak{p} * \langle b\rangle\,) = \langle b\rangle \quad \vee \quad \mathfrak{p}(\,\mathfrak{p} * \langle b\rangle\,) = \langle b\rangle\mathfrak{p}$$

and thereby $$\mathfrak{p}(\,\mathfrak{p} * \langle b\rangle\,) = \langle b\rangle$$

is satisfied, since otherwise by $\mathfrak{p} * \langle b\rangle \supseteq \langle a\rangle$ and according to (g) we would get

$$\begin{aligned}\mathfrak{p} = \langle a\rangle * \langle b\rangle &= \mathfrak{p}\cdot\langle a\rangle * \mathfrak{p}\cdot\langle b\rangle\\ &= \mathfrak{p}\cdot\langle a\rangle * \mathfrak{p}(\,\mathfrak{p} * \langle b\rangle\,)\\ &\supseteq \langle a\rangle * (\,\mathfrak{p} * \langle b\rangle\,)\\ &= \langle 1\rangle\,,\end{aligned}$$

a contradiction! Hence $\mathfrak{p}$ is even a divisor and resulting from this $\mathfrak{S}$ is a Krull monoid. □

If $\mathfrak{I}$ is an integral domain then (g), with respect to d-ideals, is equivalent to integral closedness, which was shown above and which follows on the other hand from Prüfer's paper [352], compare also Krull [245].

This demonstrates the analogy with a result due to Krull and presented by van der Waerden in [418] , telling:

Dedekindsch

$$\Longleftrightarrow$$

noethersch + ganz-abgeschlossen + prim ist maximal.

In a former chapter we considered archimedean Prüfer AMLs. The most natural question arises which the difference is between Mori t-cancellative-monoids, *alias* Krull monoids, and AP-t-cancellative-monoids.

A Remark: Let $\mathfrak{H} := (\,\mathfrak{H}, + \cdot\,)$ be a cancellative commutative semi-ring with identity 1. Then $\mathfrak{H}$ admits an embedding into a quotient-extension $\mathfrak{Q}$, and the notion of an H-ideal, in the sense of a semi-ring ideal, is carried over to $\mathfrak{Q}$ by defining $\{\sum_1^n h_i\,\cdot a_i\;\;(h_i\,\in H\,,\,a_i\,\in A)\}$ as *module* $\langle A\rangle$. This way in $\mathfrak{Q}$ by the H-module a new type of ideal is exhibited. Among these modules those are of special interest,

> *"die sich durch Multiplikation mit einem $c \in H$ in ein Ideal verwandeln lassen"*

(DEDEKIND, recall the historical part!). These modules are called *fractional ideals*, whereas the semi-ring ideals are alternatively also called *integral* ideals. Like the integral ideals the fractional ideals are symbolized by Gothic letters.

By definition each semi-ring ideal $\mathfrak{a}$ is a fractional ideal, as well. Furthermore the fractional ideals in any case form an extension monoid of the monoid of integral ideals.

Let now $\mathfrak{a}$ be an H-module of $\mathfrak{Q}$. Then the set of all x, satisfying $\mathfrak{a}\cdot x \subseteq H$ forms an H-module $\mathfrak{a}^{-1}$, and it may hold $\mathfrak{a}\cdot\mathfrak{a}^{-1} = H$, consider for instance a principal ideal. In this case $\mathfrak{a}$ is called *invertible.* As is easily seen invertibility implies the existence of some $c \in H$ with $\mathfrak{a}\mathfrak{c} \subseteq \mathfrak{H}$. Hence the Gruppensatz is already satisfied if each integral ideal $\mathfrak{a}$ is invertible.

Thus in semi-rings divisibility can be studied *via* fractional ideals. This is, of course, not in any case possible, since ideals in general are not defined *internally.* So, f. i. the H-ideal, generated by A and the H-module, generated by A may be different.

As one example among others for applying quotients we give a final result, thereby doing a further step towards KRULL, compare again [112] :

13. 5. 8 Proposition. *Let $\mathfrak{H}$ be a commutative cancellative semi-ring with identity* 1, *let $\mathfrak{Q}$ be its quotient extension, and $\mathfrak{M}$ the monoid of modules of $\mathfrak{Q}$. Then the following are pairwise equivalent :*

- (i) *$\mathfrak{H}$ is a multiplication semi-ring.*
- (ii) *$\mathfrak{M}$ is a group with identity H.*
- (iii) (n) *Each $\mathfrak{a}$ is finitely generated,*
  - (g) $\langle a_1, \dots, a_n\rangle * \langle a_1, \dots, a_n\rangle \cdot \langle b\rangle = \langle b\rangle$
  - (x) *If $\mathfrak{p}$ is maximal integral then $\mathfrak{p}^{-1}$ is proper fractional.*

PROOF. We get successively :

(i) $\Longrightarrow$ (ii). If $\mathfrak{A}$ is a Mori structure and $\mathfrak{a}$ a fractional ideal, then there exists some $c \in S$ satisfying $\mathfrak{a}\cdot\langle c\rangle \subseteq H$. Hence for some suitable d we get the inclusion $\mathfrak{a}\cdot\langle c\rangle \supseteq \langle d\rangle$ and thereby the equation $\mathfrak{a}\cdot\langle c\rangle\cdot\mathfrak{x}\cdot\langle d\rangle^{-1} = \langle 1\rangle \;\; (\exists\ \mathfrak{x})$. But this implies $\mathfrak{a}\cdot\mathfrak{a}^{-1} \supseteq \langle 1\rangle$ and thereby $\mathfrak{a}\cdot\mathfrak{a}^{-1} = \langle 1\rangle = S$.

$(ii) \Longrightarrow (i)$. By (ii) we get $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a}^{-1} \subseteq \mathfrak{b}^{-1}$, whence it follows $\mathfrak{a}\cdot\mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{b}$ with $\mathfrak{a}^{-1}\mathfrak{b} \subseteq S$.

$(i) \Longleftrightarrow (iii)$. It suffices to verify $(iii) \Longrightarrow (i)$ and thereby it suffices – according to 13.5.7 – to prove the equivalence of (x) and (w), which follows by:

$$\begin{aligned} a/b \in \mathfrak{p}^{-1} &\Longleftrightarrow \mathfrak{p}\cdot\langle a\rangle \subseteq \langle b\rangle \;\; (\text{with} b \nmid a) \\ &\Longleftrightarrow \langle a\rangle * \langle b\rangle \supseteq \mathfrak{p} \\ &\Longleftrightarrow \langle a\rangle * \langle b\rangle = \mathfrak{p}\,, \end{aligned}$$

the final equivalence because of maximality of $\mathfrak{p}$. □

Dedekind gave three different approaches, compare [104], to his celebrated fundamental theorem of classical ideal theory. He showed, that on the one hand it is possible to develop the fundamental theorem first, in order to prove the multiplication property, but that on the other hand, it is possible as well, to prove the multiplication property first, in order to develop the ZPI-(Zerlegung (in) Prim/Ideale)-property, starting from condition (M).

In [41] Aubert posed the question whether this result also holds for t-ideals. Twelve years later, in [41], Aubert informs that the answer is affirmative, as was pointed out by (his PhD-student) [1)], K. Gudlaugsson, [176]. We prove Gudlaugssons result along the lines of the present paper.

Recall – by our remark above, according to [245] – it holds:

13. 5. 9 Proposition. *Let $\mathfrak{S}$ be a cancellative monoid. Then condition (M) for t-ideals implies the Noether property for t-ideals.*

This implies further along well known lines, that Mori t-ideal monoids have the ZPI property. But it also holds:

13. 5. 10 Proposition. *Let $\mathfrak{S}$ be a cancellative commutative monoid. Then $\mathfrak{S}$ is a t-multiplication-monoid iff each t-ideal is a product of prime t-ideals.*

[1)] personal remark of the author

PROOF. We prove first that the quotient $\mathfrak{b} * \mathfrak{c}$ of divisors $\mathfrak{b}, \mathfrak{c}$ is again a divisor, and thereby finitely generated, according to the proof of KRULLs lemma above.

We start from the *prime factorizations* of $\mathfrak{b}\,, \mathfrak{c}\,.$ Since all principal t-ideals are cancellable, the prime t-ideals of these factorizations are clearly cancellable, and they are divisors since in case that $\mathfrak{p} \cdot \mathfrak{x}$ is a divisor it results $\mathfrak{p} \supseteq \langle c \rangle \Longrightarrow \mathfrak{p} \cdot \mathfrak{x} \supseteq \langle c \rangle \cdot \mathfrak{x} \Longrightarrow \mathfrak{p} \cdot \mathfrak{x} \cdot \mathfrak{y} = \langle c \rangle \cdot \mathfrak{x} \Longrightarrow \mathfrak{p} \cdot \mathfrak{y} = \langle c \rangle\,.$ But in case $\mathfrak{a} \supset \mathfrak{p}$ with divisor $\mathfrak{a}$ and prime divisor $\mathfrak{p}$ we get $\mathfrak{a} \cdot \mathfrak{p} = \mathfrak{p} \rightsquigarrow \mathfrak{a} = \langle 1 \rangle\,.$ Consequently prime divisors can't properly contain prime divisors. In particular this means that in case $\mathfrak{a} \mid \mathfrak{b}$ with divisors $\mathfrak{a}, \mathfrak{b}$ the prime ideal decomposition of $\mathfrak{a}$ is a subproduct of the prime ideal decomposition of $\mathfrak{b}\,.$ From this it follows easily by dividing and cancelling that $\mathfrak{b} \cap \mathfrak{c}$ is built by *maximal prime powers* like the classical LCM in $\mathbf{N}\,.$ Hence $\mathfrak{b} \cap \mathfrak{c}$ is a product of cancellable prime divisors and thereby a divisor itself. Hence $\mathfrak{b} * \mathfrak{c} = \mathfrak{b} * (\mathfrak{a} \cap \mathfrak{c})$ is a divisor, too, with

$$(\mathfrak{b} * (\mathfrak{b} \cap \mathfrak{c})) * (\mathfrak{b} \cap \mathfrak{c}) = \mathfrak{b}\,. \tag{13.24}$$

We now show that all t-ideals are finitely generated.

To this end consider some arbitrary t-ideal $\mathfrak{a}\,.$ If $\mathfrak{a}$ is of type $\langle b \rangle * \langle c \rangle\,,$ then $\mathfrak{a}$ is a divisor and hence finitely generated. Otherwise there exists a finitely generated sub-t-ideal $\langle a_1, \ldots, a_n \rangle$, satisfying for some suitable pair b_1, c_1 and some suitable a_{n+1}

$$\begin{array}{ccc} c_1 \mid \langle a_1, \ldots, a_n \rangle \cdot b_1 & \& & c_1 \nmid \langle a_1, \ldots, a_n, a_{n+1} \rangle \cdot b_1 \\ & \rightsquigarrow & \\ \langle b \rangle_1 * \langle c \rangle_1 \supseteq \langle a_1, \ldots, a_n \rangle & \& & \langle b \rangle_1 * \langle c \rangle_1 \not\supseteq \langle a_1, \ldots, a_n, a_{n+1} \rangle \end{array}$$

Next we find some $\langle b \rangle_2 * \langle c \rangle_2 \supseteq \langle a_1, \ldots, a_n, a_{n+1} \rangle$ but – for some suitable a_{n+2} – satisfying $\langle b \rangle_2 * \langle c \rangle_2 \not\supseteq \langle a_1, \ldots, a_{n+1}, a_{n+2} \rangle$ etc. Thus we are led successively to a series $\langle b \rangle_1 * \langle c \rangle_1\,, \ldots, \langle b \rangle_n * \langle c \rangle_n\,, \ldots$ of divisors of $\langle a \rangle_1$, and it is easily seen by (13.24) that these divisors have pairwise different complements $(\langle b \rangle_k * \langle c \rangle_k) * \langle a \rangle_1\,.$

Hence $\mathfrak{a}$ is finitely generated. But this means that 13.3.2 works also in the present situation, in particular that $\langle a \rangle * \langle b \rangle + \langle b \rangle * \langle a \rangle = \langle 1 \rangle$ is satisfied. □

A Remark: Obviously the preceding proof works even in case that we require the ZPI-property for v-ideals. But, of course, v-multiplication-monoids need not have the ZPI-property. Consider some infinite boolean ring.

In [39] Aubert stated the problem whether the classical theorem that condition (M) holds for d-ideals if and only if any d-ideal is a product of prime d-ideals is valid for t-ideals, too. 12 years later he informs in [41] that his PHD-student Gudlaugson succeeded in solving that problem. We give a proof based on the **divisor lemma.**

13. 5. 11 Proposition. *A cancellative monoid $\mathfrak{S}$ is a t-multiplication monoid iff any t-ideal is a product of prime t-ideals.*

PROOF. Necessity is obvious, since by 13.5.9 the chain condition holds.

Sufficiency. The first part of this proof is valid for any ideal system with cancellable principal ideals.

We consider a prime divisor, observe, not only a prime element but even a prime divisor. Since any such prime divisor divides some a any prime divisor is cancellable. So prime divisors cannot properly contain prime divisors. In particular this means that in case of divisors $\mathfrak{a} \supseteq \mathfrak{b}$ the prime ideal decomposition of $\mathfrak{a}$ is a subproduct of that of $\mathfrak{b}$. From this it results next that the prime ideal decomposition of divisors $\mathfrak{b} \cap \mathfrak{c}$ is built like the GCD in number theory. Hence $\mathfrak{b} * \mathfrak{c} = \mathfrak{b} * (\mathfrak{b} \cap \mathfrak{c})$ is a divisor, too. This means in particular that any $a * b$ is a divisor, meaning that condition (d) is satisfied.

Hence we are through if we can show, that all t-ideals are finitely generated, since in that case all t-ideals are also v-ideals and vice versa, and since moreover in that case any principal t-ideal has only finitely many divisors, yielding $\mathfrak{a}^n \mid b \ (\forall\, n \in \mathbf{N}) \Longrightarrow \mathfrak{a} = 1$.

So, assume that $\mathfrak{a}$ is no divisor, in particular not of type $b * c$. Then there exists a finitely generated sub$-t$-ideal $\langle a_1, \ldots, a_n\rangle$ with some $b_1 * c_1 \supseteq \langle a_1, \ldots, a_n\rangle$ but – for some suitable a_{n+1} – satisfying $b_1 * c_1 \not\supseteq \langle a_1, \ldots, a_n, a_{n+1}\rangle$. And next we get some b_2, c_2, a_{n+2} satisfying the conditions $b_2 * c_2 \supseteq \langle a_1, \ldots, a_n, a_{n+1}\rangle$ but $b_2 * c_2 \not\supseteq \langle a_1, \ldots, a_{n+1}, a_{n+2}\rangle$.

Continuing, thus we are led to a series $b_1 * c_1, \ldots, b_n * c_n$ of divisors of – for instance a_1, and it is easily seen that divisors $\mathfrak{b}, \mathfrak{c}$ satisfy $(\mathfrak{b}*(\mathfrak{b}\cap\mathfrak{c}))*(\mathfrak{b}\cap\mathfrak{c}) = \mathfrak{b}$ whence the divisors $(b_k * c_k) * a_1$ have pairwise different complements. But all complements are subproducts of the prime decomposition of a_1.

Hence $\mathfrak{a}$ is finitely generated. This means that any v-ideal is finite. So, applying 13.5.9 the proof is complete. $\square$

Next we turn to AMLs with cancellable generators, thus including r- d- and t-ideals of cancellative zero monoids and integral domains.

Applying 12.3.1 and 13.5.9 here we get as a first result:

13. 5. 12 Proposition. *Let $\mathfrak{A}$ be an AML generated by a cancellative zero monoid $\mathcal{A}_c$. Then $\mathfrak{A}$ has the multiplication property if and only if any $A \neq 0$ is a product of maximal elements.*

The proof of the preceding proposition could also have been done by applying 13.4.1 and the Prüfer property. The way above, however avoids (n)$\Longrightarrow$(P).

13.6 Sorrowing looking back

Starting point of the author's scientific work was the CLIFFORD PAPER [93] written in 1932 – the author's birth year – and published in 1938.

CLIFFORD's question: Which conditions are necessary and sufficient in order that a given holoid $(S, \cdot, 1)$ admits a normal extension $(\sum, \cdot, 1)$ whose elements are unique irredundant products of atoms of $\sum$. At this place we come back to that question – after a break of more than 40 years, compare [60, 61].

13. 6. 1 A general v-Ideal-Theorem. *Let $\mathfrak{S}$ be a commutative monoid. Then $\mathfrak{S}$ admits a normal extension with unique atom decompositions if and only if its t-ideal monoid satisfies the condition:*

$$(\mathfrak{a} * \mathfrak{b}) * \mathfrak{b} = (\mathfrak{b} * \mathfrak{a}) * \mathfrak{a}.$$

PROOF. One direction is clear, recall 12.4.2. The other one is a consequence of the uniqueness property which by 7.2.7 implies the existence of some $|$- normal extension meaning that the v-ideal extension and thereby the t-ideal extension has the Noether- and the Prüfer property. $\square$

Bibliography

[1] Arnold, I.: *Ideale in kommutativen Halbgruppen.* Math. Sb. **36** (1929), 401 - 407.

[2] Akizuki, Y.: *Bemerkungen über den Aufbau des Nullideals.* Proc. Phys.-Math. Soc. Japan **14** (1932), 253 - 262.

[3] Anderson, D. D.: *Multiplication ideals, Multiplication rings, and the ring R (X).* Canad. J. Math **XXVIII** (1976), 760 -768.

[4] Anderson, D. D.: *Abstract commutative ideal theory without chain condition.* Alg. Univ. **6** (1976), 131 - 145.

[5] Anderson, D. D.: *Some remarks on the Ring R (X).* Comm. Math. Univ. St. Pauli **2** (1977), 137 - 140.

[6] Anderson, D. D.: *Noetherian rings in which every ideal is a product of primary ideals.* Canad. Math. Bull. **23** (1980), 457 - 459.

[7] Anderson, D. D.: *Some remarks on multiplication ideals.* Math. Japon. **25** (1980), 463 - 469.

[8] Anderson, D. D. and D. F. Anderson: *Generalized GCD-Domains.* Comm. Math. Univ. St. Pauli **28** (1979), 215 - 221.

[9] Anderson, D. D. and D. F. Anderson: *Some remarks on cancellation ideals.* Math. Japon. **29** (1984), 879 - 886.

[10] Anderson, D. D., Anderson, D. F. and R. Markanda: *The rings $R(X)$ and $R\langle X\rangle$.* J. Algebra **95** (1985), 96 - 115.

[11] Anderson, D. D., Anderson, D. F., Costa, D. L., Dobbs, D. E., Mott, J. L. and M. Zafrullah: *Some characterizations of v-domains and related properties.* Coll. Math. **58** (1989), no. 1, 1 - 9.

[12] Anderson, D. D., Anderson, D. F., M. Zafrullah: *Splitting the t-class group.* J. Pure Appl. Algebra **74** (1991), no. 1, 17 - 37.

[13] Anderson, D. D. and E. W. Johnson: *Arithmetically embeddable local Noether lattices.* Michigan Math. J. **23** (1976), 177 - 184.

[14] Anderson, D. D. and E. W. Johnson: *Ideal Theory in commutative Semigoups.* Semig. For. **30** (1984), 127 - 158.

[15] Anderson, D. D. and E. W. Johnson: *A new characterization of Dedekind domains.* Glasgow. Math. J. **28** (1986), 237 - 239.

[16] Anderson, D. D. and B. G. Kang: *Some remarks on the Ring R (X).* Comm. Math. Univ. St.Pauli **2** (1977), 137 - 140.

[17] Anderson, D. D. and R. Markanda: *Unique factorization rings with zero divisors.* Houston J. Math. **11** (1985), 15 - 30.

[18] Anderson, D. D. and L. A. Mahaney: *Commutative rings in which every ideal is a product of primary ideals.*J. Algebra **106** (1987), 528 - 535.

[19] Anderson, D. D. and L. A. Mahaney: *On primary factorization.* J. Pure and Applied Algebra **54** (1988), 141 - 154.

[20] Anderson, D. D., and J. Pascual: *Characterizing Prüfer rings via their regular ideals.* Comm. Algebra **15** (1987), 1287 - 1295.

[21] Anderson, D. D. and J. Pascual: *Regular ideals in commutative rings, sublattices of regular ideals, and Prüfer rings.* J. Algebra **111** (1987), 404 - 426.

[22] Anderson, D. D. and M. Zafrullah: *Weakly factorial domains and groups of divisibility.* Proc. Amer. Math. Soc. **109** (1991), no. 4, 907 - 913.

[23] Anderson, D. D. and M. Zafrullah: *Almost Bézout domains. J. Algebra* **142** *(1991), no. 2, 285 - 309.*

[24] Arapovic, M.: *On general ZPI-rings.* Rad. Math. **3** (1987), 99 - 103.

[25] Arnold, I.: *Ideale in kommutativen Halbgruppen.* Mat. Sb. **36** (1929), 401 - 408.

[26] Artin, E.: *Zur Arithmetik hyperkomplexer Zahlen.* Abh. Math. Sem. Hamburg **5** (1927), 261 - 289.

[27] Artin, E.: *Über die Bewertungen algebraischer Zahlkörper.* J. Reine Angew. Math. **167** (1932), 157 - 159.

[28] ASANO, K.: *Über kommutative Ringe, in denen jedes Ideal als Produkt von Primidealen darstellbar ist.* J. Math. Soc. Japan **1** (1951), 82 - 90.

[29] AUBERT, K. E.: *On the ideal theory of commutative semigroups.* Math. Scand. **1** (1953), 39 - 54.

[30] AUBERT, K. E.: *Some characterizations of valuation rings.* Duke Math. J. **21** (1954), 517 - 525.

[31] AUBERT, K. E.: *Über Bewertungen mit halbgeordneter Wertegruppe.* Math. Ann. **127** (1954), 8 - 14.

[32] AUBERT, K. E.: *Some characterizations of valuation rings.* Duke Math. J. **21** (1954), 517 - 526.

[33] AUBERT, K. E.: *Généralisation de la théorie des r-idéaux de Prüfer-Lorenzen.* C. R. Acad. Sci. Paris **238** (1954), 2.214 - 2.216.

[34] AUBERT, K. E.: *Contribution à la théorie des idéaux et à la théorie des valuations.* Thèse, Paris 1957.

[35] AUBERT, K. E.: *Un thèorème de reprèsentation dans la théorie des idéaux.* C. R. Acad. Sci. Paris **242** (1956), 303 - 305.

[36] AUBERT, K. E.: *Charactérizations des anneaux de valuation à l'aide de la theorie des r-idéaux.* Semig. P. Dubreil et C. Pisot **10**, 1958.

[37] AUBERT, K. E.: *Un théorème d'immersion pour une classe étendue de structures algébriques réticulés.* An. Acad. Brasil, Ci. **31** (1959), 321 - 329.

[38] AUBERT, K. E.: *Theory of x-ideals.* Acta Math. **107** (1962), 1 - 52.

[39] AUBERT, K. E.: *Additive ideal systems.* J. Algebra **18** (1971), 511 - 528.

[40] AUBERT, K. E.: *Localization dans les systemes d'idéaux.* C. R. Acad. Sci. Paris Ser. 1 Math. **272** (1971), 465 - 468,

[41] AUBERT, K. E.: *Divisors of finite character.* Ann. Mat. Pura Appl., IV. Ser. **133** (1983), 327 - 361.

[42] BANDYOPADHYAYA, S. D.: *Valuations in groups and rings.* Czech. Math. J. **19** (1969), 275 - 276.

[43] BANDYOPADHYAYA, S. D.: *Rings with valuations.* Math. Nach. **44** (1970), 1 - 18.

[44] Bandyopadhyaya, S. D.:*On U-semigroups.* Math. Nach. **44** (1970), 19 - 27.

[45] Barnes, W. E.: *Primal ideals and isolated components in noncommutative rings.* Trans. Amer. Math. Soc. **82** (1956), 1 - 16.

[46] Barnes, W. E. and W. M. Cunnea: *Ideal decompositions in Noetherian rings.* Canad. J. Math. **17** (1965), 178 - 184.

[47] Barnes, W. E. and W. M. Cunnea: *On primary representations of ideals in noncommutative rings.* Math. Ann. **173** (1967), 233 - 237.

[48] Barucci, Valentina: *On a class of Mori domains.* Comm. Algebra **11** (1983), 1989 - 2001.

[49] Barucci, Valentina: *On the polynomial ring over a Mori domain.* Publ. Dép. Math. Nouvelle Sr. B, Univ. Claude-Bernard Lyon, **3** (1988), 59 - 63.

[50] Barucci, Valentina and Stephania Gabelli: *How far is a Mori domain from being a Krull domain?* J. Pure Appl. Algebra **45** (1987), 101 - 102.

[51] Barucci, Valentina; Gabelli, Stephania and M. Roitman: *On semi-Krull domains.* J. Algebra **145** (1992), no. 2, 306 - 328.

[52] Bogart, K. P.: *Distributive local Noether lattices.* Michigan Math. J. **16** (1969), 215 - 223.

[53] Boisen, M. and M. D. Larsen: *Prüfer and valuation rings with zero divisors.* Proc. Amer. Math. Soc. **40** (1973), 87 - 90.

[54] Boisen, M. and M. D. Larsen: *On Prüfer rings as images of Prüfer domains.* Proc. Amer. Math. Soc. **40** (1973), 87 - 90.

[55] Borewicz, S. I. and I. R. Šafarevič: *Zahlentheorie.* Birkhäuser Verlag Basel und Stuttgart 1966.

[56] Bosbach, B.: *Charakterisierungen von Halbgruppen mit eindeutigen Halbprimfaktorzerlegungen.* Math. Ann. **139**, (1960), 184 - 196.

[57] Bosbach, B.: *Charakterisierungen von Halbgruppen mit eindeutigen Halbprimfaktorzerlegungen unter Berücksichtigung der Verbände und Ringe.* Math. Ann. **141**, (1960), 193 - 209.

[58] Bosbach, B.: *Arithmetische Halbgruppen.* Math. Ann. **144**, (1961), 239 - 252.

[59] Bosbach, B.: *Eine Zerlegungs- und Idealtheorie für kommutative Halbgruppen.* Math. Zeitschr. **82**, (1963), 37 - 58.

[60] Bosbach, B.: *Zur Zerlegungs- und Idealtheorie kommutativer Halbgruppen.* Math. Zeitschr. **84**, (1964), 45 - 51.

[61] Bosbach, B.: *Zur konstruktiven Idealtheorie kommutativer Halbgruppen.* Math. Zeitschr. **84**, (1965), 190 - 206.

[62] Bosbach, B.: *Transzendente Ringerweiterungen.* Math. Ann. **178**, (1968), 299 - 301.

[63] Bosbach, B.: *Komplementäre Halbgruppen, Axiomatik und Arithmetik.* Fund. Math. **LXIV** (1969), 257 - 287.

[64] Bosbach, B.: *Komplementäre Halbgruppen, Kongruenzen und Quotienten.* Fund. Math. **LXIX** (1970), 1 - 14.

[65] Bosbach, B.: *Zur Theorie der Teilbarkeitshalbgruppen.* Semig. For. **3** (1971), 1 - 30.

[66] Bosbach, B.: *Schwache Teilbarkeitshalbgruppen.* Semig. For. **12** (1976), 119 - 135.

[67] Bosbach, B.: *Zur Struktur der inversen Teilbarkeitshalbgruppen.* Semig. For. **12** (1976), 137 - 143.

[68] Bosbach, B.: *Zur Theorie der stetigen Teilbarkeitshalbgruppen.* Semig. For. **20** (1980), 299 - 317.

[69] Bosbach, B.: *Archimedische Teilbarkeitshalbgruppen und Quaderalgebren.* Semig. For. **20** (1980), 319 - 334.

[70] Bosbach, B.: *Zur Theorie der vollständigen Teilbarkeitshalbgruppen.* Semig. For. **25** (1982), 111 - 124.

[71] Bosbach, B.: *Teilbarkeitshalbgruppen mit vollständiger Erweiterung.* J. Algebra **83** (1983), 237 - 255.

[72] Bosbach, B.: *Lattice ordered binary systems.* Acta Sci. Math. **52** (1988), 257 - 289.

[73] Bosbach, B.: *Separative Teilbarkeitshalbgruppen.* Contrib. Alg. **6** (1988), 49 - 65.

[74] Bosbach, B.: *Hyperarchimedische Teilbarkeitshalbgruppen.* Czech. Math. J. **39** (114) (1989), 528 - 543.

[75] Bosbach, B.: *Representable Divisibility Semigroups.* Proc. Edinb. Math. Soc. **34** (1991), 45 - 64.

[76] Bosbach, B.: *Idealhalbgruppen* – $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \mid \mathfrak{b}$. Universität Kassel, 1994, a private manuscript.

[77] Bosbach, B.: *Teilbarkeitshalbgruppen.* Universität Kassel, 1997, a private manuscript.

[78] Bosbach, B.: *Residuationsstrukturen.* Universität Kassel 1997, a private manuscript.

[79] Bosbach, B.: *Algebraic multiplication m-lattices.* Alg. Univ. **44** (2000), 47 - 64.

[80] Bosbach, B.: *Classical Ideal Semigroups.* Result. Math. **37** (2000), 36 - 46.

[81] Bosbach, B.: *Convex chains in lattice monoids and lattice loops.* Acta. Sc. Math. (Szeged) **67** (2001), 57 - 75.

[82] Bosbach, B.: *Archimedean Prüfer sructures, alias Filter archimedean dsemigroups.* Acta Math. Hungar. **95** (2002), 53 - 73 ,

[83] Bosbach, B.: *Ideal Divisibility Monoids.* Result. Math. **41** (2002), 40 - 67.

[84] Bosbach, B.: *Ringlike Ideal Monoids.* Sc. Math. Japon. **55** (2002), 233 - 249.

[85] Brandal, W.: *Constructing Bézout domains.* Rocky Mountain J. of Math. **6** (1976), 383 - 399.

[86] Brungs, H. H.: *Generalized discrete valuation rings.* Canad. J. Math. **6** (1969), 1404 - 1408.

[87] Burris, St. H.P. Sankappanavar.: *A course in universal algebra.* Graduate Texts in Mathematics, **78**. Springer, New York – Berlin, 1981. xvi+276 pp.

[88] Butts, H. S.: *Unique factorization of ideals into nonfactorable ideals.* Proc. Amer. Math. Soc. **15** (1964), 21 - 21.

[89] Butts, H. S. and R. W. Gilmer: *Primary ideals and prime power ideals.* Canad. J. Math. **18** (1966), 1183 - 1195.

[90] Butts, H. S. and R. C. Phillips: *Almost multiplication rings.* Canad. J. Math. **17** (1965), 267 - 277.

[91] Butts, H. and W. Smith: *Prüfer rings.* Math. Z. **95** (1967), 196 - 211.

[92] Chew, K. L.: *On a conjecture of D. C. Murdoch concerning primary decompositions of an ideal.* Proc. Amer. Math. Soc. **19** (1968), 925 - 932.

[93] Clifford, A. H.: *Arithmetic and ideal theory of commutative semigroups.* Ann. Math. **39** (1938), 594 - 610.

[94] Cohen, I. S.: *Commutative rings with restricted minimum condition.* Duke Math. J. **17** (1950), 27 - 42.

[95] Cohn, P. M.: *Bézout rings and their subrings.* Proc. Cambridge Phil. Soc. **64** (1968), 251 - 264.

[96] Cohn, P. M.: *Systems of ideals.* Canad. J. Math. **21** (1969), 783 - 807.

[97] Costa, D. and M. Roitman: *A lifting approach to t- and v-ideals.* Comm. Algebra. **18** (1990), no. 11, 3725 - 3742.

[98] Cunnea, W. M.: *Unique factorization in algebraic function fields.* Illinois J. Math. **8** (1964), 425 - 438.

[99] Dieudonnè J.: *Sur la Theorie de la Divisibilitè.* Bull. Soc. Math. France **49** (1941), 1 - 12.

[100] Dedekind, R.: *Über die Zerlegungen der Zahlen durch ihre größten gemeinschaftlichen Teiler.* Festschrift der T. H. Braunschweig zur 60. Versammlung deutscher Naturforscher und Ärzte 1897, 1 - 40.

[101] Dedekind, R.: Über die von drei Moduln erzeugte Dualgruppe. Math. Ann. **53** (1900), 371 - 403.

[102] Dedekind, R. und H. Weber: *Theorie der algebraischen Funktionen einer Veränderlichen.* J. Reine Angew. Math. **92** (1882), 181 - 290.

[103] Dilworth, R. P.: *Abstract commutative ideal theory.* Pacific J. Math. **12** (1962), 481 - 498.

[104] Dirichlet, P. G.: *Vorlesungen über Zahlentheorie.* Vieweg und Sohn, Braunschweig, 1.,2.,3.,4. Auflage 1872 - 1894.

[105] Dobbs, D. E., Houston, E. G., Lucas, T. G. , and M. Zafrullah: *t-linked overrings and Prüfer v-multiplication domains.* Comm. Algebra **17** (1989), no. 11, 2835 - 2852.

[106] Dobbs, D. E., Houston, E. G., Lucas. T. G., Roitman, M. and M. Zafrullah: *On t-linked overrings.* Comm. Algebra **20** (1992), no. 5, 1463 - 1488.

[107] Dorofeeva, M. P.: *Hereditaryand semi-hereditary monoids.* Semig. For. **4** (1972), 301 - 311.

[108] Dorofeeva, M. P., Mannepalli V. L. and M. Satyanarayana: *Prüfer and Dedekind monoids.* Semig. For. **9** (1975), 294 - 309.

[109] Dorofeeva, M. P., Mannepalli V. L. and M. Satyanarayana: *Prüfer and Dedekind monoids* II. Semig. For. **11** (1975), 102 - 114.

[110] El-Bast, Z. A. and P. F. Smith: *Multiplication modules.* Comm. Algebra **16** (1988), no. 4, 755 - 779.

[111] El-Bast, Z. A. and P. F. Smith: *Multiplication modules.* Comm. Algebra **16** (1988), no. 4, 781 - 796.

[112] Edwards, H. M.: *The background of Kummer's proof of Fermat's last theorem for regular primes.* Arch. Hist. Exact. Sci. **14** (1975), 219 - 236.

[113] Edwards, H. M.: *Postscript to "The background of Kummer's proof of Fermat's last theorem for regular primes".* Arch. Hist. Exact. Sci. **17** (1977), 381 - 394.

[114] Edwards, H. M.: *Ferm at's Last Theorem.* Springer, Berlin - Heidelberg - New York, 1977.

[115] Edwards, H. M.: *The Genesis of Ideal Theory.* Arch. Hist. Ex. Sci., **23** (1980) 321 - 378.

[116] Edwards, H. M.: *Dedekind's Invention of Ideals.* Bull. Lond. Math. Soc. **15** (1983), 8 - 17.

[117] Edwards. M. H.: *Divisor Theory.* Birkhäuser, Boston-Basel-Berlin, 1990.

[118] Edwards, H. M., Neumann, O. and b W. Purkert: *Dedekinds "Bunte Bemerkungen" zu Kroneckers "Grundzüge(n)".* Arch. Hist. Ex. Sci. **27** (1982), 49 - 85.

[119] Eggert, N. and H. Rutherford: *A local characterization of Prüfer rings.* J. Reine Angew. Math. **250** (1971), 109 - 112.

[120] Engström, H. T.: *The theorem of Dedekind in the ideal theory of Zolotarev.* Trans. Amer. Math. Soc. **32** (1930), 879 - 887.

[121] Erdoŏgdu, V.: *Regular multiplication rings.* J. Pure Appl. Algebra **59** (1989), 55 - 59.

[122] Erdoŏgdu, V.: *The distributive hull of a ring.* J. Algebra, **132** (1989), no. 2, 263 - 269.

[123] Faith, C.: *The structure of valuation rings.* J. Pure Appl. Alg. **31** (1984), 7 - 27.

[124] Fleischer, I.: *Equivalence of x-systems and m-lattices.* Contributions to Lattice Theory, Szeged, Hungary (1980), 381 - 400.

[125] Fleischer, I.: *Abstract Prüfer Ideal Theory.* J. Algebra **115** (1988), 332 - 339.

[126] Fleischer, I.: *Abstract Ideal Theory.* Normat **3** (1995), 120 - 135.

[127] Fitting, H.: *Primärkomponentenzerlegung in nicht kommutativen Ringen.* Math. Ann. **111** (1935), 19 - 41.

[128] Fraenkel, A.: *Über die Teiler der Null und die Zerlegung von Ringen.* (Crelles) J. Reine Angew. Math. **145** (1915), 139 176.

[129] Fuchs, L.: *On quasi-primary ideals.* Acta. Sci. Math. **11** (1947), 174 - 183.

[130] Fuchs, L.: *A condition under which an irreducible ideal is primary.*Quart. J. Math. Oxford. Ser. **19** (1948), 235 - 237.

[131] Fuchs, L.: *Über die Ideale arithmetischer Ringe.* Comm. Math. Helv. **23** (1949), 334 - 341.

[132] Fuchs, L.: *The generalization of the valuation theory.* Duke Math. J. **18** (1951), 19 - 56.

[133] Fuchs, L.: *On the fundamental theorem of commutative ideal theory.* Acta Math. Acad. Sci. Hungar. **5** (1954), 95 - 99.

[134] Fuchs, L.: *An extension theorem on valuations.* J. Math. Soc. Japan **17** (1965), 67 - 71.

[135] Fuchs, L.: *Teilweise geordnete algebraische Strukturen.* Vandenhoek und Ruprecht, Göttingen, 1966.

[136] Fukawa, M.: *On the theory of valuations.* J. Fac. Sci. Univ. Tokyo Ser. I, **XII** (1965), 57 - 79.

[137] Gabelli, Stephania: *Completely integrally closed domains and t-ideals.* Boll. Un. Math. Ital. B (7) **3** (1989), 327 - 343.

[138] Ganesan, N.: *Properties of rings with a finite number of zero divisors.* Math. Ann. **157** (1964), 215 - 218.

[139] Ganesan, N.: *Properties of rings with a finite number of zero divisors* II. Math. Ann. **161** (1965), 241 - 246.

[140] Geroldinger, A.: *Über nicht-eindeutige Zerlegungen in irreduzible Elemente.* Math. Z. **197** (1988), 505 - 529.

[141] Geroldinger, A. and F. Halter-Koch: *Realization Theorems for Semigroups with Divisor Theory.* Semig. For. **44** (1992), 229 - 237.

[142] Gilmer, R. W. Jr.: *Rings in which semi-primary ideals are primary.* Pacific J. Math. **12** (1962), 1273 - 1276.

[143] Gilmer, R. W. Jr.: *On a classical theorem of Noether in ideal theory.* Pacific J. Math. **13** (1963), 579 - 583.

[144] Gilmer, R. W. Jr.: *Commutative rings containing at most two prime ideals.* Mich. Math. J. **10** (1963), 263 - 268.

[145] Gilmer, R. W. Jr.: *Rings in which the unique primary decomposition theorem holds.* Proc. Amer. Math. Soc. **14** (1963), 777 - 781.

[146] Gilmer, R. W. Jr.: *Integral domains which are almost Dedekind.* Proc. Amer. Math. Soc. **15** (1964), 813 - 818.

[147] Gilmer, R. W. Jr.: *Extensions of results concerning rings in which semi-primary ideals are primary.* Duke Math. J. **31** (1964), 73 - 78.

[148] Gilmer, R. W. Jr.: *The cancellation law for ideals in a commuative ring.* Canad. J. Math. **17** (1965), 281 - 287.

[149] Gilmer, R. W. Jr.: *Overrings of Prüfer domains.* J. Algebra **4** (1966), 331 - 340.

[150] Gilmer, R. W. Jr.: *Domains in which valuation ideals are prime powers.* Arch. Math. (Basel) **17** (1966), 210 - 215.

[151] Gilmer, R. W. Jr.: *The pseudo-radical of a commutative ring.* Pacific J. Math. **19** (1966), 275 - 284.

[152] Gilmer, R. W. Jr.: *A class of domains in which primary ideals are valuation ideals* II . Math. Ann. **171** (1967), 93 - 96.

[153] Gilmer, R. W. Jr.: *Commutative rings in which each prime ideal is principal.* Math. Ann. **183** (1969), 151 - 158.

[154] Gilmer, R. W. Jr.: *A note on semigroup rings.* Amer. Math. Monthly **75** (1969), 36 - 37.

[155] Gilmer, R. W. Jr.: *Two constructions of Prüfer domains.*
J. Reine Angew. Math. **239/240** (1970), 153 - 162.

[156] Gilmer, R. W. Jr.: *Multiplicative Ideal Theory.* Marcel Dekker, New York, 1972.

[157] Gilmer, R. W. Jr.: *On Prüfer rings.*
Bull. Amer. Math. Soc. **78** (1972), 223 - 224.

[158] Gilmer, R. W. Jr.: *Eleven nonequivalent conditions on a commutative ring.* Nagoya Math. J. **26** (1966), 183 - 194.

[159] Gilmer, R. W. and W. J. Heinzer: *Overrings of Prüfer domains* II. J. Algebra **7** (1967), 281 - 302.

[160] Gilmer, R. W. and W. J. Heinzer: *Irredundant intersections of valuation rings.* Math. Z. **103** (1968), 306 - 317.

[161] Gilmer, R. W. and W. J. Heinzer: *Primary ideals and valuation ideals* II. Trans. Amer. Math. Soc. **131** (1968), 149 - 162.

[162] Gilmer, R. W. and J. Hoffmann: *A characterization of Prüfer domains in terms of polynomials.* Pac. J. Math. **60** (1975), 81 - 85.

[163] Gilmer, R. W. and J. L. Mott: *Multiplication rings as rings in which ideals with prime radical are primary.* Trans. Amer. Math. Soc. **114** (1965), 40 - 52.

[164] Gilmer, R. W. and T. Parker: *Divisibility properties in semigroup rings.* Mich. Math. J. **21** (1974), 65 - 86.

[165] Gilmer, R. W. and T. Parker: *Semigroup rings as Prüfer rings.* Duke Math. J. **41** (1974), 219 - 230.

[166] Gilmer, R. W. and J. Ohm: *Primary ideals and valuation ideals.* Trans. Amer. Math. Soc. **117** (1965), 237 - 250.

[167] Gräter, J.: *Über die Distributivität des Idealverbandes eines kommutativen Ringes.* Rec. Math. Soc. Math. Moscou **32** (1924), 135 - 151. (Russisch, franz. Referat)

[168] Gravé, D.: *Über die Grundlagen der Theorie der Idealzahlen.* Rec. Math. Soc. Math. Moscou **32** (1924), 135 - 151. (Russisch, franz. Referat)

[169] Gravé, D.: *Über die Zerlegung der Zahlen in ideale Faktoren.* Rec. Math. Soc. Math. Moscou **32** (1925), 542 - 561. (Russich, franz. Referat).

[170] Griffin, M.: *Some results on v-multiplication rings.* Can. J. Math. **19** (1967), 710 - 722.

[171] Griffin, M.: *Families of finite character and essential valuations.* Trans. Amer. Math. Soc. **130** (1968), 75 - 85.

[172] Griffin, M.: *Rings of Krull type.* J. Reine Angew. Math. **229** (1968), 1 - 27.

[173] GRIFFIN, M.: *Prüfer rings with zero divisors.* J. Reine Angew. Math. **239/240** (1970), 55 - 67.

[174] GRIFFIN, M.: *Valuations and Prüfer rings.* Can. J. Math. **26** (1974), 412 - 429.

[175] GRIFFIN, M.: *Multiplication Rings via their total Quotient Rings.* Can. J. Math. **26** (1974), 430 - 449.

[176] GUDLAUGSSON,K.: *Unique factorization in ordered groups.* Thesis (in Norwegian), Oito 1982.

[177] HALTER-KOCH, F.: *Halbgruppen mit Divisorentheorie.* Expos. Math. **8** (1990), 27 - 67.

[178] HALTER-KOCH, F.: *Ein Approximationssatz für Halbgruppen mit Divisorentheorie.* Math. Res. **19** (1991), 74 - 82.

[179] HALTER-KOCH, F.: *Finiteness Theorems for Factorizations* Semig. For. **44** (1992), 112 - 117.

[180] HARDY, B. and T. SHORES: *Arithmetical semigroup rings.* Can. J. Math. **32** (1980), 1361 - 1371.

[181] HARRISON, D. K. and M. A. VITULLI: *v-Valuations of a Commutative Ring* I. J. Agebra **126** (1989), 264 - 292.

[182] HATTORI, A.: *On Prüfer rings.* J. Math. Soc. Japan **9** (1957), 381 - 385.

[183] HEBISCH, U. UND H. J. WEINERT: *Halbringe.* Teubner Studienbücher. B. G. Teubner, Stuttgart, 1993.

[184] HEINZER, W. J. and D. LANTZ: *The Laskerian property in commutative rings.* J. Algebra **72** (1981), 101 - 114.

[185] HELMS, A.: *Ein Beitrag zur algebraischen Theorie.* Math. Ann. **111** (1935), 438 - 458.

[186] HENSEL, K.: *Theorie der algebraischen Zahlen.* Teubner, Leipzig, 1908.

[187] HENSEL, K.: *Gedächtnisrede auf E. E. Kummer.* Abh. Gesch. Math. Wiss. Teubner, Berlin und Leipzig, 1910.

[188] HENSEL, K.: *E. E. Kummer und der große Fermatsche Satz.* Marburger Akademische Reden **23**, 1910.

[189] HENSEL, K.: *Über eindeutige Zerlegung in Primelemente.* J. Reine Angew. Math. **158** (1927), 195 - 198.

[190] Hermes, H.: *Einführung in die Verbandstheorie. 2. erw. Aufl.* Die Grundlehren der mathematischen Wissenschaften, Band 73 xii+209 pp. Springer-Verlag, Berlin New-York 1967.

[191] Hermida, J. A. and G. Sánchez-Tirada: *Sur les anneux de Prüfer.* Géométrie algébrique et applications (I) . (La Rábida 1984) 117 - 123, Hermann, Paris 1987.

[192] Hochster, M.: *Prime ideal structure of commutative rings.* Trans. Amer. Math. Soc. **142** (1969), 43 - 60.

[193] Holzapfel, R. P.: *Eine allgmeine Primärzerlegungstheorie.* Math. Nachr. **41** (1969), 227 - 245.

[194] Hopkins, C.: *Rings with minimal condition for left ideals.* Ann. of Math. **40** (1939), 712 - 730.

[195] Houston, E. G., T. G. Lucas, T. M. Viswanathan: *Primary Decomposition of Divisorial Ideals in Mori Domains.* J. Algebra **117** (1988), 327 - 342.

[196] Houston, E. G., Malik, S. B. and J. L. Mott: *Characterizations of *-multiplication domains.* Canad. Math. Bull. **27** (1984), 48 - 52.

[197] Houston, E. and M. Zafrullah: Integral domains in which each t-ideal is divisorial. Michigan Math. J. **35** (1988), no. 2, 291 - 300.

[198] Houston, E. and M. Zafrullah: On t-invertibility II. Comm. Algebra **17** (1989), 1955 - 1969.

[199] Huckaba, J. A.: *Extensions of pseudovaluations.* Pacific J. Math. **29** (1969), 295 - 302.

[200] Huckaba, J. A.: *Some results on pseudovaluations.* Duke Math. J. **37** (1970), 1 - 9.

[201] Huckaba, J. A.: *On valuation rings that contain zero divisors.* Proc. Amer. Math. Soc. **40** (1973), 9 - 15.

[202] Huckaba, J. A.: *The integral closure of a Noetherian ring.* Trans. Amer. Math. Soc. **220** (1976), 159 - 166.

[203] Huckaba, J. A.: *Commutative rings with zero divisors.* Marcel Decker Inc., New York and Basel, 01988.

[204] Hurwitz, A.: *Über die Theorie der Ideale.* Nachr. Ges. Wiss. Göttingen 1894, 291 - 298.

[205] Hurwitz, A.: *Über einen Fundamentalsatz der Theorie der algebraischen Größen.* Nachr. Ges. Wiss. Göttingen 1895, 230 - 240.

[206] Ihringer, Th: *Allgemeine Algebra.* Teubner Studienbücher. B. G. Teubner, Stuttgart 1988.

[207] Ishikawa, T.: *On Dedekind rings.* J. Math. Soc. Japan **1** (1959), 83 - 84.

[208] Jaffard, P.: *Théorie arithmétique des anneaux du type de Dedekind.* Bull. Soc. Math. France **80** (1952), 61 - 100.

[209] Jaffard, P.: *Théorie arithmétique des annaux du type de Dedekind* II. Bull. Soc. Math. France **81** (1953), 41 - 61.

[210] Jaffard, P.: *La notion de valuation.* Enseignement Math. **40** (1954), 5 - 26.

[211] Jaffard, P.: *Dimension des anneaux de polynomes. La notion de dimension valuative.* C. R. Acad. Sci. Paris Ser. A-B **246** (1958), 3305 - 3307.

[212] Jaffard, P.: *Dimension des anneaux de polynomes. Comportement asymptotique de la dimension.* C. R. Acad. Sci. Paris Ser. A-B **246** (1958), 3199 - 3201.

[213] Jaffard, P.: *Les Systèmes d'Ideaux.* Dunod, Paris, 1960.

[214] Jaffard, P.: *La théorie des idéaux d'Artin-Prüfer-Lorenzen.* Semig. A. Chatelet et P. Dubreil **3** (1961), 5 - 6.

[215] Jaffard, P.: *Valuations d'un anneaux Noethérian et théorie de la dimension.* Semig. P. Dubreil , M. L. Dubreil-Jacotin et C. Pisot **12** (1961), 13.

[216] Jain, R. K.: *On Dedekind monoids.* Semig. For. **24** (1982), 91 - 92.

[217] Jain, R. K.: *On multiplication rings.* Math. Student. **46** (1978), 359 - 363. (1982)

[218] Jain, R. K.: *On multiplication ideals.* Math. Student. **46** (1978), 116 - 120. (1982)

[219] Janowitz, M. F.: *Principle multiplicative lattices.* Pacific J. Math. **33** (1970), 653 - 656.

[220] Jensen, C. U.: *On characterizations of Prüfer rings.* Math. Scand. **13** (1963), 90 - 98.

[221] Jensen, C. U.: *A remark on arithmetical rings.* Proc. Amer. Math. Soc. **15** (1964), 951 - 954.

[222] Jensen, C. U.: *Arithmetical rings.* Acta Math. Acad. Sci. Hungar. **17** (1966), 115 - 123.

[223] Jensen, C. U.: *A remark on the distributive law for an ideal of a commutative ring.* Proc. Glasgow Math. Assoc. **7** (1966), 193 - 198.

[224] Jensen, C. U.: *A remark on flat and projective modules.* Canad. J. Math. **18** (1966), 943 - 949.

[225] Kang, B. G.: *Some questions on v-multiplication domains.* Comm. Algebra **17** (1989), no. 3, 553 - 564.

[226] Kang, B. G.: Prüfer v-multiplication domains and the ring $R[X]_N$. J. Algebra **123** (1989), no. 1, 151 - 170.

[227] Kaplansky, I.: Modules over Dedekind rings and valuation rings. Trans. Amer. Math. Soc. **72** (1952), 327 - 340.

[228] Kaplansky, I.: A characterization of Prüfer rings. J. Indian Math. Soc. (N.S.) **24** (1960), 279 - 281.

[229] Kaplansky, I.: Commutative Rings. Allyn and Bacon, Boston, Massachusetts, 1969.

[230] Kelly, P. H. and M. D. Larsen: Valuation rings with zero divisors. Proc. Amer. Math. Soc. **30** (1971), 426 - 430.

[231] Kennedy, R.: Krull rings. Pac. J. Math. **89** (1980), 131 - 136.

[232] Kirby, D.: Components of ideals in a commutative ring. Ann. Mat. Pura Appl. (4) **71** (1966), 109 - 125.

[233] Kirby, D.: Closure operations on ideals and submodules. J. London Math. Soc. **44** (1969), 283 - 291.

[234] Kirby, D.: Integral dependence and valuation algebras. Proc. London Math. Soc. (3) **20** (1970), 79 - 100.

[235] Kneser, H.: Eine direkte Ableitung des Zornschen Lemmas aus dem Auswahlaxiom. Math. Z. **53** (1950), 110 - 113.

[236] Kobayashi, Y. and M. Moriya: Eine hinreichende Bedingung für die eindeutige Primfaktorzerlegung der Ideale in einem kommutativen Ring. Proc. Imp. Acad. Tokyo **17** (1941), 134 - 138.

[237] Krause, U.: On monoids of finite real character. Proc. Amer. Math. Soc. **105** (1989), 546 - 554.

[238] Kronecker, L.: Grundzüge einer arithmetischen Theorie der ganzen algebraischen Größen. (Crelles) J. Reine Ang. Math. **92** (1882), 1 - 122.

[239] Krull, W.: Ein neuer Beweis für die Hauptsätze der allgemeinen Idealtheorie. Math. Ann. **90** (1923), 55 - 64.

[240] Krull, W.: Axiomatische Begründung der allgemeinen Idealtheorie. Sitzungsberichte der physikalisch-medizinischen Societät zu Er **56** (1924), 47 - 63.

[241] Krull, W.: Die verschiedenen Arten der Hauptidealringe. S. B. Heidelberger Akad. Wiss. 6 (1924), 1 - 16.

[242] Krull, W.: Über Multiplikationsringe. S. B. Heidelberger Akad. Wiss. **5** (1925), 13 - 18.

[243] Krull, W.: Die Theorie der allgemeinen Zahlringe. Math. Ann. **99** (1928), 51 - 70.

[244] Krull, W.: Idealtheorie in Ringen ohne Endlichkeitsbedingung. Math. Ann. **101** (1929), 729 - 744.

[245] Krull, W.: Idealtheorie. Springer, Berlin, Heidelberg, New York, 1. Auflage 1935, 2. Auflage 1968.

[246] Krull, W.: Über allgemeine Multiplikationsringe. Tôhoku Math. J. **41** (1935 - 36), 320 - 326.

[247] Krull, W.: *Beiträge zur Arithmetik kommutativer Integritätsbereiche II v-Ideale und vollständig ganz abgeschlossene Integritätsbereiche.* Math. Z. **41** (1936), 665 - 679.

[248] Krull, W.: *Zur Arithmetik der endlichen diskreten Hauptordnungen.* J. Reine Angew. Math. **189** (1951), 118 - 128.

[249] Krull, W.: *Zur Theorie der kommutativen Integritätsbereiche.* J. Reine Angew. Math. **192** (1953), 230 - 252.

[250] Krull, W.: *Zur Idealtheorie der unendlichen algebraischen Zahlkörper.* J. Sci. Hiroshima Univ. Ser. A **21** (1957/58), 79 - 88.

[251] Krull, W.: *Über Laskersche Ringe.* Rend. Circ. Mat. Palermo (2) **7** (1958), 155 - 166.

[252] Krull, W.: *Über einen Existenzsatz der Bewertungstheorie.* Abh. Math. Sem. Univ. Hamburg **23** (1959), 29 - 35.

[253] Krull, W.: *Ordnungsfunktionen und Bewertungen von Körpern.* Math. Z. **77** (1961), 135 - 148.

[254] Kummer, E. E.: *De numeris complexis, qui radicibus unitatis et numeris integris realibus constant.* Gratulationsschrift der Universität Breitau zur Jubelfeier der Universität Königsberg, 1844, s. auch (Crelles) J. Reine Angew. Math. **35** (1847), 319 - 326.

[255] Kummer, E. E.: *Zur Theorie der komplexen Zahlen.* Monatsber. Akad. Wiss. Berlin 1846, s. auch (Crelles) J. Reine Angew. Math. **35** (1847), 319 - 326.

[256] Kummer, E. E.: *Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen.* Zahlen in ihre Primfaktoren. (Crelles) J. Reine Angew. Math. **35** (1847), 327 - 367.

[257] Kummer, E. E.: *Beweis des Fermatschen Satzes der Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche Anzahl von Primzahlen λ.*. Monatsberichte, Akad. Wiss. Berlin 1847, 132 - 141 und 305 - 319.

[258] Kummer, E. E.: *Allgemeine Reciprocitätsgesetze für beliebig hohe Potenzreste.* Monatsberichte Akad. Wiss. Berlin 1850, 154 - 165.

[259] Kummer, E. E.: *Allgemeiner Beweis des Fermat'schen Satzes, daß die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zählern der ersten $(\lambda - 3)/2$ Bernoulli'schen Zahlen als Faktoren nicht vorkommen.* (Crelles) J. Reine Angew. Math. **40** (1850), 130 - 138.

[260] Kummer, E. E.: *Über die gaußischen Perioden der der Kreisteilung entsprechenden Congruenzwurzeln.* (Crelles) J. Reine Angew. Math. **53** (1857), 142 - 148.

[261] Landau, E.: *Einführung in die elementare und analytische Theorie der algebraischen Zahlen.* Chelsea Publishing Company New York 1949, Nachdruck, erste Auflage 1917.

[262] Lasker, E.: *Zur Theorie der Moduln und Ideale.* Math. Ann. **60** (1905), 20 - 116.

[263] Larsen, M. D.: *Equivalent conditions for a ring to be a P-ring and a note on flat overrings.* Duke Math. J. **34** (1967), 273 - 280.

[264] Larsen, M. D.: *A generalization of almost Dedekind domains.* J. Reine Angew. Math. **245** (1970), 119 - 123.

[265] Larsen, M. D.: *Prüfer rings of finite character.* J. Reine Angew. Math. **247** (1971), 92 - 96.

[266] Larsen, M. D.: *Ideal theory in Prüfer rings with zero divisors.* J. Reine Angew. Math. **251** (1971), 76 - 80.

[267] Larsen, M. D. and P. J. McCarthy: *Overrings of almost multiplication rings.* J. Sci. Hiroshima Univ. Ser. A - I **31** (1967), 123 - 129.

[268] Larsen, M. D. and P. J. McCarthy: *Multiplicative Theory of Ideals.* Academic Press, New York and London, 1971.

[269] Lazard, M.: *Théorie des idéaux dans les anneaux de Dedekind.* Semig. A. Chatelet et P. Dubreil **2** (1961), 5 - 6.

[270] Lediaev, J. P.: *Relationship between Noether lattices and x-systems.* Acta Math. Acad. Sci. Hungar. **21** (1970), 323 - 325.

[271] Leonhardt, G.: *Beiträge zur Residuation.* Dissertation, Kassel 1995.

[272] Lettl, G.: *Subsemigroups of finitely generated groups with divisor theory.* Mh. Math. **106** (1988), 205 - 210.

[273] Lewis, W. J.: *The spectrum of a ring as a partially ordered set.* J. Algebra **25** (1973), 419 - 434.

[274] Lorentzen, H. B.: *Localization in x-Systems with Applications.* Thesis (in Norwegian). Osto 1968.

[275] Lorenzen, P.: *Abstrakte Begründung der multiplikativen Idealtheorie.* Math. Z. **45** (1939), 533 - 553.

[276] Lorenzen, P.: *Über halbgeordnete Gruppen.* Math. Z. **52** (1949), 483 - 526.

[277] Lorenzen, P.: *Teilbarkeitstheorie in Bereichen.* Math. Z. **55** (1952), 269 - 275.

[278] Smith P. F.: *On non-commutative AM-Rings.* Houston J. Math. **11** (1985), No. 3, 405 - 422.

[279] Low, G. M. and P. F. Smith: *Multiplication modules and ideals.* Comm. Algebra **18** (1990), no. 12, 4353 - 4375.

[280] Lucas, T.: *Some results on Prüfer rings.* Pac. J. Math. **124** (1986), 333 - 343.

[281] Malik, S., Mott J. L. and M. Zafrullah: *On t-invertibility.* Comm. Algebra **16** (1988), 149 - 170.

[282] Manis, M.: *Extension of valuation theory.* Bull. Amer. Math. Soc. **83** (1967), 735 - 736.

[283] Manis, M.: *Valuations on a commutative ring.* Proc. Amer. Math. Soc. **20** (1969), 193 - 198.

[284] Manis, M.: *Valuations on a commutative ring.* Proc. Amer. Math. Soc. **26** (1973), 249 - 272.

[285] Mannepalli, V. L.: *Multiplication semigroups.* Semig. For. **11** (1975/76), 310 - 327.

[286] Mannepalli, V. L.: *Multiplication semigroups* II. Semig. For. **12** (1976), 145 - 164.

[287] Mannepalli, V. L. and M. Satyanarayana: *Multiplication semigroups* III. Semig. For. **12** (1976), 165 - 175.

[288] Mannepalli, V. L. and M. Satyanarayana: *Monoids of Dedekind type.* Semig. For. **9** (1974), 19 - 27.

[289] Maranda, J. M.: *Factorization rings.* Canad. J. Math. **9** (1957), 597 - 623.

[290] Matsusita, K.: *Über ein bewertungstheoretisches Axiomensystem für die Dedekind-Noethersche Idealtheorie.* Japan. J. Math. **19** (1944), 97 - 110.

[291] McCarthy, P. J.: *Note on primary ideal decompositons.* Canad. J. Math. **18** (1966), 950 - 952.

[292] McCarthy, P. J.: *Note on abstract commutative ideal theory.* Amer. Math. Monthly **74** (1967), 706 - 707.

[293] McCarthy, P. J.: *Arithmetical rings and multiplicative lattices.* Ann. Mat. Pura Appl. **82** (1969), 267 - 274.

[294] McCarthy, P. J.: *The ring of polynomials over a von Neumann regular ring.* Proc. Amer. Math. Soc. **39** (1971), 43 - 45.

[295] Močkoř, J.: *Groups of Divisibility.* Mathematics and its Applications. D. Reidel Publishing Company Dordrecht-Boston-Lancaster 1983.

[296] Mori, Sh.: *Über Ringe, in denen die größten Primärkomponenten jedes Ideals eindeutig bestimmt sind.* J. Sci. Hiroshima Univ. Ser. A **1** (1931), 159 - 191.

[297] Mori, Sh.: *Minimale Primärideale eines Ideals.* J. Sci. Hiroshima Univ. Ser. A **2** (1932), 21 - 32.

[298] Mori, Sh.: *Axiomatische Begründung der Multiplikationsringe.* J. Sci. Hiroshima Univ. Ser. A **3** (1932), 45 - 59.

[299] Mori, Sh.: *Über eindeutige Reduktion in Ringen ohne Teilerkettenbedingung.* J. Sci. Hiroshima Univ. Ser. A **3** (1933), 275 - 318.

[300] Mori, Sh.: *Über allgemeine Multiplikationsringe* I. J. Sci. Hiroshima Univ. Ser. A **4** (1934), 1 - 26.

[301] Mori, Sh.: *Über allgemeine Multiplikationsringe* II. J. Sci. Hiroshima Univ. Ser.A **4** (1934), 99 - 109.

[302] Mori, Sh.: *Struktur der Multiplikationsringe.* J. Sci. Hiroshima Univ. Ser. A **16** (1952), 1 - 11.

[303] Mori, Sh.: *Über die Idealtheorie der Multiplikationsringe.* J. Sci. Hiroshima Univ. Ser. A **19** (1956), 429 - 437.

[304] Mott, J. L.: *Equivalent conditions for a ring to be a multiplication ring.* Canad. J. Math. **16** (1964), 429 - 434.

[305] Mott, J. L.: *On the complete integral closure of an integral domain of Krull type.* Math. Ann. **173** (1967), 238 - 240.

[306] Mott, J. L.: *Multiplication rings containing only finitely many minimal prime ideals.* J. Sci. Hiroshima Univ. Ser. A - I **33** (1969), 73 - 83.

[307] Mott, J. L.: *The group of divisibility and its applications.* Lecture Notes in Math. **311** (1973), 1 - 15.

[308] Mott, J. L.: *Groups of Divisibility: A Unifying Concept for Integral Domains and Partially Ordered Groups.* Lattice-Ordered Groups, Advances and Techniques. Mathematics and its Applications, A.M. Glass and W. Charles Holland ed. Kluwer Academic Publishers. Dordrecht/Boston/London. (1989), 80 - 104.

[309] Mott, J. L. and M. Zafrullah: *On Krull domains.* Arch. Math. (Basel) **56** (1991), no. 6, 559 - 568.

[310] Mott, J. L. and M. Zafrullah: *On Prüfer v-multiplication domains.* Manuscripta Math. **35** (1981), 1 - 26.

[311] Murata, K.: *Primary decomposition of elements in compactly generated integral multiplicative lattices.* Osaka J. Math. **7** (1970), 97 - 115.

[312] Murata, K.: *Generalized prime elements in a compactly generated S-semigroup I.* Proc. Japan Acad. **49** (1973), 134 - 139.

[313] Murata, K.: *Generalized prime elements in a compactly generated S-semigroup II.* Proc. Japan Acad. **49** (1973), 310 - 313.

[314] MURATA, K.: *On Submodules over an Asano order of a ring.* Proc. Japan Acad. **50** (1974), 584 - 588.

[315] MURATA, K.: *A divisor theory and integrally closed orders.* Alg. Univ. **16** (1983), 167 - 177.

[316] MURATA, K.: *On divisor theory and its divisor class group in semi-groups.* Proc. 9th symp., Naruto City 1985, (1986) 9 - 15.

[317] MURDOCH, D. C.: *Contributions to noncommutative ideal theory.* Canad. J. Math. **4** (1952), 43 - 57.

[318] NAKANO, N.: *Über die Umkehrbarkeit der Ideale im Integritätsbereiche.* Proc. Imp. Acad. Tokyo **19** (1943), 230 - 234.

[319] NAKANO, N.: *Über den Fundamentalsatz der Idealtheorie in unendlichen algebraischen Zahlkörpern.* J. Sci. Hiroshima Univ. Ser. A **15** (1952), 171 - 175.

[320] NAKANO, N.: *Idealtheorie in einem speziellen unendlichen algebraischen Zahlkörper.* J. Sci. Hiroshima Univ. Ser. A **16** (1953), 425 - 439.

[321] NAKANO, N.: *Über idempotente Ideale in unendlichen algebraischen Zahlkörpern.* J. Sci. Hiroshima Univ. Ser. A **17** (1953), 11 - 20.

[322] NAKANO, N.: *Über die kürzeste Darstellung der Ideale in unendlichen algebraischen Zahlkörpern.* J. Sci. Hiroshima Univ. Ser. A **17** (1953), 21 - 25.

[323] NAKANO, N.:*Idealtheorie in unendlichen algebraischen Zahlkörpern.* Proc. Int. Symp. on Algebra and Number Theory, Tokyo and Nikko (1955), 249 - 251. (Science Council of Japan, Tokyo, 1956)

[324] NAKANO, N.: *Über den Primäridealquotienten in unendlichen algebraischen Zahlkörpern.* J. Sci. Hiroshima Univ. Ser. A **18** (1955), 257 - 269.

[325] NAKANO, N.: *Idealtheorie in Stiemkeschen Körpern.* J. Sci. Hiroshima Univ. Ser. A Math. **18** (1955), 271 - 287.

[326] NAKANO, N.: *Über die Multiplikativeigenschaft der Ideale in unendlichen algebraischen Zahlkörpern.* J. Sci. Hiroshima Univ. Ser. A **19** (1956), 439 - 455.

[327] NAKANO, N.: *A theorem on lattice ordered groups and its applications to valuation theory.* Math. Z. **83** (1964), 140 - 146.

[328] Naoum, A. G. and K. R. Sharaf: *A note on the dual of a finitely generated multiplication module.* Beiträge Algebra Geom. **27** (1988), 5 - 11.

[329] Naoum, A. G. and K. R. Sharaf: *On the dual of a finitely generated multiplication module II.* Beiträge Algebra Geom. **27** (1988), 83 - 88.

[330] Naoum, A. G.: *Flat modules and multiplication modules.* Period. Math. Hungarica **21** (1990), no. 4, 309 - 317.

[331] Naoum, A. G.: *On the module of homomorphisms on finitely generated multiplication modules I.* Period. Math. Hungarica **22** (1991), no. 2, 97 - 105.

[332] Naoum, A. G.: *On the module of homomorphisms on finitely generated multiplication modules II.* Period. Math. Hungarica **22** (1991), no. 3, 153 - 160.

[333] Narkiewicz, W.: *Numbers with unique factorization in an algebraic number field.* Acta Arith. **21** (1972), 313 - 322.

[334] Narkiewicz, W.: *Finite abelian groups and factorization problems.* Coll. Math. **42** (1979), 319 - 330.

[335] Neuman, J. von: *Zur Prüferschen Theorie der idealen Zahlen.* Acta Litt. Sci. Szeged **2** (1926), 193 - 227.

[336] Noether, Emmy.: *Die allgemeinsten Bereiche aus ganzen transzendenten Zahlen.* Math. Ann. **77** (1915), 103 - 128.

[337] Noether, Emmy.: *Idealtheorie in Ringbereichen.* Math. Ann. **83** (1921), 23 - 67.

[338] Noether, Emmy.: *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern.* Math. Ann. **96** (1927), 26 - 61.

[339] Northcott, D. G.: *A note on the intersection theorem for ideals.* Proc. Cambridge Philos. Soc. **48** (1952), 366 - 367.

[340] Northcott, D. G.: *A note on classical ideal theory.* Proc. Cambridge Philos. Soc. **51** (1955), 766 - 767.

[341] Ohm, J.: *Primary ideals in Prüfer domains.* Canad. J. Math. **18** (1966), 1024 - 1030.

[342] Ohm, J.: *Integral closure and* $(x, y)^n = (x^n, y^n)$. Monatsh. Math. **71** (1967), 32 - 39.

[343] OHM, J. and P. VICKNAIR: *Monoid rings which are valuation rings.* Comm. Algebra **11** (1983), 1355 - 1368.

[344] PAPERT, D.: *A representation theory for lattice-groups.* Proc. London Math. Soc. **12** (1962), 100 - 120.

[345] PAPICK, IRA J.: *A note on Prüfer v-multiplication domains.* Boll. Un. Math. Ital. **1** (1982), 133 - 136.

[346] PERIĆ, V.: *Eine Bemerkung zu den invertierbaren und fastinvertierbaren Idealen. Arch. Math.* **15** *(1964), 415 - 417.*

[347] PERIĆ, V.: *Zu den fastinvertierbaren Idealen in kommutativen Ringen und Halbgruppen.* Glasnik Mat. Ser. III **1** (1966), 139 - 146.

[348] PERIĆ, V.: *Eine Charakterisierung der S-Komponenten der Ideale und der Halbgruppe* $(\mathbf{R}_S, \cap)$. Publ. Inst. Math. (Beograd) **7** (1967), 93 - 98.

[349] PERIĆ, V.: *Fastinvertierbare Primideale der kommutativen Ringe.* Publ. Inst. Math. (Beograd) **7** (1967), 99 - 109.

[350] PIRTLE, E. M.: *Families of valuations and semigroups of fractionary ideal classes.* Trans. Amer. Math. Soc. **144** (1969), 427 - 440.

[351] PRÜFER, H.: *Neue Begründung der algebraischen Zahlentheorie.* Math. Ann. **94** (1925), 198 - 243.

[352] PRÜFER, H.: *Untersuchungen über Teilbarkeitseigenschaften in Körpern.* J. Reine Angew. Math. **168** (1932), 1 - 36.

[353] RACHUNEK, J.: *Prime subgroups of ordered groups.* Czech. Math. J. **24** (1974), 541 - 551.

[354] RATLIFF, L. J.: *Δ-closures of ideals and rings.* Trans. Amer. Math. Soc. **313** (1989), 221 - 247.

[355] REES, D.: *A note on valuations associated with a local domain.* Proc. Cambridge Philos. Soc. **51** (1955), 252 - 253.

[356] REES, D.: *Valuations associated with a local ring* I. Proc. London Math. Soc. **5** (1955), 107 - 128.

[357] REES, D.: *Valuations associated with a local ring* II. J. London Math. Soc. **31** (1956), 228 - 235.

[358] REES, D.: *Valuations associated with ideals.* J. London Math. Soc. **31** (1956), 221 - 228.

[359] Rees, D.: *Valuations associated with ideals* II. Proc. London Math. Soc. (3) **6** (1956), 161 - 174.

[360] Rees, D.: *Two classical theorems of ideal theory.* Proc. Cambridge Philos. Soc. **52** (1956), 155 - 157.

[361] Rees, D.: *filtrations as limits of valuations.* J. London Math. Soc. **32** (1957), 97 - 102.

[362] Ribenboim, P.: *Modules sur un anneau de Dedekind.* Summa Brasil. Math. **3** (1952), 21 - 36.

[363] Ribenboim, P.: *Sur une conjecture de Krull en theorie des valuations.* Nagoya Math. J. **9** (1955), 87 - 973.

[364] Ribenboim, P.: *Sur une note de Nagata relative á un problème de Krull.* Math. Z. **64** (1956), 159 - 168.

[365] Ribenboim, P.: *Sur la theorie des idéaux dans certains anneaux de type infini.* An. Acad. Brasil Ci. **28** (1956), 21 - 39.

[366] Ribenboim, P.: *Anneaux normaux réels à caractère fini.* Summa Brasil. Math. **3** (1956), 213 - 253.

[367] Ribenboim, P.: *Un théorème sur les anneaux primaires et complètement intégralement clos.* Math. Ann. **130** (1956), 399 - 404.

[368] Ribenboim, P.: *Le théorème d'approximation pour les valuations de Krull.* Math. Z. **68** (1957), 1 - 18.

[369] Ribenboim, P.: *Sur les groupes totalement ordonnés et l'arithmetique des anneaux de valuation.* Summa Brasil. Math. **4** (1958), 1 - 64.

[370] Ribenboim, P.: *On the theory of Krull valuations.* Bol. Soc. Mat. Sao Paulo **11** (1959), 1 - 106.

[371] Ribenboim, P.: *Remarques sur le prolongement des valuations de Krull.* Rend. Circ. Mat. Palermo (2) **8** (1959), 152 - 159.

[372] Ribenboim, P.: *Anneaux de Rees intégralement clos.* J. Reine Angew. Math. **204** (1960), 99 - 107.

[373] Ribenboim, P.: *Sur la théorie du prolongement des valuation de Krull.* Math. Z. **75** (1961), 449 - 466.

[374] Ribenboim, P.: *On ordered modules.* J. Reine Angew. Math. **225** (1967), 120 - 146.

[375] Ribenboim, P.: *Corrections to my paper "On ordered modules".* J. Reine Angew. Math. **238** (1969), 132 - 134.

[376] Robinson, A.: *Non-standard theory of Dedekind rings.* Proc. Kon. Nederl. Akad. Weten. **70** (1967), 444 - 452.

[377] Roitman, M.: *On Mori domains and commutative rings with $CC^{\perp}$ I.* J. Pure Appl. Algebra **56** (1989), 247 - 268.

[378] Roitman, M.: *On Mori domains and commutative rings with $CC^{\perp}$ II.* J. Pure Appl. Algebra **61** (1989), 53 - 77.

[379] Roitman, M.: *On the complete integral closure of a Mori domain.* J. Pure Appl. Algebra **66** (1990), no. 1, 55 - 79.

[380] Rotman, J. J.: *Mixed modules over valuation rings.* Pacific J. Math. **10** (1960), 607 - 623.

[381] Rotman, J. J. and T. Yen: *Modules over a complete discrete valuation ring.* Trans. Amer. Math. Soc. **98** (1961), 242 - 254.

[382] Rubin, H. and J. E. Rubin: *Equivalents of the axiom of choice.* Studies in Logic and the Foundations of Mathematics. North-Holland Publishing Co., Amsterdam-London, xxiii+134 pp., 1970

[383] Sakuma, M.: *Existence theorems of valuations centered in a local domain with preassigned dimension and rank.* J. Sci. Hiroshima Univ. Ser. A **2** (1957/58), 61 - 67.

[384] Samuel, P.: *On the unique factorization rings.* Illinois J. Math. **5** (1961), 1 - 17.

[385] Samuel, P.: *Sur les anneaux factoriels.* Bull. Soc. Math. France **89** (1961), 155 - 173.

[386] Satyanarayana, M.: *Commutative semigroups in which primary ideals are prime.* Math. Nach. **48** (1971), 107 - 111.

[387] Scholz, A.: *Zur Idealtheorie in unendlichen algebraischen Zahlkörpern.* J. Reine Angew. Math. **185** (1943), 113 - 126.

[388] Seidenberg, A.: *Valuation ideals in polynomial rings.* Trans. Amer. Math. Soc. **57** (1945), 387 - 425.

[389] Sheldon, P.: *How changing $D[[X]]$ changes its quotient field.* Trans. Amer. Math. Soc. **199** (1971), 233 - 244.

[390] Sheldon, P.: *Prime ideals in GCD-domains.* Can. J. Math **26** (1974), 98-107.

[391] Shores, T.: *On generalized valuation rings.* Mich. Math. J. **21** (1974), 405-409.

[392] Skula, L.: *Divisorentheorie einer Halbgruppe.* Math. Z. **114** (1970), 113-120.

[393] Smith, P. F.: *Some remarks on multiplication modules.* Arch. Math. (Basel) **50** (1988), no. 3, 223 - 235.

[394] Smith, P. F., T. Ukegawa and N. Umaya: *On Non-commutative Noetherian Multiplication Rings.* Math. Sem. Notes, Kobe University **11**, (1983), 259 - 276.

[395] Smith, St.: *Fermat's last theorem and Bézout's theorem in GCD domains.* J. Pure Appl. Algebra **79**, (1992), no. 1, 63 - 85.

[396] Snapper, E.: *Completely primary rings* I. Ann. of Math. (2) **52** (1950), 666 - 693.

[397] Snapper, E.: *Completely primary rings* II. *Algebraic and transcendental extensions.* Ann. of Math. (2) **53** (1951), 125 - 142.

[398] Snapper, E.: *Completely primary rings* III. *Imbedding and isomorphism theorems.* Ann. of Math. (2) **53** (1951), 207 - 234.

[399] Snapper, E.: *Completely primary rings* IV. *Chain conditions.* Ann. of Math. (2) **55** (1952), 46 - 64.

[400] Sono, M.: *On congruences I.* Mem. Coll. Sci. Kyoto **2** (1917), 203 - 226.

[401] Sono, M.: *On congruences II.* Mem. Coll. Sci. Kyoto **3** (1918), 113 - 149.

[402] Storrer, H. H.: *A characterization of Prüfer rings.* Canad. Math. Bull. **12** (1969), 809 - 812.

[403] Szpiro, L.: *Fonctions d'ordre et valuations.* Bull. Soc. Math. France **94** (1966), 301 - 311.

[404] Tschebotarev, M.: *Neue Begründung der Idealtheorie (nach Zolotarev).* Bull. Soc. Phys.-Math. Kasan **2** (1925), 1 - 14.

[405] Ukegawa, T.: *Some properties of non-commutative multiplication rings.* Proc. Japan Acad. **54** A (1978), 279 - 284.

[406] Ukegawa, T.: *On the unique maximal idempotent ideals of non-commutative.* multiplication rings. Proc. Japan Acad. **55** A (1979), 132 - 135.

[407] Ukegawa, T.: *Left noetherian multiplication rings.* Osaka J. Math. **17** (1980), 449 - 453.

[408] Ukegawa, T.: *On M-rings and general ZPI-rings.* Semigroup theory and its related subjects. Proc. of the 4. Symposium, Yamaguchi (1980), 112 - 116.

[409] Ukegawa, T. and N. Umaya: *On a Theorem of Asano and some related Results of Cohen.* Mathematics Seminar Notes **10** (1982), 609 - 617.

[410] Ukegawa, T.: *Some remarks on M-Rings.* Math. Japonica **28** issue 2 (1983), 195 - 203.

[411] Ukegawa, T. and N. Umaya: *Supplementary Remarks: 'On a Theorem of Asano and some related Results of Cohen'.* Mathematics Seminar Notes **11** (1983), 133 - 137.

[412] Underwood, D. H.: *On some uniqueness question in primary representations of ideals.* J. Math. Kyoto Univ. **9** (1969), 69 - 94.

[413] Viswanathan, T. M.: *Ordered modules of fractions.* J. Reine Angew. Math. **235** (1969), 78 - 107.

[414] Viswanathan, T. M.: *Generalization of Hölder's theorem to ordered modules.* Canad. J. Math. **21** (1969), 149 - 157.

[415] Waerden, van der, B. L.: *Eine Verallgemeinerung des Bézout'schen Theorems.* Math. Ann. **99** (1928), 497 - 541.

[416] Waerden, van der, B. L.: *Zur Produktzerlegung der Ideale in ganz-abgeschlossenen Ringen.* Math. Ann. **101** (1929), 293 - 308.

[417] Waerden, van der, B. L.: *Zur Idealtheorie der ganz-abgeschlossenen Ringe.* Math. Ann. **101** (1929), 309 - 312.

[418] Waerden, van der, B. L.: *Algebra II.* , etwa 5. Auflage. Springer, Berlin-Heidelberg-New York, 1967.

[419] Ward, M.: *Residuation in structures over which a multiplication is defined.* Duke Math. J. **3** (1937), 627 - 636.

[420] Ward, M.: *Residuated distributive lattices.* Duke Math. J. **6** (1940), 641 - 651.

[421] Ward, M. and R. P. Dilworth: *Residuated lattices.* Trans. Amer. Math. Soc. **45** (1939), 335 - 354.

[422] Ward, M. and R. P. Dilworth: *The lattice theory of ova.* Ann. Math. **40** (1939), 600 - 608.

[423] Weber, H.: *Lehrbuch der Algebra.* Vieweg, Braunschweig, 1895, 1896; Nachdruck Chelsea, New York, 1962, 1979.

[424] WEYL, H.: *Algebraic Theory of Numbers.* Princeton University Press, Princeton, 1940, 1951.

[425] WOOD, C. A.: *Commuative rings for which each proper homomorphic image is a multiplication ring.* J. Sci. Hiroshima Univ. Ser. A - I **33** (1969), 85 - 94.

[426] WOOD, C. A.: *On general Z. P. I.-rings.* Pacific J. Math. **30** (1969), 837 - 846.

[427] YOSHIDA, M. and M. SAKUMA: *A note on semilocal rings.* J. Sci. Hiroshima Univ. Ser. A **17** (1953), 181 - 184.

[428] YOSHIDA, M. and M. SAKUMA: *On integrally closed Noetherian rings.* J. Sci. Hiroshima Univ. Ser. A **17** (1954), 311 - 315.

[429] ZAFRULLAH, M.: *On generalized Dedekind domains.* Mathematika **33** (1986), 285 - 295.

[430] ZAFRULLAH, M.: *Two characterizations of Mori domains.* Math. Japon. **33** (1988), no. 4, 645 - 652.

[431] ZAFRULLAH, M.: *Flatness and invertibility of an ideal.* Comm. Algebra **18** (1990), no. 7, 2151 - 2158.

[432] ZAFRULLAH, M.: *Well behaved prime t-ideals.* J. Pure Appl. Algebra **65** (1990), no. 2, 199 - 207.

[433] ZARISKI, O. and P. SAMUEL: *Commutative Algebra, Vol. I.* Van Nostrand-Reinhold, Princeton N.J., 1958.

[434] ZELINSKY, D.: *Topological characterization of f ields with valuations.* Bull. Amer. Math. Soc. **54** (1948), 1145 - 1150.

[435] ZOLOTAREV, G.: *Théorie des nombres entiers complex avec une application au calcul intégral.* Bull. Acad. Sci. Petersburg 1874.

[436] ZORN, M.: *A remark on a method in transfinite algebra.* Bull. Amer, Math. Soc. **41** (1935), 667 - 670.

[437] ZYGLINSKI, E.: *Zur Begründung der Idealtheorie.* C. R. Acad. Sci. Varsovie **24** (1932), 87 - 92.

Index

algebra
  boolean, 44, 61, 71, 180
algebraic, 85
AML
  divisor -, 87
    left, 86
  multiplication, 175
  noetherian, 88
  normal, 171
    hyper -, 169
  ringlike, 169
archimedean, 25, 88, 186
  hyper -, 159
arithmetic
  ideal, 29
  ring, 29
arithmetical, 122
associated, 33
atom, 233

basis, 86
  fixed, 23
bound, 53

cancellable
  0 -, 172
cancellative, 71, 212
  0 -, 71, 178
  P -, 157
chain, 53, 99
  ascending, 99
    condition, 42
  descending
    condition, 112
  maximal, 63
chain condition, 42
character, 47
  finite, 19, 47, 77
characteristic, 31
closed, 9
  integrally, 9
    completely, 213
  under multiplication, 23
co-maximal , 163
coded, 11
coefficient, 8
  integral algebraic -, 8
combination
  linear, 82
compact, 85
comparable, 53
complement
  set theoretical, 67
complemented, 61
  relatively, 61
complete
  conditionally, 69
completion
  of a ring, 31
composition
  direct, 30

condition
- left Prüfer, 24
- Mori, 24

congruence, 7, 16
- class, 7
- permutable, 115

conjugated, 8
cover, 63
cube
- lattice -, 26

decomposable, 34
decomposition, 39, 67
- canonical, 208
- direct, 39
- irredundant, 36
- subdirect, 178, 188

Dedekindian, 17
depth, 109
- of a prime P, 109

determinants, 8
diagram, 61
diamond, 62
dimension
- in algebraic geometry, 109
- Krull , 109

dimensional
- r -, 31

distributive, 16
divisibility, 32
divisor, 13, 23, 32, 86, 87, 96
- greatest common, 32
- left, 24, 86, 96
- prime, 25
- proper, 32
- zero, 26, 32, 186

domain, 5, 41
- Bézout, 11
- Dedekind, 13
- factorial, 30
- integral, 15
- Krull, 20, 21
- Mori, 21, 138
- number, 5, 29, 72
- Prüfer, 15
- UF -, 19

dual
- self -, 58

DV-AML
- semiprime, 51

element
- - free, 17, 24
- fixing, 122, 177
- maximal, 99
- principal, 23, 165, 167
  - join -, 165
  - meet -, 165
- residue, 99

elements
- orthogonal, 48

encode, 67
equivalent, 32
exponent, 11
extension
- 0-monoid, 71
- *d*-ideal -, 19
- *d*-monoid, 128
- exponent -, 19
- multiplicative -, 7
- normal
  - |-normal, 127
- Prüfer, 127

factorial
  semi -, 36
factorization
  prime, 11, 72
    unique, 7
  unique, 5, 31
field, 66
  agebraically closed, 32
  function, 10
  perfect, 31
  residue, 31
filter, 26
  m -, 22, 75
  order, 67, 74
    principal, 67
function, 8
  complex
    infinite, 110
  elementary symmetrical -, 8

generated, 11
  1-generated, 19
  2-generated, 15
  finitely, 11, 13, 213
generator
  compact, 23
geometry
  convex, 222
global, 71
group, 33
  d-group
    theorem, 19
  v-group
    theorem, 19
  abelian, 60
  dual, 17, 58
  semi -, 22
  sub -, 60
groupoid, 16
Gruppensatz, 10

height
  of a prime P, 109
  of an A, 109
holoid, 216
homomorphism
  ideal, 101
hull, 68

ideal, 5, 9, 25, 77
  ϕ-, 73
  c-, 74
  t-, 30, 46, 80
  v-, 17, 30, 46, 80
    fractional, 219
  x-, 20
  arithmetic, 77
    v-, 83
  Dedekindian, 46
  fractional, 229
  integral, 229
  lattice, 22
  maximal, 54
    unique, 31
  monoid, 87
  multiplicative, 22
  order, 21
    principal, 67
  primary, 14
  prime factorization, 10
  principal, 11, 23, 34, 73, 85, 165
  quotient, 90
  Rees, 21
  semilattice, 68

semiring, 74
structure, 23
theory, 5, 44, 72
abstract, 30
identity, 5, 71, 74
- root
p-th primitive -, 5
IDM
DV -, 185
normal, 122
image, 33
homomorphic, 19, 33
pre -, 40
inclusion., 67
indecomposable, 202
injective, 64
integer, 87
integral, 13
- completeness, 13
almost -, 18
interval, 53
invertible, 16, 229
irreducible, 33
irredundant
decomposition
prime-, 38
isotone, 64
isotonicity, 59

join, 57

kernel, 106, 107, 182
of an element, 173
of an ideal, 30

lattice, 23, 39, 58
m -, 86
- cube, 188
- group
- cone, 75, 157, 166
algebraic m -, 16, 24
boolean, 61
complemented, 61
complete, 70
complete m -, 23
distributive, 59, 75
ideal
distributive, 115
modular, 60, 100
semi -, 22, 85
inf -, 57
sup -, 57
sub -
forbidden, 62
Lemma
Divisor, 95
length, 109
finite, 64
of a chain, 63
of a prime chain, 109
limit, 53
localization, 15, 24, 26, 101, 104, 105

matrix, 66
maximal, 53, 99
maximum, 61
meet, 57
minimum, 61
module, 219, 228
monoid, 17, 21, 26, 33, 71
0 -, 71
cancellative, 17
commutative, 33
divisibility, 222
ideal

AP -, 186
archimedean, 178
normal, 171
Prüfer, 171
Krull, 21, 27
lattice ordered, 188
Mori, 212
Prüfer, 211
reduced, 127
valuation, 125
with zero, 17
multiple, 32
lowest common, 32
proper, 32

neighbour, 64
nilpotent, 177
noetherian, 88
normal, 124
d-normal, 124
t-normal, 124
hyper -, 25, 108
normal|-, 233
number, 5
algebraic, 8
ideal complex, 5, 7
integral, 7
numbers
relatively prime, 6

operator, 100
closure, 24, 73, 102
ideal, 73
order
ideal, 67
partial, 34
orthogonal, 87

pentagon, 62
point
regular, 31
simple, 31
smooth, 31
polynomial, 8
irreducible
normed, 8
normed, 8
primary, 97
P -, 97
special, 196
prime, 29, 33, 97, 139
completely, 33, 97
minimal, 14
relatively, 32, 41, 87
semi -, 33
prime factor, 11
ideal, 11
principal
weak meet, 166
problem
Mori, 25
Prüfer, 24
product
complex, 177
direct, 179
property
archimedean, 205
Mori, 26
Noether, 44, 178, 180
Prüfer, 26, 169

quotient, 90
left ideal, 25
right, 90
right ideal, 25

radical, 14, 98, 183
rank
  of the Jacobian matrix, 31
regular
  von Neumann, 43, 179
relation, 33
  congruence, 33
  divisibility, 8
  order, 16
residual, 90
  right, 90
residuation, 90
residue, 99
  class, 99
rest product, 208
ring, 8, 23, 61
  v-multiplication, 22
  AM -, 13
  arithmetical, 22
  Bézout, 115
  commtative
    with identity, 32
  factorial, 24, 29, 42
  formal power series, 31
  GCD -, 45
  Krull, 22
  local, 31
  multiplication, 13
    almost, 26
  Prüfer, 16
  principal t-ideal, 29, 47, 48
  principal v-ideal, 47, 48
  principal ideal , 45
  principal$d$-ideal, 47
  residue class, 19
  semi -, 23, 74
    cancellative, 166
  special primary, 30, 40, 41
  with identity, 54

scalar, 66
semigroup, 23, 71
  d -, 22
  d-ideal, 30
  t-ideal, 30
  v-ideal, 19
  divisibility, 22
  ideal, 19, 23, 30, 87
    classical, 157
  lattice, 22, 75
  of ideals, 87
  po -, 71
  Rees ideal, 21
sequence, 11
  composition -, 12
  of exponents, 11
set, 80
  po -, 53
  power -, 80
  totally ordered, 53
singularity
  resolution of, 32
space
  affine, 110
  affine n-, 31
  linear, 54, 61
structure
  AP -, 186
  Dedekind, 16
  ideal, 87
    hyper-normal , 167
    modular, 167
  Mori, 25, 138

multiplication, 138
Prüfer, 16, 116
left, 116
right, 116
successor, 99
sum
inner direct, 40, 41
orthogonal, 41
surjective, 64
system
d-ideal -, 20
v-ideal -, 12, 20
ideal -, 12, 25
of sets, 67
residue -, 24, 26

theorem, 18
dimension, 109
principal ideal, 109
ZPI -, 18
theory
divisor -, 20, 216, 222
transitive, 32
tuple
n -, 66

unit, 32
of a ring, 41

valuation, 12
value, 69
variety
algebraic, 31, 32
arithmetical, 115
irreducible
affine, 110

zero, 71

Residuationsstrukturen

Residuation Structures
to the memory of

Robert P. Dilworth
1914-1993

the great pioneer
of order, lattices, and residuation

researched and presented by

Bruno Bosbach

1994 - 1998 - 2004 - 2014

Inhalt

1 Ein Wort vorweg **5**

1.1 Einführung 5

2 Verbände **9**

2.1 Partialordnung und Verband 9

2.2 Distributive Verbände 11

2.3 Vollständige Verbände 14

2.4 Der boolesche Verband 15

2.5 Zur Verbandsgruppenarithmetik 20

3 Komplementäre Halbgruppen **23**

3.1 Einleitung 23

3.2 Axiomatik 25

3.3 Arithmetik und ideale Arithmetik 34

3.4 Komplementäre Halbgruppen und Ringe 48

3.5 Archimedizität und Vollständigkeit 52

3.6 Klassische Vertreter 54

3.7 Rechts-Kongruenzen 64

3.8 Kongruenzen 68

3.9 Repräsentierbarkeit 73

3.10 Polynome 74

3.11 States 76

3.12 Quotienten 77

3.13 Halbgruppenerweiterungen 83

3.14 Quotienten im links-komplementären Fall 86

3.15 Wann ist $\mathfrak{Q}$ invers? 93

3.16 Der idempotente Fall 95

3.17 Beispiele 96

4 Gleichungsbasen **99**
4.1 Zur rechtskomplementären Halbgruppe 99
4.2 Zur komplementären Halbgruppe 104
4.3 Eine „Muttergleichung“ 109
4.4 Der boolesche Sonderfall 114
4.5 Der Kegel-Sonderfall 115
4.6 Ausblick 121

5 Residuationsgruppoide **125**
5.1 Redukte 125
5.2 Allgemeine Clans 126
5.3 Symmetrische ℓ-Gruppenclans 134
5.4 Zur Struktur der Produkterweiterungen 136

6 ℓ-Gruppen-Redukte **143**
6.1 Vorbemerkungen 143
6.2 Arithmetik 144
6.3 Vom Kegel-Clan zum Kegel 149
6.4 Weiteres zur Produktalgebra 153
6.5 Vom Kegel zum Brick 156
6.6 Repräsentierbarkeit 159
6.7 Schwache Kegelalgebren 161
6.8 ℓ-Gruppen-Clans 164

7 Sup-Clans **173**
7.1 Vorbemerkungen 173
7.2 Arithmetik der DR-Gruppoide 174
7.3 Normalität 178
7.4 Sup-Clans 183
7.5 Der brouwersche und der boolesche Clan 191
7.6 Der boolesche 0-Abschluss 194

8 Verbandsgruppen-Verbände **197**
8.1 Verbände von ℓ-Gruppen-Kegeln 198
8.2 ℓ-Gruppen-Verbände 200

9 Kommutative Bricks **203**
9.1 Vorbemerkungen 203
9.2 Axiomatische Aspekte 204
9.3 Darstellungen 209
9.4 Vollständige Bricks 213
9.5 Würfelalgebren 218

10 Allgemeine Bricks **227**
10.1 GMV-Algebren 227
10.2 Die Relative Kürzungseigenschaft 229
10.3 Vom Brick zum Kegel – auf neuen Wegen 233
10.4 Zur Einbettung von Semiclans 237
10.5 Zur Einbettung kommutativer Bricks 244
10.6 Abschließende Bemerkungen 246

11 Teilbarkeits-Semiloops **249**
11.1 Einführung 249
11.2 d-Semiloops 252
11.3 Der Verbandsloop-Kegel 262
11.4 Die Kettenbedingung 268
11.5 Vollständige d-semiloops 269
11.6 Vervollständigung 273
11.7 Kongruenzen 279

12 Repräsentierbarkeit **283**
12.1 Zur Repräsentierbarkeit 284
12.2 Ein allgemeiner Darstellungssatz 284
12.3 Ein perspektivischer Hinweis 296

13 Jakubík-Ketten in lo-Gruppoiden **299**

14 Ideale – Linearität – Orthogonalität **309**
14.1 Ideale 310
14.2 Prime Ideale 311
14.3 Polaren 315
14.4 Filets und z-Ideale 318
14.5 Minimal prime Ideale 321

14.6 Direkte Faktoren 323
14.7 Lexikographische Erweiterungen 325
14.8 RNDV-Gruppoide mit einer Basis 331
14.9 Ortho-finite RNDV-Gruppoide 334
14.10 Projizierbare RNDV-Gruppoide 337

Kapitel 1

Ein Wort vorweg

Residuation ist der natürlichste Gegenspieler der Multiplikation und ist über einen Zeitraum von 80 Jahren in den verschiedensten Rollen und Situationen studiert worden, z.B. als verallgemeinertes Quotientenideal oder auch als verallgemeinerte Implikation.

1.1 Einführung

(1) Man betrachte das natürliche Intervall $\{O, \mathsf{I}\}$ oder auch das reelle Intervall $[0,1]$ bezüglich $a * b := b - \min(a,b)$.

(2) Man betrachte einen Ring und setze

$$\mathfrak{a} * \mathfrak{b} := \mathfrak{b} : \mathfrak{a}\,.$$

(3) Man betrachte die logische Implikation $\Rightarrow$ und setze

$$a * b := a \Rightarrow b\,.$$

(4) Man betrachte eine *po*-set mit Minimum 1 und setze

$$a * b \quad := \quad \begin{cases} 1 & \text{gdw.} \quad a \geq b \\ b & \text{gdw.} \quad a \not\geq b\,. \end{cases}$$

(5) Man betrachte eine Gruppe und setze

$$a * b := a^{-1}b.$$

(6) Man betrachte die Menge A aller Ordnungsautomorphismen einer Kette bezüglich der Komposition und punktweisen Maximum- und Minimumbildung. Dann bildet A eine verbandsgeordnete Gruppe, in englisch eine *lattice group,* kurz eine ℓ-Gruppe, d.h. eine Algebra $(A, \wedge, \vee, \cdot, ^{-1})$ des Typs $(2, 2, 2, 1)$, die bezüglich $\cdot$ den Gruppenbedingungen und bezüglich $\wedge, \vee$ den Verbandsbedingungen genügt und zudem das Gesetz der Isotonie

$$\text{(ISO)} \qquad a \le b \implies xay \le xby \ (\forall x, y)\,.$$

erfüllt. Definiere nun

$$a * b := 1 \vee a^{-1}b \qquad \text{and} \qquad a : b := ba^{-1} \vee 1\,.$$

(7) Betrachte einen Verbandsgruppenkegel und definiere

$$a * b := a\backslash(a \vee b) \qquad \text{and} \qquad a : b := (b \vee a)/a\,.$$

In jeder dieser Situationen ist eine „Residuation" erklärt, die auf dem Wege schlichter Zusatzforderungen außerordentlich starke Implikationen gewährleistet.

Wie fruchtbar Residuation und Multiplikation zu interagieren vermögen, wird evident durch das

Theorem: *Es gibt ein gemeinsames Muster einer 1-basigen Charakterisierung der booleschen'schen Algebra, des (abelschen) ℓ-Gruppenkegels, des abelschen ℓ-Loopkegels, der (abelschen) ℓ-Gruppe, der (abelschen) ℓ-Loop, nämlich*

$$\text{(F)} \qquad f_x \circ \Big\{\Big(\big(f_y \circ (a \circ (a * b)\,\Delta\,(b * a))\big) \circ c\Big)\,\Delta\, c\Big\} = b\,,$$

worin Δ in dem einen Falle die Bedeutung $(a * b) \circ (b * a)$ haben mag, während in einem anderen Falle Δ zu lesen ist als $:$, man vergleiche [21].
Das ständig wachsende Interesse an der Residuation erschließt sich eindrucksvoll aus einer Flut von Artikeln und den Monographien[67], [51] und [13].
Jedoch: obwohl diese Monographien tiefgreifend und inhaltsreich zugleich sind, decken sie nicht das gesamte weite Feld ab. So fehlt beispielsweise eine Berücksichtigung der „Industrie" der element-freien Idealtheorie, zu deren Studium schon Wofgang Krull angeregt hat.
In dieser Lecture Note stellen wir Ergebnisse des Autors zusammen, wie sie sich über eine längere Phase seiner Forschungsbemühungen eingestellt haben. Nicht hingegen gehen wir ein auf die Flut der Publikationen wie sie

sich eingestellt hat über Artikel und Monographien. Abschwächend könnte man sagen:

Vorgestellt werden nach einer Grundlegung der verbandstheoretischen Voraussetzungen ausschließlich Ergebnisse des Autors in neuer Komposition auf dem Feld der Residuation – zur Erleichterung für die Akteure.

Zitiert werden demzufolge lediglich die in den Arbeiten des Autors bereits zitierten Arbeiten.

Kapitel 2

Verbände

Ziel dieses Kapitels ist eine Einführung in die *Verbandstheorie* soweit sie einerseits als Basis für die späteren Kapitel vonnöten ist, zum anderen aber darüber hinaus so ausladend, dass der Leser einen Einblick in diese Theorie zu gewinnen vermag, soweit sie als Teil jeder mathematischen Allgemeinbildung anerkannt sein sollte.

2.1 Partialordnung und Verband

2. 1. 1 Definition. Eine Menge M zusammen mit einer auf ihr definierten 2-stelligen Relation Relation $\leq$ – kurz ein $(M, \leq)$ – heißt eine *partial geordnete Menge*, wenn $\leq$ für alle a, b, c den Bedingungen genügt:

(R) $$a \leq a$$

(S) $$a \leq b \leq a \implies a = b$$

(T) $$a \leq b \leq c \implies a \leq c\,.$$

Gilt darüber hinaus

$$\forall a, b\ \exists\, c =: sup(a, b) : (a \leq c \geq b) \quad \& \quad (a \leq x \geq b \Longrightarrow c \leq x)\,,$$

so heißt $(M, \leq)$ ein *sup-Halbverband.* Dual erklärt man den Begriff *inf-Halbverband.*
Schließlich heißt $(M, \leq)$ eine *Kette*, wenn je zwei Elemente *vergleichbar* sind.

Ist $(M, \leq)$ ein sup-Halbverband, so symbolisieren wir $\sup(a, b)$ auch mittels $a \vee b$, gelesen als a sup b bzw. als a *verbunden* b, und ist $(M, \leq)$ ein inf-Halbverband, so schreiben wir $\inf(a, b)$ auch als $a \wedge b$, gelesen als a inf b bzw. als a *geschnitten* b.

2. 1. 2 Lemma. *Ist* $(M, \leq)$ *ein* sup-*Halbverband, so haben wir:*

$$\begin{array}{llcl} (\mathrm{I}) & a \vee a & = & a \\ (\mathrm{K}) & a \vee b & = & b \vee a \\ (\mathrm{A}) & a \vee (b \vee c) & = & (a \vee b) \vee c\,. \end{array}$$

DENN: $\sup(a, b) = \sup(x, y)$ ist äquivalent zu $u \geq a, b \Longleftrightarrow u \geq x, y$. $\square$

2. 1. 3 Lemma. *Sei* $(H, \cdot)$ *ein Gruppoid, das* (I), (K) *und* (A) *erfüllt, also eine idempotente kommutative Halbgruppe. Dann liefert die Festsetzung*

$$a \leq b \;:\Longleftrightarrow\; a \cdot b = b$$

auf H *eine* sup-*abgeschlossene Partialordnung mit* $\sup(a, b) = ab$.

BEWEIS. Unter den gegebenen Umständen gelten:

(R) wegen $a \cdot a = a \rightsquigarrow a \leq a$,

(S) wegen $a \cdot b = b \;\&\; b \cdot a = a \Longrightarrow a = b \cdot a = a \cdot b = b$,

(T) wegen $a \cdot b = b \;\&\; b \cdot c = c \Longrightarrow a \cdot c = a \cdot b \cdot c = b \cdot c = c$

und

$a \cdot b = \sup(a, b)$, wegen $a, b \leq a \cdot b \;\&\; a \cdot x = x = b \cdot x \Longrightarrow (a \cdot b) \cdot x = x$. $\square$

Nach 2.1.2 und 2.1.3 können wir also jedem *sup-Halbverband* $(M, \leq)$ eine idempotente, kommutative Halbgruppe $\mathfrak{H}(M, \leq)$ zuordnen und jeder idempotenten kommutativen Halbgruppe $(H, \cdot)$ einen sup-Halbverband $\mathfrak{P}(H, \cdot)$. Tatsächlich erhalten wir sogar noch mehr, nämlich:

2. 1. 4 Proposition. *Die oben erklärten Operatoren* $\mathfrak{H}$ *und* $\mathfrak{P}$ *erfüllen:*

$$\begin{array}{lrcl} & \mathfrak{P}(\mathfrak{H}(M, \leq)) & \cong & (M, \leq) \\ \text{und} & \mathfrak{H}(\mathfrak{P}(H, \cdot)) & \cong & (H, \cdot)\,. \end{array}$$

Hiernach kommen wir zur Definition des *Verbandes,* einer Struktur, die schon von DEDEKIND unter dem Namen *Dualgruppe* eingeführt wurde, vgl. [99].

2. 1. 5 Definition. Sei $\mathfrak{V} := (\mathfrak{V}, \vee, \wedge)$ eine Algebra vom Typ (2,2). Dann heißt $\mathfrak{V}$ ein *Verband*, wenn gilt:

$$\begin{array}{llllll} (\mathrm{I}\vee) & a \vee a = a & \qquad & (\mathrm{I}\wedge) & a \wedge a = a \end{array}$$

$$\begin{array}{llll}
(\mathrm{K}\vee) & a \vee b = b \vee a & (\mathrm{K}\wedge) & a \wedge b = b \wedge a \\
(\mathrm{A}\vee) & a \vee (b \vee c) = (a \vee b) \vee c & (\mathrm{A}\wedge) & a \wedge (b \wedge c) = (a \wedge b) \wedge c \\
(\mathrm{V}\vee) & a \vee (b \wedge a) = a & (\mathrm{V}\wedge) & a \wedge (b \vee a) = a
\end{array}$$

Wie man unmittelbar erkennt, ist der Verband eine *selbstduale* Struktur. Das bedeutet: mit jeder Gleichung in $\mathfrak{V}$ gilt auch die durch *Umpolung* ($\vee \longmapsto \wedge, \wedge \longmapsto \vee$) gewonnene Gleichung.
Weniger evident ist die Tatsache, dass (I$\vee$) und (I$\wedge$) aus den übrigen Gleichungen *ableitbar* sind, was sich wie folgt ergibt:
Gelten etwa (V$\vee$),(K$\vee$),(V$\wedge$), so folgt

$$\begin{aligned}
a \wedge a &= a \wedge (a \vee (b \wedge a)) (\mathrm{V}\vee) \\
&= a \wedge ((b \wedge a) \vee a) (\mathrm{K}\vee) \\
&= a \qquad\qquad\qquad (\mathrm{V}\wedge)\,.
\end{aligned}$$

Weiter erhalten wir mittels (K$\vee$), (K$\wedge$), (V$\wedge$), (V$\vee$) die Äquivalenz:

$$a \wedge b = a \iff a \vee b = b\,. \tag{2.11}$$

Damit erhalten wir zusammenfassend die

2. 1. 6 Proposition. *Ist* $(V, \vee, \wedge)$ *ein Verband, so liefert die Festsetzung*

$$\begin{aligned}
a \leq b \;&:\iff a \wedge b = a \\
&(\iff a \vee b = b)
\end{aligned}$$

eine Partialordnung auf V *, die nach (2.11) den Regeln der Isotonie genügt:*

$$\text{(ISO)} \qquad \begin{aligned}
b \leq c \implies &a \wedge b \leq a \wedge c \\
\& \quad &a \vee b \leq a \vee c\,.
\end{aligned}$$

2.2 Distributive Verbände

Bei der großen Vielfalt an Verbänden sind wir natürlich interessiert an fundamentalen und zentralen Klassen von Verbänden. Solche Klassen werden hier jene Verbandsklassen sein, die in ein System von Mengen oder auch in ein System von Gruppen „hineinspielen".

Als natürliche Beispiele seien angeführt Verbände von Schaltungen bzw. Aussagen einerseits sowie Verbände von Unterräumen linearer Räume andererseits.

2. 2. 1 Definition. Ein Verband heißt *distributiv*, wenn er die beiden Distributivgesetze erfüllt:

$$(\mathrm{D}\wedge) \qquad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

$$(\mathrm{D}\vee) \qquad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c),$$

also nach (ISO), wenn er den beiden Abschätzungen genügt:

$$(\mathrm{D}'_\wedge) \qquad a \wedge (b \vee c) \leq (a \wedge b) \vee (a \wedge c)$$

$$(\mathrm{D}'_\vee) \qquad a \vee (b \wedge c) \geq (a \vee b) \wedge (a \vee c),$$

da die jeweils umgekehrte Vergleichsrelation stets erfüllt ist.

Man beachte, dass mit Blick auf die Selbstdualität des Verbandes auch die Distributivität – zunächst – selbstdual gefordert wird, während die distributive Kopplung etwa bei Ringen „unsymmetrisch" ist. Tatsächlich lässt sich diese selbstduale Forderung aber ohne Verlust reduzieren, wie der nächste Satz zeigt:

2. 2. 2 Proposition. $(V, \vee, \wedge)$ *ist schon dann distributiv, wenn eines der beiden oben genannten Gesetze* $(\mathrm{D}'_\wedge)$, $(\mathrm{D}'_\vee)$ *erfüllt ist.*

DENN: gelte $(\mathrm{D}'\wedge)$, dann folgt $(\mathrm{D}_\wedge)$ und wir erhalten mittels $(\mathrm{V}\vee)$

$$\begin{aligned} (a \vee b) \wedge (a \vee c) &= \big((a \vee b) \wedge a\big) \vee \big((a \vee b) \wedge c\big) \\ &= a \vee (a \wedge c) \vee (b \wedge c) \\ &= a \vee (b \wedge c)\,. \end{aligned} \qquad \square$$

Als ein halbverbandstheoretisches Äquivalent der Distributivität – unter vielen anderen – erhalten wir

2. 2. 3 Proposition. *Ein Verband* $\mathfrak{V}$ *ist genau dann distributiv, wenn er die nachfolgende Zerlegungsbedingung erfüllt:*

$$(\mathrm{Z}) \qquad x \leq a \vee b \Longrightarrow x = x_a \vee x_b \ \ (x_a \leq a, x_b \leq b)$$

BEWEIS. Wir bemerken vorweg, dass $\mathfrak{V}$ schon dann distributiv ist, wenn

$$a \leq b \vee c \Longrightarrow a = (a \wedge b) \vee (a \wedge c)\,,$$

erfüllt ist, was sich vermöge $a \wedge (b \vee c) = a = (a \wedge b) \vee (a \wedge c)$ einstellt. Gelte nun (Z). Dann folgt $a \leq b \vee c \Longrightarrow a = a_b \vee a_c$ mit $a_b \leq a \wedge b$ und $a_c \leq a \wedge c$, also $a \leq (a \wedge b) \vee (a \wedge c)$ und damit $a = (a \wedge b) \vee (a \wedge c)$, da $\geq$ stets gilt. Also gilt (Z) $\Longrightarrow$ (D):
Sei nun (D) erfüllt. Dann folgt (Z) unmittelbar *via*

$$x = x \wedge (a \vee b) = (x \wedge a) \vee (x \wedge b) =: x_a \vee x_b \ \ (x_a \leq a, x_b \leq b)\,. \qquad \square$$

2. 2. 4 Proposition. *Ist ein Verband $\mathfrak{V}$ distributiv, so erfüllt er die Implikation:*

$$\text{(CD)} \qquad \begin{array}{c} a \wedge x = a \wedge y \\ \& \\ a \vee x = a \vee y \end{array} \Longrightarrow x = y\,.$$

DENN: Aus der Prämisse folgt mittels der Verschmelzungs- und der Distributivgesetze:

$$\begin{aligned} x &= x \wedge (a \vee x) \\ &= x \wedge (a \vee y) \\ &= (x \wedge a) \vee (x \wedge y) \\ &= (y \wedge a) \vee (y \wedge x) \\ &= y \wedge (a \vee x) \\ &= y \wedge (a \vee y) \\ &= y\,. \end{aligned}$$

$\square$

2. 2. 5 Definition. Ein Verband $(V, \vee, \wedge)$ mit 0 als Minimum und 1 als Maximum heißt *komplementär*, wenn zu jedem x ein x' existiert mit

$$\text{(COM)} \qquad x \vee x' = 1 \quad \& \quad x \wedge x' = 0.$$

Ist diese Bedingung bezogen auf jedes *Hauptideal* $(\, x\,]$ erfüllt, so nennt man $\mathfrak{V}$ *abschnittskomplementär.*

2. 2. 6 Definition. Ist $\mathfrak{V}$ distributiv und komplementär, so heißt $\mathfrak{V}$ ein *boolescher Verband*, auch eine *boolesche Algebra.*

Das klassische Beispiel für den booleschen Verband ist der Potenzmengenverband.

2.3 Vollständige Verbände

2. 3. 1 Definition. Ein Verband $\mathfrak{V}$ heißt *vollständig*, wenn zu jedem $A \subseteq V$ unter allen *oberen Schranken* $s \geq a$ $(\forall a \in A)$ eine und damit die kleinste existiert, symbolisiert durch $\mathrm{Sup}(A)$ und bezeichnet als *obere Grenze.* . Dual erklärt man das Element $\mathrm{Inf}(A)$, bezeichnet als untere Grenze.

Ist $\mathfrak{V}$ vollständig, so bezeichnen wir $\mathrm{Inf}(V)$ mit 0 und $\mathrm{Sup}(V)$ mit 1. Offenbar ist ein Verband schon dann vollständig, wenn alle $\mathrm{Sup}(A)$ oder alle $\mathrm{Inf}(A)$ existieren. (Man beachte, dass die leere Menge $\square$ den Gleichungen $\mathrm{Sup}(\square) = \mathrm{Inf}(V)$ und $\mathrm{Inf}(\square) = \mathrm{Sup}(V)$ genügt).

2. 3. 2 Definition. Ein Verband heißt *bedingt vollständig*, wenn er *lückenfrei* ist, d. h., wenn jede *nach oben beschränkte* Teilmenge sogar *nach oben begrenzt*, also wenn zu jeder nach oben beschränkten Teilmenge das Supremum existiert. Ein bedingt vollständiger Verband heißt *vereinigungs-distributiv*, wenn er das Gesetz erfüllt:

(DV) $$s = \bigwedge a_i \ (i \in I) \implies x \vee s = \bigwedge (x \vee a_i) \ (i \in I) \ ,$$

Dual erklärt man den Begriff des *durchschnitts-distributiven* Verbandes, bzw. das Axiom (DS).
Schließlich heißt ein bedingt vollständiger Verband *vollständig distributiv,* wenn er (für jeweils existierende Grenzen) den Gesetzen genügt:

(DV1) $$\bigwedge_C \Big[\bigvee_{A_\gamma} a_{\gamma,\alpha}\Big] = \bigvee_\Phi \Big[\bigwedge_C a_{\gamma,\phi(\gamma)}\Big]$$

(DV2) $$\bigvee_C \Big[\bigwedge_{A_\gamma} a_{\gamma,\alpha}\Big] = \bigwedge_\Phi \Big[\bigvee_C a_{\gamma,\phi(\gamma)}\Big] \ ,$$

worin die γ die Menge C durchlaufen und Φ die Menge aller Abbildungen ϕ von C in die Vereinigungsmenge derjenigen A_γ darstellt, die der Bedingung $\phi(\gamma) \in A_\gamma$ genügen.

Offenbar ist jede bedingt vollständige Kette vollständig distributiv, insbesondere also auch vereinigungs- und durchschnitts-distributiv. Andererseits lässt sich zeigen, dass (DV1) und (DV2) voneinander unabhängig sind.
Denn: Man betrachte das System aller abgeschlossenen Punktmengen der Ebene. Ist dann C der Kreis $x^2 + y^2 = 1$ und bezeichnen wir mit C_k die Punktmengen $x^2 + y^2 \leq 1 - k^{-2}$ $(k \in \mathbf{N})$, so gilt im Verband aller abgeschlossenen Teilmengen der Ebene $C \cap \bigvee C_k = C \neq \emptyset = \bigvee (C \cap C_k)$.

2.4 Der boolesche Verband

Der Begriff des booleschen Verbandes wurde unter 2.2.6 erklärt. Über boolesche Algebren existiert eine Flut an Literatur, mehr als verständlich, wenn man bedenkt, dass hier *Ringe, Gruppen, topologische Räume* und *Verbände* zusammenspielen.
Uns geht es in diesem Kapitel lediglich um die Auffassung des Booleschen Verbandes als Ring. Hierzu vorweg eine Reduktion des Axiomensystems.

2. 4. 1 Proposition. *Eine Algebra* $\mathfrak{B} := (B, \wedge, \vee, ')$ *ist schon dann ein boolescher Verband, wenn sie den Gleichungen genügt:*

$$a \wedge b = b \wedge a \tag{B11}$$

$$a \vee b = b \vee a \tag{B12}$$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \tag{B21}$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \tag{B22}$$

$$a \wedge (b \vee b') = a \tag{B31}$$

$$a \vee (b \wedge b') = a \tag{B32}$$

BEWEIS. Wir beweisen zunächst die beiden Gleichungen:

$$a \wedge a' = b \wedge b' \tag{2.25}$$

$$a \vee a' = b \vee b'. \tag{2.26}$$

Wegen der $\wedge/\vee$ Dualität reicht es natürlich die Gleichung (2.25) zu beweisen, die sich wie folgt einstellt:

$$\begin{aligned} b \vee b' &= (b \vee b') \wedge (c \vee c') \\ &= (c \vee c') \wedge (b \vee b') \\ &= c \vee c' \end{aligned}$$

Hiernach bezeichnen wir $a \wedge a'$ mit 0 und $a \vee a'$ mit 1. Weiter lassen sich $(I, \wedge)$ und $(I, \vee)$ leicht bestätigen vermöge

$$\begin{aligned} a \wedge a &= (a \wedge a) \vee (a \wedge a') \\ &= a \wedge (a \vee a') \\ &= a \wedge 1 \\ &= a \end{aligned}$$

und der hierzu dualen Herleitung. Als nächstes verifizieren wir:

$$a \wedge 0 = a \tag{2.27}$$
$$a \vee 1 = 1 \tag{2.28}$$

via

$$\begin{aligned} a \wedge 0 &= (a \wedge 0) \vee 0 \\ &= 0 \vee (a \wedge 0) \\ &= (a \wedge a') \vee (a \vee 0) \\ &= a \wedge (a' \vee 0) \\ &= a \wedge a' \\ &= 0 \end{aligned}$$

Bevor wir zum alles entscheidenden Assoziativgesetz kommen, vorweg noch die beiden Verschmelzungsgesetze

$$a \wedge (b \vee a) = a \tag{V$\wedge$}$$
$$a \wedge (b \vee a) = a \tag{V$\vee$}$$

die sich geradeaus ergeben vermöge:

$$\begin{aligned} a \wedge (b \vee a) &= (a \wedge b) \vee (a \wedge a) \\ &= (a \wedge b) \vee (a \vee 1) \\ &= (a \wedge b) \vee 1 \\ &= a \wedge 1 \\ &= a \end{aligned}$$

und er hierzu $\wedge/\vee$-dualen Herleitung.
Hiernach lässt sich Assoziativitätsgesetz herleiten. Dabei werden wir als alles entscheidende Methode die Überführung von $(a \wedge b) \wedge c$ in einen a, c-symmetrischen Term einsetzen. Klar – immer ist es leichter, eine Klammer aufzulösen als eine Klammer zu setzen. Deshalb verfahren wir „von hinten nach vorne" und erhalten:

$$\begin{aligned} ((a \wedge b) \wedge c) \vee (a \wedge (b \wedge c)) &= \big((a \wedge b) \vee (a \wedge (b \wedge c))\big) \wedge \big(c \vee (a \wedge (b \wedge c))\big) \\ &= (a \wedge (b \vee (b \wedge c))) \wedge ((c \vee a) \wedge (c \vee (b \wedge c) \\ &= (a \wedge b) \wedge ((c \vee a) \wedge c) \\ &= (a \wedge b) \wedge c \\ &= f(a, b, c) \\ &= f(c, b, a) \\ &= a \wedge (b \wedge c \end{aligned}$$

Wir halten ausdrücklich fest, was zu beweisen war:

$$(A\wedge) \qquad a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

$$(A\vee) \qquad a \vee (b \vee c) = (a \vee b) \vee c$$

Wir erinnern noch einmal an (COM), insbesondere also an $a'' = a$. Diese Gleichung liefert uns zusammen mit der Distributivität:

2. 4. 2 Die Regeln von de Morgan.

$$(V\wedge) \qquad (a \wedge b)' = a' \vee b'$$

$$(V\vee) \qquad (a \vee b)' = a' \wedge b'$$

DENN, man beachte die beiden Gleichungen

$$(a \wedge b) \wedge (a' \vee b') = (a \wedge b \wedge a') \vee (a \wedge b \wedge b') = 0$$
$$(a \vee b) \vee (a' \wedge b') = (a \vee b \vee a') \wedge (a \vee b \vee b') = 1$$

und ziehe die (2.27), (2.28) heran. □

boolesche Algebren lassen neben den Verbandsoperationen die Definition einer Gruppenoperation zu, die schönere Eigenschaften nicht haben könnte. Doch es gilt noch sehr viel mehr, nämlich:

2. 4. 3 Proposition. *Setzen wir in einem booleschen Verband* $(V, \wedge, \vee, ')$

$$(2.35) \qquad a \oplus b := (a \wedge b') \vee (b \wedge a')$$

$$(2.36) \qquad a \odot b := a \wedge b\,,$$

so bildet V bezüglich dieser beiden Operationen einen idempotenten *Ring* $\mathfrak{R}(V)$*, und es bildet umgekehrt jeder idempotente Ring* $(R, +, \cdot, 1)$ *bezüglich*

$$(2.37) \qquad a \wedge b := a \cdot b$$

$$(2.38) \qquad a \vee b := a + ab + b$$

$$(2.39) \qquad a' := a + 1$$

einen booleschen Verband $\mathfrak{V}(R)$*. Darüber hinaus erfüllen die beiden hier vorgestellten Operatoren die* Galoisbedingung:

$$(2.40) \qquad \mathfrak{V}(\mathfrak{R}(V) = \mathfrak{V} \quad \& \quad \mathfrak{R}(\mathfrak{V}(R) = \mathfrak{R}$$

BEWEIS. Der Leser ermittelt geradeaus:

(R11) $$a \odot b = b \odot a$$

(R12) $$(a \odot b) \odot c = a \odot (b \odot c)$$

(R13) $$a \odot a = a$$

(R14) $$a \odot 1 = a$$

(R21) $$a \oplus b = b \oplus a$$

(R22) $$a \oplus a = 0$$

(R22) $$a \oplus 0 = a$$

Komplizierter sind die beiden restlichen Herleitungen. Zunächst verifizieren wir das Assoziativgesetz

(R23) $$a \oplus (b \oplus c) = (a \oplus b) \oplus c$$

Hier kommen wir zum Ziel vermöge:

$$\begin{aligned}
& a \oplus (b \oplus c) \\
= \ & \Big(a \wedge ((b \wedge c') \vee (c \wedge b'))'\Big) \vee \Big(((b \wedge c') \vee (c \wedge b')) \wedge a'\Big) \\
= \ & \Big(a \wedge (b' \vee c) \wedge (c' \wedge b))\Big) \vee \Big(b \wedge c' \wedge a'\Big) \vee \Big(a \wedge b' \wedge a'\Big) \\
= \ & \Big(a \wedge ((b' \wedge c') \vee 0 \vee 0 \vee (c \wedge b)\Big) \vee \Big(b \wedge c' \wedge a'\Big) \vee \Big(c \wedge b' \wedge a'\Big) \\
= \ & (a \wedge b' \wedge c') \vee (a \wedge c \wedge b) \vee (b \wedge c' \wedge a') \vee (c \wedge b' \wedge a') \\
= \ & f(a, b, c) = f(c, b, a) \\
= \ & (a \oplus b) \oplus c\,.
\end{aligned}$$

Schließlich erhalten wir das Distributivgesetz

(R23) $$a \odot (b \oplus c) = a \odot b \oplus a \odot c$$

via
$$\begin{aligned}
a \odot (b \oplus c) &= a \wedge ((b \wedge c') \vee (c \wedge b')) \\
&= (a \wedge b \wedge c') \vee (a \wedge c \wedge b') \\
&= 0 \vee (a \wedge b \wedge c') \vee 0 \vee (a \wedge c \wedge b')
\end{aligned}$$

$$
\begin{aligned}
&= \Big(a \wedge b \wedge a'\Big) \vee \Big(a \wedge b \wedge c'\Big) \vee \Big(a \wedge c \wedge a'\Big) \vee \Big(a \wedge c \wedge b'\Big) \\
&= \Big((a \wedge b) \wedge (a' \vee c')\Big) \vee \Big((a \wedge c) \wedge (a' \vee b')\Big) \\
&= \Big((a \wedge b) \wedge (a \wedge c)'\Big) \vee \Big((a \wedge c) \wedge (a \wedge b)'\Big) \\
&= (a \wedge b) \oplus (a \wedge c) \\
&= (a \odot b) \oplus (a \odot c)\,.
\end{aligned}
$$

Damit ist dem booleschen Verband $\mathfrak{V}$ ein idempotenter Ring $\mathfrak{R}$ gemäß den angegebenen Regeln zugeordnet.
Sei hiernach $\mathfrak{R}$ ein idempotenter Ring. Dann erhalten wir aus der Idempotenz unmittelbar

$$a + a = (a+a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a \Longrightarrow a + a = 0$$

also $a = -a$, woraus

$$a + b = (a+b)^2 = a^2 + ab + ba + b^2 \Longrightarrow ab + ba = 0\,,$$

und damit

$$ab = ba \tag{2.50}$$

resultiert. Der Rest darf dem Leser als Übung überlassen bleiben.
Zu verifizieren bleibt (2.40). Betrachten wir also die Operatoren $\mathfrak{V}$ und $\mathfrak{R}$. Hier haben wir zunächst $ab = a \wedge b = a \odot b$ und $a' = a + 1$, wegen $a' \oplus a = 0 \rightsquigarrow a' = a + 1$. Und dies impliziert weiter:

$$
\begin{aligned}
a + b &= ab + a + ab + ab + ab + ab + ba + b \\
&= a(b+1) + a(b+1) \cdot b(a+1) + b(a+1) \\
&= (a \wedge b') \vee (b \wedge a') \\
&= a \oplus b
\end{aligned}
$$

Damit sind wir am Ziel. □

Obacht: Neben den booleschen Ringen (mit 1) existieren natürlich auch idempotente Ringe ohne Eins, denn es bildet ja jedes Ideal eines booleschen Ringes einen solchen idempotenten Ring.
Um der Klarheit willen werden wir im folgenden unterscheiden zwischen booleschen Ringen, also idempotenten Ringen mit 1, und idempotenten Ringen.

Ferner werden wir den booleschen Verband und den booleschen Ring miteinander identifizieren zur *booleschen Algebra,* d. h. wir werden von booleschen Algebren sprechen und dabei die Operationen $\wedge, \vee, {}', \cdot, +, 1$ gemeinsam vor Augen haben.

2.5 Zur Verbandsgruppenarithmetik

Eine Algebra $(G, \cdot, \wedge, \vee)$ heißt eine ℓ-Gruppe – herrührend vom englischen *lattice group,* zu deutsch auch Verbandsgruppe – wenn $(G, \cdot)$ eine Gruppe, $(G, \wedge, \vee)$ ein Verband ist und wenn zusätzlich gilt: $a \leq b \Rightarrow xay \leq xby$. Ist dies erfüllt,so resultiert:

$$a \leq b \Longleftrightarrow a^{-1}ab^{-1} \ \leq \ a^{-1}bb^{-1} \Longleftrightarrow b^{-1} \leq a^{-1}. \tag{2.51}$$

Hieraus folgen weiter

$$x(a \wedge b)y \ = \ xay \wedge xby, \tag{2.52}$$
$$x(a \vee b)y \ = \ xay \vee xby, \tag{2.53}$$

wegen

$$\begin{aligned} z \leq x(a \wedge b)y \ &\Longleftrightarrow\ x^{-1}zy^{-1} \leq a \wedge b \\ &\Longleftrightarrow\ x^{-1}zy^{-1} \leq a \ \&\ x^{-1}zy^{-1} \leq b \\ &\Longleftrightarrow\ z \leq xay \wedge z \leq xby \\ &\Longleftrightarrow\ z \leq xay \wedge xby, \end{aligned}$$

und der hierzu dualen Herleitung. Hiernach erhalten wir insbesondere

$$(1 \wedge a)(1 \vee a) = 1 = (1 \vee a)(1 \wedge a) \tag{2.54}$$

vermöge

$$\begin{aligned} a \leq (1 \vee a) \wedge (a \vee a^2) \ &= \ (1 \vee a)(1 \wedge a) \\ &= \ (1 \wedge a) \vee (a \wedge a^2) \leq a. \end{aligned} \tag{2.55}$$

Als nächstes erhalten wir

$$(a \wedge b)^{-1} = 1 = a^{-1} \vee b^{-1} \tag{2.56}$$
$$(a \vee b)^{-1} = 1 = a^{-1} \wedge b^{-1} \tag{2.57}$$

wegen

$$\begin{aligned} x \leq (a \vee b)^{-1} \ &\Longleftrightarrow\ x^{-1} \geq a \vee b \\ &\Longleftrightarrow\ x^{-1} \geq a \ \&\ x^{-1} \leq b \\ &\Longleftrightarrow\ x \leq a^{-1} \ \&\ x \leq b^{-1} \\ &\Longleftrightarrow\ x \leq a^{-1} \wedge b^{-1} \end{aligned}$$

und der hierzu dualen Herleitung.

$$x = ab \;\&\; a \wedge b^{-1} = 1 \implies 1 \vee x = a \;\&\; 1 \wedge x = b\,, \tag{2.58}$$

denn die Prämisse führt wegen $a^{-1} \vee b = a \wedge b^{-1}$ zu

$$\begin{aligned} & 1 \vee x = 1 \vee ab = aa^{-1} \vee ab &=& \; a(a^{-1} \vee b) = a \\ \& \quad & 1 \wedge x = 1 \wedge ab = b^{-1}b \wedge ab &=& \; (b^{-1} \wedge a)b = b\,. \end{aligned}$$

Als nächstes folgt:

$$(1 \vee a) \wedge (1 \wedge a)^{-1} = 1, \tag{2.59}$$

wegen

$$\begin{aligned} (1 \vee a) \wedge (1 \wedge a)^{-1} &= a(1 \vee a^{-1}) \wedge 1(1 \wedge a)^{-1} \\ &= a(1 \wedge a)^{-1} \wedge 1(1 \wedge a)^{-1} \\ &= (a \wedge 1)(1 \wedge a)^{-1} \\ &= 1. \end{aligned}$$

Nun sind wir in der Lage, die Distributuivität nachzuweisen:

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c). \tag{2.60}$$

BEWEIS.

$$\begin{aligned} a \wedge (b \vee c) &= (b \vee c)((b \vee c)^{-1}a \wedge 1) \\ &= (b \vee c)((b^{-1} \wedge c^{-1})a \wedge 1) \\ &= (b \vee c)(b^{-1}a \wedge c^{-1}a \wedge 1) \\ &= (a \wedge bc^{-1}a \wedge b) \vee (cb^{-1}a \wedge a \wedge c) \\ &\leq (a \wedge b) \vee (a \wedge c) \\ &\implies \\ a \wedge (b \vee c) &= (a \wedge b) \vee (a \wedge c). \end{aligned}$$

Fertig ! □

Zur Erinnerung: mit (2.60) gilt, wie wir ja schon wissen, auch

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c). \tag{2.61}$$

Hiernach betrachten wir den Kegel P von $(G, \cdot, \vee, \wedge)$, das ist die Menge aller positiven Elemente, also $P := \{x \,|\, x \geq 1\}$. Wir erhalten sofort, dass P abgeschlossen ist bezüglich $\cdot, \vee, \wedge$, und man verifiziert leicht für die Operationen $*$ and $:$, definiert über

$$\begin{aligned} a * b := (a \wedge b)^{-1} \cdot b &= 1 \vee a^{-1}b \in P, \\ \text{und} \quad b : a := b \cdot (a \wedge b)^{-1} &= 1 \vee ba^{-1} \in P, \end{aligned}$$

die Gleichungen

$$
\begin{array}{lrcl}
\text{(A1)} & a * ab & = & b \\
\text{(A2)} & ba : a & = & b \\
\text{(A3)} & a(a * b) & = & b(b * a) \\
\text{(A4)} & (b : a)a & = & b(b * a) \\
\text{(A5)} & ab * c & = & b * (a * c).
\end{array}
$$

Auf der anderen Seite haben wir gezeigt, dass jede Algebra $(P, \cdot, *. :)$, die den Gesetzen (A1) bis (A5) genügt, als ein ℓ-Gruppen-Kegel betrachtet werden kann mit

$$a(a * b) = a \vee b = (b : a)a$$
$$\text{und} \quad b : (a * b) = a \vee b = (a : b) * a.$$

Das soll in diesem Kapitel genügen.

Kapitel 3

Komplementäre Halbgruppen

3.1 Einleitung

Sei $\mathfrak{S} := (S, \cdot)$ eine *Halbgruppe*, also eine Menge S betrachtet unter einer *assoziativen binären Operation.* Dann stehe $a \,\big|_\ell\, b$ für „*a ist Links-Teiler* von *b*”, also für die Existenz eines $x \in S$ mit $a \cdot x = b$, und es stehe dual $a \,\big|_r\, b$ für „*a ist Rechts-Teiler* von *b*”, also für die Existenz eines $y \in S$ mit $y \cdot a = b$. Als *linkskürzbar* bezeichnet man $\mathfrak{S}$ genau dann, wenn alle a der Äquivalenz $a \cdot x = a \cdot y \Longleftrightarrow x = y$ genügen. Dual ist die *rechtskürzbare* Halbgruppe definiert. Ist $\mathfrak{S}$ sowohl links- als auch rechts-kürzbar, so nennt man $\mathfrak{S}$ *kürzbar. Eine Halbgruppe* $\mathfrak{S}$ heißt *idempotent,* wenn für alle $a \in S$ die Gleichheit $a^2 = a$ erfüllt ist. $\mathfrak{S}$ heiße *rechtskomplementär* , wenn zu je zwei Elementen a, b aus $\mathfrak{S}$ genau ein Element $a * b$ in $\mathfrak{S}$ existiert mit $b \,\big|_\ell\, a \cdot x \Longleftrightarrow a * b \,\big|_\ell\, x$ bezeichnet als das *Rechtskomplement von a in b.* Dual definieren wir die *linkskomplementäre* Halbgruppe und bezeichnen das *Linkskomplement* mit $b : a$. Als Lesart ließe sich einführen *a rechts-ergänzt zu b* bzw. *a links-ergänzt zu b.* Ist $\mathfrak{S}$ eine rechtskomplementäre Halbgruppe, so existiert in $\mathfrak{S}$, wie wir später sehen werden, eine 1 mit $a \cdot 1 = a = 1 \cdot a$, und es gilt $a \,\big|_\ell\, b \;\&\; b \,\big|_\ell\, a \Longrightarrow a = b$. Daher ist jede rechtskomplementäre Halbgruppe bezüglich $\big|_\ell$ *teilweise geordnet* , weshalb wir auch $a \leq_\ell b$ statt $a \,\big|_\ell\, b$ schreiben werden und $a <_\ell b$ statt $a \,\big|_\ell\, b \;\&\; a \neq b$. Eine Halbgruppe $\mathfrak{S}$, die sowohl rechts- als auch linkskomplementär ist, heiße *komplementär,* wenn sie $a \cdot S = S \cdot a$ erfüllt für alle $a \in S$, also wenn $\big|_\ell$ und $\big|_r$ übereinstimmen.

Rechtskomplementäre Halbgruppen sind $\vee$-*abgeschlossen* und zwar gilt genauer $a(a * b) = \sup(a, b)$, doch sind nicht einmal komplementäre Halbgruppen notwendig $\wedge$-abgeschlossen.

Als Beispiel einer *linear geordneten* linkskürzbaren rechtskomplementären Halbgruppe, die keine komplementäre Halbgruppe ist, sei die Menge der *Ordinalzahlen* von der *Mächtigkeit* $\aleph_0$ bezüglich der Addition genannt. Als Beispiel einer komplementären Halbgruppe nennen wir den Bereich $\mathbf{N}$ der *natürlichen Zahlen,* betrachtet bezüglich der Multiplikation, oder allgemein jede *Zerlegungshalbgruppe,* (in [16] bezeichnet als *vollkanonisches Holoid*), den Bereich $\mathbf{Q}^{\geq 0}$ der *rationalen* Zahlen ≥ 0, betrachtet bezüglich der Addition, oder allgemein die Klasse der *streng archimedischen d-Halbgruppen,* siehe [39]. Weiter erwähnen wir die Menge der *Ordnungsautomorphismen* ϕ mit $a \leq \phi(a)$ $(\forall a)$ auf der Kette $\mathbf{Q}$ oder allgemein jeden *Verbandsgruppenkegel* und schließlich die Potenzmenge von $\mathbf{N}$, betrachtet bezüglich $\cup$ oder allgemein jeden *booleschen Ring,* betrachtet bezüglich seiner Multiplikation. Diese Konkretisierungen machen die zentrale Stellung der komplementären Halbgruppe deutlich.

Dem nun folgenden ersten großen Kaptitel über Residuation liegt der folgende Plan zugrunde:

In Abschnitt 1 wird die Struktur der rechtskomplementären Halbgruppen unter Berücksichtigung der rechtskürzbaren und der idempotenten Halbgruppen durch Gleichungssysteme charakterisiert, so dass diese fast unmittelbar eine Charakterisierung der entsprechenden komplementären Halbgruppen in Abschnitt 2 ermöglichen.

Abschnitt 3 liefert die für alle weiteren Untersuchungen wesentlichen arithmetischen Gesetze der komplementären Halbgruppen. In Abschnitt 4 engen wir die komplementäre Halbgruppe durch jeweils ein Zusatzaxiom nacheinander ein zur *Zerlegungshalbgruppe,* zur *archimedischen komplementären Halbgruppe,* zum *brouwerschen Halbverband,* zum *Verbandsgruppenkegel,* zum *booleschen Verband* bzw. zum *booleschen Ring,* sowie zum *direkten Produkt* des brouwerschen Halbverbandes mit einem Verbandsgruppenkegel, um hiernach jene komplementären Halbgruppen zu charakterisieren, die *subdirekt* zerfallen in Verbandsgruppenkegel und boolesche Ringe, bzw. in *Verbandsgruppenkegel mit* 0.

Hinter den einzelnen Axiomen erwähnen wir jeweils, abgekürzt in der Form $\big(\mathrm{B}n\big)$, dasjenige Beispiel – siehe hierzu den späteren Abschnitt über Beispiele –, das die Unabhängigkeit dieses Axioms von den übrigen des aufgestellten Systems beweist, hinter den einzelnen Beweiszeilen vielfach in runden Klammern denjenigen Hilfssatz, der den vollzogenen Schritt be-

gründet. Schließlich sei noch darauf hingewiesen, dass wir *duale Aussagen* natürlich als *wesensgleich* erachten und sie mitunter ohne Kommentar nur in einer Form erwähnen, respektive beweisen.
Schließlich noch eine Anmerkung: Wie üblich werden wir in dieser Lecture Note das Operationszeichen $\cdot$ „unterdrücken” bzw. fallen lassen.

3.2 Axiomatik

Wir erinnern: Eine Halbgruppe heißt *rechtskomplementär,* wenn sie der Bedingung genügt:

(RK) $$\forall\ a, b\ \exists\,(!)\ a * b\ :\quad b\,\big|_\ell\, ax \Longleftrightarrow a * b\,\big|_\ell\, x\,.$$

$\exists\,(!)$ steht hier im Sinne von *genau ein,* andernfalls wäre etwa jede Gruppe eine komplementäre Halbgruppe.
Als klassische Vertreter seien genannt der *brouwersche Halbverband* und der *Verbandsgruppenkegel.*
Ziel dieses Abschnitts ist der Nachweis, dass die Klasse der rechtskomplementären Halbgruppen *gleichungsdefiniert* ist, also eine *Varietät* bildet, und sich damit den Fragen der allgemeinen Algebra öffnet.
Sei hiernach $\mathfrak{S} := (S, \cdot, *)$ ein *Doppelgruppoid,* das den Axiomen genügt:

$$\begin{array}{lrcll}
\text{(A1)} & a(a * b) & = & b(b * a) & \big(\text{B1}\big) \\
\text{(A2)} & ab * c & = & b * (a * c) & \big(\text{B2}\big) \\
\text{(A3)} & a(b * b) & = & a\,. & \big(\text{B3}\big)
\end{array}$$

Wir werden in einer Serie von Kalkulationen herleiten, dass $\mathfrak{S}$ eine rechtskomplementäre Halbgruppe mit $a*b$ als Rechtskomplement darstellt. Dabei behalten wir im Hinterkopf, dass natürlich alle Herleitungen ihre rechts-links - dualen Entsprechungen haben.
Im einzelnen erhalten wir – ausgehend von dem aufgeführten Axiomensystem – als erstes die Assoziativität vermöge der Herleitung:

$$\begin{array}{lrcll}
(3.5) & a * a & = & (a * a)(b * b) & \text{(A3)} \\
 & & = & (a * a)\big(b(a * a) * b\big) & \text{(A3)} \\
 & & = & (a * a)\big((a * a) * (b * b)\big) & \text{(A2)} \\
 & & = & (b * b)\big((b * b) * (a * a)\big) & \text{(A1)} \\
 & & = & b * b := e & \text{(A3)}
\end{array}$$

(3.6)
$$\begin{aligned} (ab)c*d &= c*(ab*d) && \text{(A2)}\\ &= c*\big(b*(a*d)\big) && \text{(A2)}\\ &= bc*(a*d) && \text{(A2)}\\ &= a(bc)*d && \text{(A2)} \end{aligned}$$

(3.7)
$$\begin{aligned} (ab)c &= \big((ab)c\big)\big(a(bc)*a(bc)\big) && \text{(A3)}\\ &= \big((ab)c\big)\big((ab)c*a(bc)\big) && \text{(3.6)}\\ &= \big(a(bc)\big)\big(a(bc)*(ab)c\big) && \text{(A1)}\\ &= \big(a(bc)\big)\big((ab)c*(ab)c\big) && \text{(3.6)}\\ &= a(bc)\ . && \text{(A3)} \end{aligned}$$

Dies liefert weiter die Existenz eines Einselementes vermöge der Herleitung:

(3.8)
$$\begin{aligned} (e*a)*e &= (e*a)*(e*e) && \text{(3.5)}\\ &= e(e*a)*e && \text{(A2)}\\ &= a(a*e)*e && \text{(A1)}\\ &= (a*e)*(a*e) && \text{(A2)}\\ &= e && \text{(3.5)} \end{aligned}$$

(3.9)
$$\begin{aligned} e*a &= (e*a)\big((e*a)*e\big) && \text{(3.8)}\\ &= e\big(e*(e*a)\big)\\ &= e(ee*a)\\ &= e(e*a) \end{aligned}$$

(3.10)
$$\begin{aligned} (e*a)*a &= e(e*a)*a && \text{(3.9)}\\ &= (e*a)*(e*a)\\ &= e \end{aligned}$$

(3.11)
$$\begin{aligned} e*a &= (e*a)e\\ &= (e*a)\big((e*a)*a\big) && \text{(3.10)}\\ &= a\big(a*(e*a)\big)\\ &= a(ea*a)\\ &= ea(ea*a) && \text{(3.9)}\\ &= a(a*ea)\\ &= ea(a*ea) && \text{(3.9)} \end{aligned}$$

(3.12)
$$\begin{aligned} e*ea &= e(ea)\big(ea*e(ea)\big) && \text{(3.11)}\\ &= ea(ea*ea)\\ &= ea \end{aligned}$$

$$\begin{aligned}
ea &= ea(ea * ea) \\
&= ea\big(a * (e * ea)\big) \\
&= ea(a * ea) && (3.12) \\
&= e * a && (3.11)
\end{aligned} \tag{3.13}$$

$$\begin{aligned}
ea &= e * a \\
&= a(ea * a) && (3.11) \\
&= a\big((e * a) * a\big) && (3.13) \\
&= ae && (3.10) \\
&= a && .
\end{aligned} \tag{3.14}$$

Im weiteren schreiben wir 1 statt e, um zu betonen, dass e nicht nur *Rechtseins* ist, wie *per definitionem* gefordert, sondern auch *Linkseins* und damit eindeutig bestimmte *Eins* der Halbgruppe $(S, \cdot)$. Für diese 1 gilt weiter:

$$\begin{aligned}
a * 1 &= 1(1 * a) * 1 \\
&= a(a * 1) * 1 \\
&= (a * 1) * (a * 1) \\
&= 1
\end{aligned} \tag{3.15}$$

$$\begin{aligned}
ax &= b \\
&\Rightarrow \\
b * a = ax * a &= x * (a * a) = 1 \\
&\& \\
b * a &= 1 \\
&\Rightarrow \\
b = b(b * a) &= a(a * b)\,,
\end{aligned} \tag{3.16}$$

und damit gleichbedeutend

$$a \,\big|_\ell\, b \iff b * a = 1\,. \tag{3.17}$$

Das liefert uns weiter:

$$\begin{aligned}
ax = b \quad &\& \quad by = a \\
&\Longrightarrow \\
a = a1 = a(a * b) \quad &= \quad b(b * a) = b1 = b && (3.16)
\end{aligned} \tag{3.18}$$

bzw. die Äquivalenz:

$$b \,\big|_\ell\, ax \iff x * (a * b) = 1\,, \tag{3.19}$$

die sich aus
$$\begin{array}{rcl} ax = by & \Longrightarrow & x * (a * b) = ax * b = by * b = 1 \\ & \& & \\ x * (a * b) = 1 & \Longrightarrow & ax * b = 1 \Longrightarrow b \,\big|_\ell\, ax \end{array}$$
ergibt.

Aus (3.18) folgt, dass $\mathfrak{S}$ durch $\big|_\ell$ teilweise geordnet wird, nach (3.19) ist $\mathfrak{S}$ rechtskomplementär.

Bevor wir zeigen, dass auch jede rechtskomplementäre Halbgruppe die Axiome (A1), (A2), (A3) erfüllt, beweisen wir noch die Abgeschlossenheit von $\mathfrak{S}$ bezüglich $\vee$. Genauer werden wir sehen, dass $a(a * b) = b(b * a)$ als *Supremum* fungiert, also $c \geq a, b \Longleftrightarrow c \geq a(a * b)$ erfüllt. Dies ergibt sich aus den beiden nachfolgenden Implikationen:

$$\begin{array}{rcl} c * a = & 1 & = c * b \\ & \Longrightarrow & \\ (a * c) * (a * b) & = & a(a * c) * b \\ & = & c(c * a) * b \\ & = & c * b \\ & = & 1 \\ & \Longrightarrow & \\ a(a * b) \,\big|_\ell\, a(a * c) & = & c(c * a) = c \end{array} \quad (3.19) \tag{3.20}$$

$$\begin{array}{rcl} a(a * b) * b & = & b(b * a) * b \\ & = & (b * a) * (b * b) \\ & = & (b * a) * 1 = 1 \\ & \rightsquigarrow & \\ a, b \,\big|_\ell\, a(a * b) & = & b(b * a)\,. \end{array} \quad (3.19) \tag{3.21}$$

Wir können also festhalten:

$$a(a * b) = a \vee b \;=\; b \vee a = b(b * a) \tag{3.22}$$

Sei nun umgekehrt $\mathfrak{S}$ eine rechtskomplementäre Halbgruppe. Dann gelten bezüglich der *Rechtskomplementierung* $a * b$ die Axiome (A1), (A2), (A3). Denn $a * a = e$ muss Linksteiler aller b aus $\mathfrak{S}$ sein und deshalb auch mit seinen sämtlichen Potenzen jedes Element linksteilen, woraus $e^2 = e$ resultiert, da sowohl e als auch e^2 die Bedingung für $a * a$ erfüllt. Gilt weiter $a \,\big|_\ell b \;\&\; b \,\big|_\ell a$, so erhalten wir $a = e * a = b$. Schließlich haben wir hiernach:

$$a(a * b) = bx \geq b(b * a) \;=\; ay \geq a(a * b)\,, \tag{A1'}$$

$$\text{(A2')} \qquad x \geq ab * c \Leftrightarrow abx \geq c \;\; \Leftrightarrow \;\; x \geq ab * c \Leftrightarrow x \geq b * (a * c)$$

$$\text{(A3)} \qquad a(b * b) = a(a * e) \;\; = \;\; e(e * a) = a\,.$$

Somit können wir formulieren:

3. 2. 1 Proposition. *Ein Doppel-Gruppoid* $\mathfrak{S} = (S, \cdot, *)$ *ist eine rechtskomplementäre Halbgruppe mit* $a * b$ *als Rechtskomplementierung gdw. es die Bedingungen* (A1), (A2), (A3) *erfüllt.*

Hiernach wenden wir uns dem linkskürzbaren Fall zu. Offenbar gilt hier notwendig:

$$\text{(A1)} \qquad a(a * b) \stackrel{\text{(B8)}}{=} b(b * a)$$

$$\text{(A2)} \qquad ab * c \stackrel{\text{(B9)}}{=} b * (a * c)$$

$$\text{(V1)} \qquad a * ab \stackrel{\text{(B3)}}{=} b$$

Seien also (A1), (A2), (V1) erfüllt. Dann erhalten wir zunächst:

$$\text{(3.29)} \qquad \begin{aligned} (ab)c * d &= c * (b * (a * d)) \\ &= a(bc) * d \end{aligned}$$

$$\text{(3.30)} \qquad \begin{aligned} ab &= a(a * ab) \\ &= (ab)(ab * a) \end{aligned}$$

$$\text{(3.31)} \qquad \begin{aligned} ab * ab &= ab * (ab)(ab * a) && (3.30) \\ &= ab * a \end{aligned}$$

$$\text{(3.32)} \qquad \begin{aligned} (ab)(ab * ab) &= (ab)(ab * a) && (3.31) \\ &= a(a * ab) \\ &= ab \end{aligned}$$

Daraus folgt im Falle $au = a$ die spezielle Assoziativität $(au)b = a(ub)$, die weiter zur Existenz einer Rechtseins führt, wie wir nun sehen werden. Sei also $au = a$. Dann folgen nacheinander:

$$
\begin{aligned}
(au)b &= \big((au)b\big)\big((au)b * au\big) && (3.30)\\
&= \big((au)b\big)\big(a(ub) * au\big) && (A2)\\
&= \big((au)b\big)\big(a(ub) * a\big) &&\\
&= \big((au)b\big)\big(a(ub) * a(ub)\big) && (3.30)\\
&= \big((au)b\big)\big((au)b * a(ub)\big) && (\mathrm{A2})\\
&= \big(a(ub)\big)\big(a(ub) * (au)b\big) && (\mathrm{A1})\\
&= \big(a(ub)\big)\big((au)b * (au)b\big) && (\mathrm{A2})\\
&= \big(a(ub)\big)\big(ab * ab\big) &&\\
&= \big(a(ub)\big)\big(ab * a\big) && (3.30)\\
&= \big(a(ub)\big)\big((au)b * a\big) &&\\
&= \big(a(ub)\big)\big(a(ub) * a\big) && (\mathrm{A2})\\
&= a(ub) && (3.30)
\end{aligned} \tag{3.33}
$$

$$
\begin{aligned}
au &= a &&\\
&\Rightarrow &&\\
ub = a * a(ub) &= a * (au)b = b \quad (\forall b \in G) && (3.33)
\end{aligned} \tag{3.34}
$$

$$
\begin{aligned}
ub &= b &&\\
&\Rightarrow &&\\
u * b &= u * ub = b && (3.33)
\end{aligned} \tag{3.35}
$$

$$
\begin{aligned}
au = {} & a = av \quad (\forall a \in G) &&\\
&\Rightarrow &&\\
vu = v(v * u) &= u(u * v) = uv && (3.35)
\end{aligned} \tag{3.36}
$$

Für die soeben nachgewiesene eindeutige *Linkseinheit* e gilt nun weiter:

$$
\begin{aligned}
a(a * e) &= e(e * a) &&\\
&= e * a && (3.34)\\
&= a && (3.35)\\
\rightsquigarrow \qquad a * e &= e &&\\
&\rightsquigarrow &&\\
ae &= a &&
\end{aligned} \tag{3.37}
$$

Verifizieren wir jetzt noch $b * b = e$, so ist der Anschluss an (A1), (A2), (A3) hergestellt. Es gilt aber:

$$
b * b = be * be = e * (b * be) = e * e = e \Longrightarrow ae = a \tag{3.38}
$$

Zusammenfassend erhalten wir damit *via* Satz 3.2.1

3. 2. 2 Proposition. *Ein Gruppoid $\mathfrak{S}$ ist eine linkskürzbare rechtskomplementäre Halbgruppe gdw. es bezüglich einer weiteren Operation $*$ die Axiome* (A1), (A2), (V1) *erfüllt.*

Hiernach betrachten wir *idempotente* rechtskomplementäre Halbgruppen. Als notwendig ergeben sich die Axiome:

(I1) $$a^2(a*b) = b(b*a) \qquad \text{(B1)}$$

(A2) $$ab*c = b*(a*c) \qquad \text{(B2)}$$

(A3) $$a(b*b) = a \qquad \text{(B3)}$$

Dass diese Axiome auch hinreichen, folgt fast unmittelbar, man setze in (I1) $b := a$.
Somit folgt

3. 2. 3 Proposition. *Ein Gruppoid $\mathfrak{S}$ ist eine idempotente rechtskomlementäre Halbgruppe gdw. es bezüglich einer weiteren Operation $*$ den Axiomen* (I1),(A2), (A3) *genügt.*

3. 2. 4 Proposition. *Ein Gruppoid $\mathfrak{S}$ ist eine kommutative kürzbare* (*rechts-*) *komplementäre Halbgruppe gdw. es bezüglich einer weiteren Operation $*$ den Axiomen genügt:*

(A1) $$a(a*b) = b(b*a) \qquad \text{(B8)}$$

(A2) $$ab*c = b*(a*c) \qquad \text{(B9)}$$

(V2) $$a*ba = b \qquad \text{(B3)}$$

Zum Zwecke des Beweises wählen wir zunächst ein festes a und betrachten hierzu das Element $u := a^2 * a$. Dann folgen nacheinander:

(3.45) $$\begin{aligned} a^2 &= a(a*a^2) && \text{(V2)} \\ &= a^2(a^2*a) \end{aligned}$$

(3.46) $$\begin{aligned} a^2*a &= a^2(a^2*a)*a && (3.45) \\ &= (a^2*a)*(a^2*a) \\ &=: u \end{aligned}$$

(3.47)
$$\begin{aligned} u^2 * u &= u * (u * u) \\ &= u * u && (3.46) \\ &= u \end{aligned}$$

(3.48)
$$\begin{aligned} u &= u * u^2 \\ &= u * u(u * u^2) && (V2) \\ &= u * u^2(u^2 * u) \\ &= u * u^2 u && (3.47) \\ &= u^2 \end{aligned}$$

(3.49)
$$\begin{aligned} v^2 &= v \\ &\Rightarrow \\ bv &= v * (bv)v && (3.48) \\ &= v * \big(v * (bv)v\big) \\ &= v * bv \\ &= b \end{aligned}$$

(3.50)
$$\begin{aligned} v^2 &= v \\ &\Rightarrow \\ v * b &= v * bv && (3.49) \\ &= b \end{aligned}$$

(3.51)
$$\begin{aligned} v^2 = v \quad &\& \quad u^2 = u \\ &\Rightarrow \\ v &= vu && (3.49) \\ &= v(v * u) && (3.50) \\ &= u(u * v) \\ &= u\ . \end{aligned}$$

Es gibt also nach unseren Herleitungen genau ein idempotentes Element. Dies sei von nun an mit 1 bezeichnet. Dann erhalten wir die Gleichungen:

$$(3.52)\qquad \begin{aligned} b*1 &= b*(1*1) \\ &= 1b*1 \\ &= 1(1*b)*1 && (3.50) \\ &= b(b*1)*1 \\ &= (b*1)*(b*1) \\ &= (b*1)^2*(b*1) \\ &= 1 \end{aligned}$$

$$(3.53)\qquad \begin{aligned} b1 &= b(b*1) && (3.52) \\ &= 1(1*b) \\ &= 1b \end{aligned}$$

$$(3.54)\qquad \begin{aligned} b*b &= b*(1*b1) \\ &= 1b*b1 \\ &= b1*1b && (3.53) \\ &= 1*(b*1b) \\ &= 1*1 \\ &= 1 \end{aligned}$$

$$(3.55)\qquad \begin{aligned} ab*ba &= b*(a*ba) \\ &= b*b \\ &= 1\,. \end{aligned}$$

Offenbar implizieren (3.53) und (3.54) das Axiom (A3), während (3.55) die Kommutativität gewährleistet.

Die Sätze 3.2.1, 3.2.2 und 3.2.4 zeigen den Zusammenhang auf zwischen den rechtskomplementären, den linkskürzbaren rechtskomplementären und den kommutativen kürzbaren komplementären Halbgruppen.

3. 2. 5 Proposition. *Ein Gruppoid $\mathfrak{G}$ ein brouwerscher Halbverband, gdw. es bezüglich einer weiteren Operation $*$ die Axiome*

(I 1) $$a^2(a*b) = b(b*a) \qquad \big(\mathrm{B1}\big)$$

(A2) $$ab*c = b*(a*c) \qquad \big(\mathrm{B9}\big)$$

(I 2) $$ab*b = a*(b*b) \qquad \big(\mathrm{B10}\big)$$

(A3) $$a(b*b) = a \qquad \big(\mathrm{B3}\big)$$

DENN: Aufgrund von Axiom (I2) gilt $a*b \mid b$, wegen $b*(a*b) = ab*b = a*(b*b) = 1$, also $ab \geq a\vee b$, was mit $ab \leq a\vee b$ weiter zu $ab = a\vee b = b\vee a = ba$ führt. □

Satz 3.2.5 hat noch mit ergeben, dass jede idempotente komplementäre Halbgruppe notwendig kommutativ ist.

Hinweis: Später werden wir auf die Axiomatik der hier betrachteten Stukturen zurückkommen und weitere Systeme präsentieren!

3.3 Arithmetik und ideale Arithmetik

Weiter oben hatten wir die komplementäre Halbgruppe verbal erklärt. Formal erfassen wir sie natürlich mit der Beschreibung

3. 3. 1 Definition. Eine Algebra $(S, \cdot, *, :) =: \mathfrak{S}$ ist eine komplementäre Halbgruppe gdw. sie den Bedingungen genügt:

(A1) $a(a*b) = b(b*a)$ (B1) $(b:a)a = (a:b)b$

(A2) $ab*c = b*(a*c)$ (B2) $c:ab = (c:a):b$

(A3) $a(b*b) = a$ (B3) $(b:b)a = a$

(SYM) $a(a*b) = (b:a)a$

Wir erkennen sofort die genuin gegebene $*/:$-Dualität auch an den gewählten Axiomen, die hier bewusst abhängig gewählt wurden, um diesen dualen Charakter zu betonen. Zum Einmaleins der komplementären Halbgruppe sei erwähnt:

3. 3. 2 Proposition. *Jede komplementäre Halbgruppe erfüllt:*

(3.64) $a*(b:c) = (a*b):c$

(3.65) $(a:b):(c:b) = (a:(b*c)):b$

(3.66) $(a*b)*(a*c) = a*((b:a)*c)$

DENN: (3.64) ergibt sich aus $ax \geq b:c \Longleftrightarrow axc \geq b \Longleftrightarrow xc \geq a*b \Longleftrightarrow x \geq (a*b):c$, und der Rest ist klar. □

Sei im folgenden $\mathfrak{S}$ durchgehend eine komplementäre Halbgruppe. Wir entwickeln in diesem Paragraphen Regeln der Arithmetik, wie sie für das

Weitere von Bedeutung sein werden. Dabei beschränken wir uns meist auf eine „Richtung" erinnern aber „ein für alle Mal" daran, dass die jeweils $*$, : - duale Version stets mitbewiesen ist.

(3.67) $$a \leq b \Longrightarrow c * a \leq c * b \quad \& \quad a \leq b \Longrightarrow a * c \geq b * c$$

DENN: $a \leq b \Longrightarrow c(c * b) \geq a \ \& \ b(a * c) \geq c\,.$ □

Unter Berücksichtigung von (3.67) erhalten wir weiter [1]:

(3.68) $$a(b \vee c) \;=\; ab \vee ac$$

DENN:
$$\begin{aligned} ab \vee ac &= ab(ab * ac) \\ &= ab(b * (a * ac)) \\ &= a(a * ac)((a * ac) * b) \\ &\geq ac(c * b) \\ &= a(b \vee c)\,. \end{aligned}$$ □

3. 3. 3 Lemma. *Mit $a \wedge b$ existieren auch $ax \wedge bx$ und $xa \wedge xb$, und es gilt:*

$$x(a \wedge b) = xa \wedge xb \quad \textit{und} \quad (a \wedge b)x = ax \wedge bx\,.$$

DENN:
$$\begin{array}{rrcl} & c \leq xa & \& & c \leq xb \\ \Longrightarrow & x * c \leq a & \& & x * c \leq b \\ \Longrightarrow & x * c & \leq & a \wedge b \\ \Longrightarrow & x(x * c) & \leq & x(a \wedge b) \\ \Longrightarrow & c & \leq & x(a \wedge b)\,. \end{array}$$ □

Wie schon erwähnt, ist eine komplementäre Halbgruppe nicht notwendig $\wedge$-abgeschlossen. Es gilt aber das hochrelevante Resultat:

3. 3. 4 Proposition. *Ist $\mathfrak{S}$ $\wedge$-abgeschlossen, so ist $\mathfrak{S}$ verbands-distributiv.*

DENN:
$$\begin{aligned} a \vee (b \wedge c) &= (b \wedge c)((b \wedge c) * a) \\ &= b((b \wedge c) * a) \wedge c((b \wedge c) * a) \\ &\geq b(b * a) \wedge c(c * a) \\ &= (a \vee b) \wedge (a \vee c)\,. \end{aligned}$$ □

Weiter haben wir

(3.69) $$a * (b \vee c) \;=\; (a * b) \vee (a * c)$$

[1] schon für den rechtskomplemetären Fall, falls $a * b \leq b$, wie der Leser leicht bestätigt

DENN: $ax \geq b \vee c \Longleftrightarrow x \geq (a * b) \vee (a * c)\,.$ □

Aus der letzten Gleichung folgt insbesondere:

$$a * a(a * b) = a * (a \vee b) \;=\; (a * a) \vee (a * b) = a * b \tag{3.70}$$

3. 3. 5 Lemma. *Existiert $a \wedge b$, so gilt*

$$(a \wedge b) * c \;=\; (a * c) \vee (b * c) \tag{3.71}$$

DENN: $(a \wedge b)x \geq c \Longleftrightarrow ax \geq c \leq bx \Longleftrightarrow a * c \leq x \geq b * c\,.$ □

Schließlich erhalten wir

$$a * b \;=\; (b : (a * b)) * b \tag{3.72}$$

DENN:
$$\begin{array}{rcl} (b : (a * b)) * b & \leq & a * b \;\&\; b : (a * b) \leq a \\ & \rightsquigarrow & \\ (b : (a * b)) * b & \geq & a * b\,. \end{array}$$ □

Komplementäre Halbgruppen sind nicht notwendig $\wedge$-abgeschlossen. Genauer gilt:

3. 3. 6 Lemma. *Sind a und b zwei beliebige Elemente aus S, so ist c genau dann Infimum zu a und b, wenn für jedes d aus S gilt:*

$$c * d = (a * d) \vee (b * d) \quad bzw. \quad d : c = (d : a) \vee (d : b)\,.$$

BEWEIS. Die aufgestellte Bedingung folgt aus der Behauptung nach 3. 3.5 . Umgekehrt ergeben sich aus der aufgestellten Bedingung die Implikationen

$$c * c = 1 \Longrightarrow (a * c) \vee (b * c) = 1 \Longrightarrow a * c = 1 = b * c \Longrightarrow a, b \geq c$$

$$\text{und} \quad d \leq a, b \Longrightarrow (a * d) \vee (b * d) = 1 \Longrightarrow c * d = 1 \Longrightarrow d \,\big|\, c.$$

Damit sind wir am Ziel. □

Nach 3.3.6 sind zwei Elemente a, b genau dann (*teiler-*) *fremd,* im weiteren auch *orthogonal,* i. Z. $a \perp b$, wenn alle c aus S der Gleichung genügen: $(a * c) \vee (b * c) = c$. Das liefert weiter $a \wedge b = 1 \Longrightarrow a * b = b$ und damit:

$$a \perp b \;\&\; ab = ba \Longrightarrow a\big|bc \vee a \,\big|\, cb \Longrightarrow a \,\big|\, c\,. \tag{3.73}$$

DENN: Nach Voraussetzung haben wir: $ab = a(a * b) = b(b * a) = ba$ und $c * a = c * (b * a) = bc * a = 1$. □

3. 3. 7 Definition. $p \in S$ heißt *halbprim,* wenn p der Implikation genügt: $p = ab \Longrightarrow p = a \vee p = b$.

Offenbar ist $p \in S$ halbprim gdw. $a < p \Longrightarrow ap = p$ erfüllt ist. Weiter gilt

3. 3. 8 Lemma. *Ein Element p aus S ist halbprim gdw. für alle $c \in S$ die Gleichung $c * p = 1 \vee c * p = p$ erfüllt ist, und dies impliziert weiter $p \,\big|\, ab \Longrightarrow p \,\big|\, a \vee p \,\big|\, b$.*

DENN: Ist p halbprim, so resultiert aus

$$p = (p : (c * p))(c * p) \Longrightarrow c * p = p \vee p : (c * p) = p\,,$$

dass $c * p = p$ oder $c * p = (p : (c * p)) * p = p * p = 1$ erfüllt ist.
Umgekehrt folgt aus $p = ab \;\&\; p \neq a$, dass $a * p = p$ also auch $b = p$ sein muss.
Gilt schließlich zudem $p \,\big|\, ab$, so erhalten wir die Implikation

$$\begin{aligned} ab * p = 1 \Longrightarrow b * (a * p) = 1 \;\; &\Longrightarrow \;\; a * p = 1 \vee b * p = 1 \\ &\Longrightarrow \;\; p \,\big|\, a \vee p \,\big|\, b\,. \end{aligned}$$

Fertig! □

3. 3. 9 Lemma. *Je zwei Halbprimelemente p, q kommutieren.*

DENN: Ist $pq = q$, so folgt $xp = q$ $(\exists x \in S)$, und es muss $x = q \vee p = q$ erfüllt sein. Analog schließen wir für $pq = p$.
Gilt aber $p \neq pq \neq q \neq p$, so ist zunächst $p * q = q$ und $q * p = p$ erfüllt, woraus dann $pq = p(p * q) = q(q * p) = qp$ resultiert. □

3. 3. 10 Lemma. *Ist p halbprim und gilt $a \neq ap$, so folgt $a * ap = p$.*

DENN: Sei $x = a * ap$. Dann gilt $ap = ax$. Wäre nun $p \not\leq x$, so hätten wir $a = a'p$, also wegen $x < p$ dann weiter $a = ax = ap$ – mit Widerspruch! □

3. 3. 11 Definition. $p \in S$ heiße *vollprim*, wenn p im Falle $p^n \,\big|\, ab$ beide oder aber p^n mindestens einen der beiden Faktoren teilt.

3. 3. 12 Lemma. *Jedes halbprime p aus $\mathfrak{S}$ ist sogar vollprim.*

DENN: Sei $k \leq n$ der höchste Exponent mit $p^k \leq a$. Wäre dann $k < n$ so ergäbe sich $a = p^k \cdot a' \cdot b$, und es müsste nach 3.3.10 $p \,\big|\, a' \cdot b$ erfüllt sein, ein Widerspruch! □

Wir kommen nun zu den Idempotenten in komplementären Halbgruppen.

3. 3. 13 Lemma. *Sei $\mathfrak{S}$ eine komplementäre Halbgruppe. Dann liegen die idempotenten Elemente im Zentrum und die Menge E der Idempotenten ist abgeschlossen bezüglich der Operationen $\cdot$, $*$, $:$, $\vee$ und $\wedge$.*

BEWEIS. Sei $a^2 = a$. Dann haben wir $ab = a \vee b$ wegen $b \leq a \vee b$ und $a(a \vee b) = a \vee b$.
Hieraus erhalten wir weiter für je zwei Idempotenta, b die Gleichung $(ab)^2 = a^2b^2 = ab = a \vee b = (a \vee b)^2$. Also ist E abgeschlossen bezüglich $\cdot$ und $\vee$.
Wir zeigen nun, dass E auch abgeschlossen ist bezüglich $*$.
Seien also a und b idempotent. Dann ist auch $a \vee b$ idempotent, so dass wir wegen $a * b = a * (a \vee b)$ o. B. d. A. $a < b$ annehmen dürfen. Das liefert weiter mit $a * b =: x$ die Abschätzung $a * (x * x^2) \leq a * (x * ax^2) = ax * ax = 1$, also $a(x * x^2) = a$. Daraus folgt dann aber für jedes y mit $y(x * x^2) = x$ zunächst $ay = ay(x * x^2) = ax = b$, also $x \leq y$, woraus weiter die Abschätzung $x^2 = x(x * x^2) \leq y(x * x^2) = x$ resultiert.
Ist $\mathfrak{S}$ schließlich $\wedge$-abgeschlossen, so gilt für idempotente a, b zusätzlich $(a \wedge b)^2 = a \wedge ab \wedge b = a \wedge b$. □

Zur Erarbeitung der weiteren Arithmetik führen wir den Bereich $\mathfrak{V}$ der endlich erzeugten, kurz *endlichen*, v-*Ideale* ein. Wir gehen aus von Halbgruppen $\mathfrak{S}$ mit $\big|_r = \big|_\ell$.

3. 3. 14 Definition. Sei $\mathfrak{S}$ eine beliebige Halbgruppe. Dann heiße ein nicht leeres $\mathfrak{a} \subseteq \mathfrak{S}$ ein v-Ideal, wenn gilt:

$$(s \,\big|\, u \cdot \mathfrak{a} \cdot v \Longrightarrow s \,\big|\, ucv) \Longrightarrow c \in \mathfrak{a} .$$

Wie üblich nehmen wir also die leere Menge nicht mit unter die v-Ideale auf, weisen aber darauf hin, dass dies möglich wäre. Damit haben wir:
A fortiori ist S ein v-Ideal in $\mathfrak{S}$ und man bestätigt leicht, dass der Durchschnitt einer Familie von v-Idealen leer ist oder wieder ein v-Ideal liefert, sowie, dass der Durchschnitt $\{A\}$ aller A umfassenden v-Ideale gleich der Menge aller c ist, die der Bedingung genügen:

$$s \,\big|\, uAv \;\Longrightarrow\; s \,\big|\, ucv \, .$$

Weiter gilt $\{A\}\{B\} \subseteq \{AB\}$,

wegen

$$s \mid uABv \Longrightarrow s \mid u\{A\}\{B\}v\,,$$

sowie

$$\{A\} = \{A'\} \;\&\; \{B\} = \{B'\} \Longrightarrow \{AB\} = \{A'B'\}\,,$$

wegen

$$s \mid uABv \Longrightarrow s \mid uA'Bv \Longrightarrow s \mid uA'B'v\,.$$

Aufgrund dieser Zusammenhänge wird jedem Paar von v-Idealen eindeutig ein *Produktideal* zugeordnet. Schließlich bildet zu je zwei v-Idealen $\mathfrak{a}, \mathfrak{b}$ die Menge $\mathfrak{a}/\mathfrak{b}$ aller x mit $\mathfrak{a}x \subseteq \mathfrak{b}$ und entsprechend die Menge $\mathfrak{b}\backslash\mathfrak{a}$ aller y mit $y\mathfrak{a} \subseteq \mathfrak{b}$ ein v-Ideal. Denn die Festsetzung $\mathfrak{a}/\mathfrak{b} =: \mathfrak{x}$ liefert:

$$\begin{array}{rcl}
r \mid u \cdot \mathfrak{x} \cdot v & \Rightarrow & r \mid u \cdot c \cdot v \\
& \Longrightarrow & \\
s \mid u \cdot \mathfrak{b} \cdot v & \Rightarrow & s \mid u \cdot \mathfrak{a}\mathfrak{x} \cdot v \\
& \Rightarrow & s \mid u \cdot \mathfrak{a}c \cdot v \\
& \Rightarrow & \mathfrak{a} \cdot c \subseteq \mathfrak{b} \\
& \Longrightarrow & \\
c & \in & \mathfrak{x}\,.
\end{array}$$

Im folgenden sei $\mathfrak{S}$ komplementär. Dann gehören genau diejenigen Elemente aus S zu $\{A\}$, die *gemeinsames Vielfaches* aller *gemeinsamen Teiler* von A sind. Denn $s \mid A \Longrightarrow s \mid \{A\}$ und aus $g \mid A \Longrightarrow g \mid c$ für alle $g \in S$ folgt:

$$\begin{array}{rcl}
s \mid uAv & \Longrightarrow & s : v \mid uA \\
& \Longrightarrow & u * (s : v) \mid A \\
& \Longrightarrow & u * (s : v) \mid c \\
& \Longrightarrow & u(u * (s : v)) \mid uc \\
& \Longrightarrow & u \vee (s : v) \mid uc \\
& \Longrightarrow & s : v \mid uc \\
& \Longrightarrow & (s : v)v \mid ucv \\
& \Longrightarrow & s \vee v \mid ucv \\
& \Longrightarrow & s \mid ucv\,.
\end{array}$$

Insbesondere haben wir hiernach für komplementäre Halbgruppen:

$$\{A\} = \{a\} \;\Longrightarrow\; a = \bigwedge x \;\; (x \in A)\,.$$

Weiter ergibt sich für endliche v-Ideale die wichtige Äquivalenz:

$$\mathfrak{a} \supseteq \mathfrak{b} \Longleftrightarrow \mathfrak{a} \,\Big|_{\ell}\, \mathfrak{b} \Longleftrightarrow \mathfrak{a} \,\Big|_{r}\, \mathfrak{b}\,. \tag{3.74}$$

Zunächst haben wir $\mathfrak{a}\mathfrak{x} = \mathfrak{b} \Longrightarrow \mathfrak{a} \supseteq \mathfrak{b}$ und gilt umgekehrt $\mathfrak{a} \supseteq \mathfrak{b}$, so erhalten wir im Falle $\mathfrak{a} = \{a_1, \ldots, a_n\} \ni b$ für $c = \bigvee_1^n (a_i * b)$ die Implikation:

$$\begin{array}{rcl} d \,\big|\, b & \Longrightarrow & d \,\big|\, \mathfrak{a} \cdot c \\ & \& & \\ d \,\big|\, \mathfrak{a} \cdot c & \Longrightarrow & c \leq b \vee d =: g \,\big|\, \mathfrak{a} \cdot c \\ & \Longrightarrow & g : c \,\big|\, \mathfrak{a} \\ & \Longrightarrow & g : c \,\big|\, b \\ & \Longrightarrow & (g : c)x = b \\ & \Longrightarrow & \mathfrak{a}x \geq b \\ & \Longrightarrow & x \geq c \\ & \Longrightarrow & (g : c)c \leq b \\ & \Longrightarrow & g \,\big|\, b \\ & \Longrightarrow & d \,\big|\, b\,. \end{array}$$

Somit ist $\mathfrak{a}\{c\} = \{b\}$. Durchläuft nun b eine endliche Basis $B = b_1, \ldots, b_m$ von $\mathfrak{b}$ mit korrespondierenden c_k so erhalten wir die erste Behauptung mit $\mathfrak{a}\{c_i\} = \{b_k\}$.

Der Rest folgt dual.

Da $\mathfrak{S}$ isomorph ist zum Bereich aller Hauptideale $\{a\}$, dürfen wir im folgenden die Hauptideale mit ihren *Erzeugern* identifizieren. Weiter sei verabredet, den Durchschnitt zweier v-Ideale $\mathfrak{a}, \mathfrak{b}$ mit $\mathfrak{a} \vee \mathfrak{b}$ zu bezeichnen.

Es wird also im weiteren b das Ideal $\{b\}$ bedeuten und $\mathfrak{a} * b$ das eindeutig bestimmte Element c mit $\mathfrak{a}x \subseteq \{b\} \Longleftrightarrow c \,\big|\, x$. Für $\mathfrak{a}$, $\mathfrak{b}$ ergibt sich dann leicht $\mathfrak{a}\mathfrak{b} * c = \mathfrak{b} * (\mathfrak{a} * c)$ sowie $\{\mathfrak{a}, \mathfrak{b}\} * \mathfrak{c} = \mathfrak{a} * \mathfrak{c} \vee \mathfrak{b} * \mathfrak{c}$ $(= \mathfrak{a} * \mathfrak{c} \cap \mathfrak{b} * \mathfrak{c})$.

Wie wir sofort sehen, bildet der Bereich $\mathfrak{V}$ der v-Ideale eine verbandsgeordnete Struktur, in die $\mathfrak{S}$ als komplementäre Halbgruppe eingebettet ist. Darüber hinaus erfüllt $\mathfrak{V}$ alle „wünschenswerten" Distributivgesetze, wie wir zeigen werden. Um dies herzuleiten, beachten wir (3.74). Hiermit folgt unmittelbar

$$\mathfrak{a} \cdot (\mathfrak{a} * \{c\}) \;=\; \mathfrak{a} \vee \{c\} = \mathfrak{a} \cap \{c\} \tag{3.75}$$

und somit weiter:

$$\{c\} \vee \mathfrak{a} \;=\; \{c \vee a_1, \ldots, c \vee a_n\}\,. \tag{3.76}$$

DENN: $\mathfrak{a} \cdot (\mathfrak{a} * \{c\}) \supseteq \{c \vee a_1, \ldots, c \vee a_n\}$ ist evident, und es gilt

$$\begin{aligned} \mathfrak{a} \cdot (\mathfrak{a} * \{c\}) &= \{a_1(\mathfrak{a} * \{c\}), \ldots, a_n(\mathfrak{a} * \{c\})\} \\ &\subseteq \{a_1 \vee c, \ldots, a_n \vee c\}\,. \end{aligned}$$ □

Zusammenfassend erhalten wir hiernach:

3. 3. 15 Proposition. *Der Bereich der endlichen v-Ideale einer komplementären Halbgruppe erfüllt stets die Gleichungen:*

(D) $$\mathfrak{a} \cap (\mathfrak{b}\,,\,\mathfrak{c}) = \{(\mathfrak{a} \cap \mathfrak{b}), \mathfrak{a} \cap \mathfrak{c}\}$$

(D∨) $$\mathfrak{a} \cdot (\mathfrak{b} \cap \mathfrak{c}) = \mathfrak{a} \cdot \mathfrak{b} \cap \mathfrak{a} \cdot \mathfrak{c}$$

(D∧) $$\mathfrak{a} \cdot (\mathfrak{b}\,,\,\mathfrak{c}) = \{\mathfrak{a} \cdot \mathfrak{b}\,,\,\mathfrak{a} \cdot \mathfrak{c}\}$$

bzw. in Verbandssymbolik

(D) $$\mathfrak{a} \vee (\mathfrak{b} \wedge \mathfrak{c}) = (\mathfrak{a} \vee \mathfrak{b}) \wedge (\mathfrak{a} \vee \mathfrak{c})$$

(D∨) $$\mathfrak{a} \cdot (\mathfrak{b} \vee \mathfrak{c}) = \mathfrak{a} \cdot \mathfrak{b} \vee \mathfrak{a} \cdot \mathfrak{c}$$

(D∧) $$\mathfrak{a} \cdot (\mathfrak{b} \wedge \mathfrak{c}) = \mathfrak{a} \cdot \mathfrak{b} \wedge \mathfrak{a} \cdot \mathfrak{c}$$

BEWEIS. Dies ist klar für (D∧) und folgt für (D) analog dem Beweis zu 3.3.4.
Seien nun $\mathfrak{a} = \{a_1, \ldots, a_m\}$, $\mathfrak{b} = \{b_1, \ldots, b_n\}$, $\mathfrak{c} = \{c_1, \ldots, c_p\}$ gegeben. Dann folgen die beiden Gleichungen:

$$\mathfrak{a} \cdot \mathfrak{b} \,\cap\, \mathfrak{a} \cdot \mathfrak{c} = \{a_i\, b_k \vee a_j\, c_\ell\} \;\; (1 \le i, j \le m, 1 \le k \le n, 1 \le \ell \le p)$$

und

$$\mathfrak{a} \cdot (\mathfrak{b} \,\cap\, \mathfrak{c}) = \{a_i\, b_k \vee a_i\, c_\ell\} \;\; (1 \le i \le m, 1 \le k \le n, 1 \le \ell \le p)$$

und es bleibt zu zeigen:

$$\mathfrak{a} \cdot \mathfrak{b} \cap \mathfrak{a} \cdot \mathfrak{c} \subseteq \mathfrak{a} \cdot (\mathfrak{b} \cap \mathfrak{c})$$

Es gilt aber

$$a_i b_k \vee a_j c_\ell \in \{a_i b_k, a_i c_\ell\} \cap \{a_j b_k, a_j c_\ell\}) \subseteq \mathfrak{a} \cdot (\mathfrak{b} \cap \mathfrak{c})$$

Damit sind wir am Ziel. □

Wir wenden uns nun den endlichen idempotenten v-Idealen zu. Hier erhalten wir wegen $\mathfrak{a} = \mathfrak{a}^2 \Longrightarrow \mathfrak{a} \cdot \{x\} \supseteq \mathfrak{a} \vee \{x\}$ zunächst:

(3.83) $$\mathfrak{a} = \mathfrak{a}^2 \Longrightarrow \mathfrak{a} \cdot x = x \cdot \mathfrak{a} \;\&\; \mathfrak{a} * x = x : \mathfrak{a} \;\&\; \mathfrak{a} \cdot x = \mathfrak{a} \cdot (\mathfrak{a} * x)\,.$$

Weiter erhalten wir die beiden Gleichungen:

$$\{a * b, b * a\}^2 = \{a * b, b * a\} \tag{3.84}$$

$$(a * b) * (b * a) = b * a = (b * a) : (a * b)\,. \tag{3.85}$$

DENN: Zunächst erhalten wir

$$\begin{aligned} a * b &= \{a, b\}(b * a) * b \\ &= (b * a) * \Big(\{a, b\} * b\Big) \\ &= (b * a) * (a * b) \end{aligned}$$

Setzen wir nun $\mathfrak{u} := \{a * b, b * a\}$, so folgt weiter

$$\mathfrak{u} * \{a * b\} = \{b * a\} * \{a * b\} = \{a * b\}$$

und

$$\mathfrak{u}(\mathfrak{u} * \{a * b\}) = \{a * b\}$$

Das liefert uns dann (3.84) *via*

$$\begin{aligned} \{a * b, b * a\}^2 &= \{\mathfrak{u} \cdot (a * b), \mathfrak{u} \cdot (b * a)\} \\ &= \{a * b, b * a\} \end{aligned}$$

Schließlich erhalten wir (3.85) vermöge

$$\begin{aligned} (a * b) : (b * a) &= (a * b) : \mathfrak{u} \\ &= \mathfrak{u} * (a * b) \\ &= (b * a) * (a * b) \\ &= a * b\,. \end{aligned}$$

Damit sind wir am Ziel. □

Hilfssatz (3.84) liefert als weitere Folgerungen:

$$(a * b)(b * a) = (b * a)(a * b) \tag{3.86}$$

$$x \leq a * b, b * a \Longrightarrow x(a * b) = a * b = (a * b)x\,. \tag{3.87}$$

DENN: Der Beweis der ersten Behauptung verläuft analog zum Beweis von (3.73) . Der zweite Teil ergibt sich aus (3.84) wegen $\{a * b, b * a\}(a * b) = a * b \Longrightarrow x(a * b) = a * b$ und Hilfssatz (3.83) . □

Eine komplementäre Halbgruppe heiße *normal,* wenn sie das Gesetz erfüllt:

$$(a * b) \wedge (b * a) = 1 = (a : b) \wedge (b : a) \tag{N}$$

3. 3. 16 Proposition. *Normale komplementäre Halbgruppen sind durch jedes der beiden nachfolgenden Gesetze* (N') *bzw.* (N*) charakterisiert:

$$\text{(N')} \qquad b:(a*b) \vee a:(b*a) \;=\; a \wedge b$$
$$\text{(N}^*\text{)} \qquad (a*b) \wedge (b*a) \;=\; 1\,.$$

BEWEIS. Es gilt stets

$$a, b \geq b:(a*b) \vee a:(b*a)\,.$$

Sei nun zudem (N*) erfüllt. Dann folgt für jedes c mit $c \,\big|\, a, b$ bezüglich des Elementes $x := b:(a*b) \vee a:(b*a)$, man beachte (3.72) ,

$$\begin{aligned} c \,\big|\, a \;\&\; c \,\big|\, b \;\Longrightarrow\;& x*c \leq x*b \leq a*b \\ \&\;& x*c \leq x*a \leq b*a \\ \Longrightarrow\;& x*c \leq (a*b) \wedge (b*a) = 1 \\ \Longrightarrow\;& c \,\big|\, x \end{aligned}$$

und damit insgesamt (N') . Sei hiernach (N') erfüllt. Dann folgt

$$\begin{aligned} (a:b) \wedge (b:a) &= ((a:b):((b:a)*(a:b))) \\ &\vee\; ((b:a):((a:b)*(b:a))) \\ &= ((a:b):(a:b)) \vee ((b:a):(b:a)) \\ &= 1\,. \end{aligned}$$

Damit ist aus Dualitätsgründen alles gezeigt. □

Für $\wedge$-abgeschlossene komplementäre Halbgruppen gilt noch ein Satz, der für den kommutativen Fall bereits in [158] bewiesen wurde, jedoch mit einer Methode, die sich nicht übernehmen lässt. Wir zeigen:

3. 3. 17 Proposition. *Eine $\wedge$-abgeschlossene komplementäre Halbgruppe $\mathfrak{S}$ ist genau dann normal, wenn sie eines der beiden Gesetze erfüllt:*

$$\text{(N}^*\wedge\text{)} \qquad a*(b \wedge c) \;=\; (a*b) \wedge (a*c)$$
$$\text{(N}^*\vee\text{)} \qquad (a \vee b)*c \;=\; (a*c) \wedge (b*c)\,.$$

BEWEIS. Ist $\mathfrak{S}$ normal, so folgt zunächst für $a \leq b \wedge c$:

$$\begin{aligned} a*(b \wedge c) &= (a*(b \wedge c))((b*c) \wedge (c*b)) \\ &= (a*(b \wedge c))((b \wedge c)*c) \\ &\wedge\; (a*(b \wedge c))((b \wedge c)*b) \\ &= (a*b) \wedge (a*c)\,. \end{aligned}$$

Nehmen wir hiernach a beliebig an, so ist – wie behauptet:

$$\begin{aligned} a*(b\wedge c) &= a*(a\vee(b\wedge c)) \\ &= a*((a\vee b)\wedge(a\vee c)) \\ &= (a*(a\vee b))\wedge(a*(a\vee c)) \\ &= (a*b)\wedge(a*c)\,,. \end{aligned}$$

Umgekehrt impliziert (N$^*\wedge$)

$$\begin{aligned} (a*b)\wedge(b*a) &= ((a\wedge b)*b)\wedge((a\wedge b)*a) \\ &= (a\wedge b)*(b\wedge a)=1\,. \end{aligned}$$

Analog liefert uns das Gesetz (N$^*\vee$)

$$\begin{aligned} (a*b)\wedge(b*a) &= (a*(a\vee b))\wedge(b*(a\vee b)) \\ &= (a\vee b)*(b\vee a)=1\,. \end{aligned}$$

Schließlich liefert (N) zunächst für $a\vee b\le c$ die Gleichung

$$\begin{aligned} (a\vee b)*c &= (a*b\wedge b*a)((a\vee b)*c)) \\ &= ((a*(a\vee b))\wedge((b*(a\vee b))) \\ &\quad\ \cdot((a\vee b)*c) \\ &= (a*(a\vee b))((a\vee b)*c) \\ &\wedge\ (b*(a\vee b))((a\vee b)*c) \\ &= (a*c)\wedge(b*c)\,, \end{aligned}$$

und damit allgemein:

$$\begin{aligned} (a\vee b)*c &= ((a\vee b)\wedge c)*c \\ &= ((a\wedge c)\vee(b\wedge c))*c \\ &= ((a\wedge c)*c)\wedge((b\wedge c)*c) \\ &= a*c\wedge b*c\,. \end{aligned}$$

□

Aus (3.87) folgt noch

3. 3. 18 Lemma. *Eine komplementäre Halbgruppe ist schon dann normal, wenn sie eines der beiden nachfolgenden Gesetze erfüllt:*

(BV') $\qquad a:(b*a) = b:(a*b)$

(BV) $\qquad a:(b*a) = (b:a)*b\,.$

BEWEIS. Es gilt stets $\qquad a,b \ \ge\ a:(b*a)\,.$

und es folgt unter Voraussetzung von (BV')

$$a, b \geq c \Longrightarrow a : (b * a) \ \geq \ a : (c * a) = c : (a * c) = c.$$

Daher ist $a : (b*a) = a \wedge b = b : (a*b)$ erfüllt, und wir können zurückgreifen auf 3.3.16. Analog schließen wir im Fall (BV). □

Im letzten Teil dieses Paragraphen befassen wir uns mit der Arithmetik der *kürzbaren* Elemente. Sie sind offenbar charakterisiert durch die Gleichung $(a * a(xa : a)) * x = 1$. Eine weitere wichtige Charakterisierung, die eine entscheidende Rolle bei der Konstruktion der Quotientenhülle spielen wird, lernen wir im Anschluss an den nun folgenden Satz kennen.

3. 3. 19 Proposition. *Die Menge der kürzbaren Elemente einer jeden komplementären Halbgruppe bildet ein operativ abgeschlossenes Ordnungsideal* C *.*

BEWEIS. Natürlich ist das Einselement 1 kürzbar, und es ergibt sich fast unmittelbar, dass mit a und b auch ab und mit ab auch a kürzbar ist. Hieraus resultiert die Kürzbarkeit von $a * b,\ b : a,\ a \vee b$ und – im Falle seiner Existenz – die Kürzbarkeit von $a \wedge b$. Dass für ein jedes kürzbare a alle $a \wedge b$ existieren, folgt aus $a*b, b*a \geq x \Longrightarrow x(b*a) = 1(b*a) \Longrightarrow x = 1$ und dem ersten Teil des Beweises zu 3.3.16 □

Nun bringen wir die angekündigte Charakterisierung:

3. 3. 20 Proposition. *Ein Element aus* $\mathfrak{S}$ *ist kürzbar gdw. es als* a *mit allen Paaren* b, c *bzw. als* b *mit allen Paaren* a, c *die Gleichungen erfüllt:*

(C*) $$a * bc \ = \ (a * b)\big((b * a) * c\big)$$

(C$^:$) $$cb : a \ = \ \big(c : (a : b)\big)(b : a)\,.$$

BEWEIS. Genügt x den Bedingungen des Satzes, so wähle man $a = b = x$. Dann erhält man $x * xc = (x * x)\big((x * x) * c\big) = c = \big(c : (x : x)\big)(x : x) = cx : x$.
Umgekehrt kann man zeigen:

$$\begin{array}{rcl} a(a * b)\big((b * a) * c\big) & = & b(b * a)\big((b * a) * c\big) \\ & \geq & bc \\ & \rightsquigarrow & \\ (a * b)\big((b * a) * c\big) & \geq & a * bc\,. \end{array}$$

Weiter gilt wegen $a * bc \geq a * b$ etwa $a * bc = (a * b)y$ und damit dann

$$a(a * b)y \;\geq\; bc\ .$$

Hieraus ergibt sich für kürzbares a oder b als nächstes die Implikation:

$$\begin{array}{rcl}
(a \wedge b)(b * a)(a * b)y & \geq & (a \wedge b)(a * b)c \\
& \rightsquigarrow & \\
(b * a)(a * b)y & \geq & (a * b)c \\
& \rightsquigarrow & \\
(a * b)(b * a)y & \geq & (a * b)c\ .
\end{array}$$

Wir untersuchen den weiteren Sachverhalt zunächst für $a \in C$. Dann gilt auch $b * a \in C$, weshalb wir – man beachte $a * bc = (a * b)y$ – die Herleitung erhalten:

$$\begin{array}{rcl}
(b * a)(a * b)y & = & (a * b)(b * a)y \\
& \geq & (a * b)c \vee (a * b)(b * a) \\
& = & (a * b)\big(c \vee (b * a)\big) \\
& = & (a * b)(b * a)\big((b * a) * c\big) \\
& = & (b * a)(a * b)\big((b * a) * c\big) \\
& \rightsquigarrow & \\
a * bc = (a * b)y & \geq & (a * b)\big((b * a) * c\big)
\end{array}$$

Ist hingegen b aus C, also auch $a * b$ aus C, so schließen wir:

$$\begin{array}{lrcl}
& (a * b)(b * a)y & \geq & (a * b)c \\
\rightsquigarrow & (b * a)y & \geq & c \\
\rightsquigarrow & y & \geq & (b * a) * c \\
\rightsquigarrow & x = (a * b)y & \geq & (a * b)\big((b * a) * c\big) \\
\rightsquigarrow & x = a * bc & \geq & (a * b)\big((b * a) * c\big)\ .
\end{array}$$

Der Rest folgt dual. □

Abschließend halten wir für spätere Entwicklungen noch fest:

3. 3. 21 Proposition. *Ist $\mathfrak{S}$ kürzbar, so gelten die Regeln:*

(3.97) $$x * y \;\perp\; y * x$$

DENN: $(a \wedge b)(a * b) \wedge (b * a) = a \wedge b.$ $\square$

(3.98) $$u \perp v \iff u * v = v$$

DENN: $u * v = (a \wedge v) * v\,.$ $\square$

(3.99) $$(a \wedge b) * c \;=\; a * c \vee b * c$$

DENN: Vergleiche (3.71). $\square$

(3.100) $$a * (b \vee c) \;=\; a * b \vee a * c$$

DENN: Vergleiche (3.69). $\square$

(3.101) $$a * (b \wedge c) \;=\; a * b \wedge a * c$$

DENN: Vergleiche ($\mathrm{N}^*\wedge$). $\square$

(3.102) $$(a \vee b) * c \;=\; a * c \wedge b * c$$

DENN: Vergleiche ($\mathrm{N}^*\vee$). $\square$

(3.103) $$a \wedge (b \vee c) \;=\; (a \wedge b) \vee (a \wedge c)$$

DENN: Vergleiche 3.3.4. $\square$

(3.104) $$u \perp v \iff uv = vu$$

DENN: Beachte (3.73) $\square$

(3.105) $$a(b \wedge c) \;=\; ab \wedge ac$$

DENN: Beachte 3.3.3. $\square$

(3.106) $$a \wedge bc \;\overset{(3.105)}{=}\; a \wedge (a \wedge b)c$$

(3.107) $$a \,\big|\, bc \;\&\; a \perp b \;\overset{(3.105)}{\Rightarrow}\; a \,\big|\, c\,.$$

3.4 Komplementäre Halbgruppen und Ringe

3. 4. 1 Definition. Eine Teilmenge $\mathfrak{a}$ von S heißt ein *t-Ideal,* wenn sie mit jeder endlichen Teilmenge $E \subseteq \mathfrak{a}$ auch das von E erzeugte v-Ideal enthält. Die Arithmetik der t-Ideale entspricht der Arithmetik der v-Ideale. Insbesondere erzeugt jede Teilmenge A von S ein eindeutig bestimmtes feinstes t-Ideal A_t, das wir erhalten, wenn wir alle $(A_i)_t$ mit endlichem $A_i \subseteq A$ zu ihrer mengentheoretischen Vereinigung zusammen führen. U.a. gilt die Implikation

$$A_t = B_t \;\&\; C_t = D_t \implies \langle AC\rangle_t = \langle BD\rangle_t\,,$$

deren Bestätigung hier dem Leser überlassen bleibe.
Jedoch, im Gegensatz zu v-Idealen, sind t-Ideale von *endlichem Charakter,* womit gemeint ist, das jedes Element aus A_t schon in einem E_t enthalten ist, mit einem endlichen E aus A.
Offenbar haben wir $a_v := \langle a\rangle_v = \langle a\rangle = a_t := \langle a\rangle_t = aS$. Folglich hat $\mathfrak{S}$ die GGT-Eigenschaft, falls jedes v-Ideal eins-erzeugt, also ein Haupt-v-ideal ist, und – genau so wie im Falle von Dedekind-Idealen, hier abgekürzt als d-Ideale – erfüllen v-Ideale und auch t-Ideale das Gesetz;

$$(\mathrm{D}^t) \qquad \langle a\rangle_t \cdot \langle b, c\rangle_t \;=\; \langle ab, ac\rangle_t\,.$$

Von nun an bedeute Ideal stets t-Ideal.
Wir notieren Hauptideale mittels kleiner Buchstabe im sf-Format. während Kleinbuchstaben im Frakturformat zu Bezeichnung von Idealen im Allgemeinen dienen werden.

3. 4. 2 Definition. Ein Monoid $\mathfrak{S}$ heiße ring-artig, wenn es ein Null-Element 0 enthält, worauf bezogen die Ideale der Implikation genügen:

$$(\mathrm{D}^t) \qquad \mathsf{a}\cdot\mathfrak{u} = \mathsf{a} \Longrightarrow \exists\, \mathfrak{u}^*\perp\mathfrak{u} : \mathsf{a}\cdot\mathfrak{u}^* = 0\,.$$

Sei im weiteren $\mathfrak{S}$ eine ringartige komplementäre Halbgruppe und sei $\mathfrak{A}$ die korrespondierende Ideal-Erweiterung. Man beachte, dass $\mathfrak{S}$ isomorph ist zu der Halbgruppe der Hauptideale, die jedoch über die Multiplikation hinaus in $\mathfrak{A}$ noch *via* $\mathfrak{a}+\mathfrak{b} := (\mathfrak{a}, \mathfrak{b})$ auch eine Addition zulassen – sowie die Konstruktion von Quotienten (in $\mathfrak{A}$). Aus diesem Grunde werden wir mit

Hauptidealen kalkulieren statt mit Elementen. Als ein erstes Hauptergebnis erhalten wir:

$$\begin{aligned} \mathsf{b} : \mathsf{a} = \mathsf{c} \quad \& \quad & \mathsf{a}\mathfrak{u} = \mathsf{a} \;\&\; \mathsf{c}\mathfrak{u} = \mathsf{c} \\ \Longrightarrow \quad & \mathsf{b} \supseteq \mathsf{a}(\mathfrak{u}^* + \mathsf{c}) \\ \Longrightarrow \quad & \mathfrak{u} \supseteq \mathsf{c} \supseteq (\mathfrak{u}^* + \mathsf{c}) \\ \Longrightarrow \quad & \mathfrak{u} \supseteq \mathfrak{u}^* \Rightarrow \mathfrak{u} = 1\,. \end{aligned} \tag{3.110}$$

Dies impliziert in jedem Falle

$$\mathsf{u} = \mathsf{u}^2 \supseteq \mathsf{a}^2 : \mathsf{a} \neq 0 \Longrightarrow \mathsf{u} = 1\,. \tag{3.111}$$

Sei hiernach $\mathfrak{S}$ eine komplementäre Halbgruppe. Dann folgt wegen

$$s\big|Av \Longrightarrow s : v\big|A \Longrightarrow (s : v)\big|c \Longrightarrow (s : v)v\big|cv \Longrightarrow s\big|cv$$

zunächst:

$$c \in \mathfrak{a} \Longleftrightarrow s \;\big|\; \mathfrak{a} \Longrightarrow s\big|c \tag{3.112}$$

Weiterhin erhalten wir, vgl. 3.74,

$$\langle a_1, \ldots, a_n \rangle \supseteq \mathsf{b} \iff \langle a_1, \ldots, a_n \rangle \cdot \textstyle\bigvee_1^n (b : a_i) = \mathsf{b}\,, \tag{3.113}$$

wie der Leser bestätige. Dies liefert dann weiter:

$$(\mathsf{a} : \mathsf{b}) : (\mathsf{b} : \mathsf{a}) = \mathsf{a} : \mathsf{b} \tag{3.114}$$

$$(\mathsf{a} : \mathsf{b} + \mathsf{b} : \mathsf{a})^2 = \mathsf{a} : \mathsf{b} + \mathsf{b} : \mathsf{a} \tag{3.115}$$

da (3.114) aus

$$\begin{aligned} \mathsf{a} : \mathsf{b} &= \mathsf{a} : (\mathsf{a} + \mathsf{b})(\mathsf{b} : \mathsf{a}) \\ &= (\mathsf{a} : (\mathsf{a} + \mathsf{b})) : (\mathsf{b} : \mathsf{a}) \\ &= (\mathsf{a} : \mathsf{b}) : (\mathsf{b} : \mathsf{a}) \end{aligned}$$

folgt und $\mathfrak{u} := a : b + b : a$ zu (3.115) führt, wegen

$$\begin{aligned} (a : b + b : a)^2 &= (a : b) \cdot \mathfrak{u} + (b : a) \cdot \mathfrak{u} \\ &= a : b + b : a\,. \end{aligned}$$

Sei hiernach $\mathfrak{S}$ ringartig und komplementär. Dann erfüllt $\mathfrak{A}$ nach (3.111):

$$\mathsf{a} : \mathsf{b} + \mathsf{b} : \mathsf{a} = 1\,. \tag{3.116}$$

Dies führt insbesondere, siehe oben, zu

$$\mathsf{a} : (\mathsf{b} \vee \mathsf{c}) \;=\; a : b + a : c\,. \tag{3.117}$$

3. 4. 3 Proposition. *Sei $\mathfrak{S}$ eine ringartige komplementäre Halbgruppe. Dann sind paarweise äquivalent:*

(a) *Jedes* a *besitzt eine Zerlegung* $\mathsf{u} \cdot \mathsf{v}$ *mit idempotentem* u *und kürzbarem* v.

(b) $\mathfrak{S}$ *ist semiprim, d.h.* $\mathfrak{S}$ *erfüllt* $\mathsf{a}^2 = 0 \Longrightarrow \mathsf{a} = 0$.

BEWEIS. (a)$\Longrightarrow$(b). Sei $\mathsf{a} = \mathsf{uv}$, $u = u^2$ und v kürzbar. Dann folgt

$$\mathsf{a}^n = 0 \Longrightarrow (\mathsf{uv})^n = 0 \Longrightarrow \mathsf{uv}^n = 0 \Longrightarrow \mathsf{u} = 0 \Longrightarrow \mathsf{a} = 0\,,$$

weshalb $\mathfrak{A}$ semiprim ist.
(b)$\Longrightarrow$(a) Aus der Annahme resultiert

$$\mathsf{b} \cdot \mathsf{c} = 0 \Longrightarrow (\mathsf{bc})^2 = 0 = (\mathsf{c} \vee \mathsf{b})^2 \Longrightarrow \mathsf{b} \vee \mathsf{c} = 0 = \mathsf{b} \cdot \mathsf{c}\,. \tag{3.118}$$

Daher erhalten wir im Falle $\mathsf{b} \neq 0$ zum einen $0 : \mathsf{c} =: \mathsf{v} \neq 0$ und zum anderen $1 \neq 0 : \mathsf{v} =: \mathsf{u} \leq \mathsf{c}$ was mittels

$$0 : (0 : (0 : \mathsf{u})) = 0 : \mathsf{u} = 0 : (0 : \mathsf{v})) = \mathsf{v}$$

und

$$\mathsf{u} \vee \mathsf{v} = \mathsf{uv} = 0$$

nach sich zieht

Es gilt

$$\mathsf{u} + \mathsf{v} = 0 : \mathsf{v} + 0 : \mathsf{u} = 0 : (\mathsf{u} \vee \mathsf{v}) = 1$$

also auch

$$\mathsf{u} \perp \mathsf{v}\ \&\ \mathsf{u}^2 \big| \mathsf{uv} = 0 \Longrightarrow \mathsf{u} = \mathsf{u}^2 \leq \mathsf{c}\,.$$

Demzufolge muss im Falle $\mathsf{b} \neq 0$ das Element c einen eigentlichen idempotenten Teiler besitzen
Insbesondere würde $\mathsf{a}^2 : \mathsf{a}$ einen eigentlichen idempotenten Teiler besitzen, falls $\mathsf{x} \neq 0\ \&\ \mathsf{x} \cdot (\mathsf{a} * \mathsf{a})^2 = 0$ erfüllt wäre, was wegen (3.111) nicht möglich ist . Somit ist $a^2 : a$ kürzbar. Es ist aber

$$(\mathsf{a} : (\mathsf{a}^2 : \mathsf{a})\underline{)(}\mathsf{a}^2 : \mathsf{a}) \cdot (\mathsf{a} : (\mathsf{a}^2 : \mathsf{a}\underline{))(}\mathsf{a}^2 : \mathsf{a}) = \mathsf{a}^2 = (\mathsf{a}^2 : \mathsf{a})(\mathsf{a} : (\mathsf{a}^2 : \mathsf{a})) \cdot (\mathsf{a}^2 : \mathsf{a}),$$

woraus $(\mathsf{a} : (\mathsf{a}^2 : \mathsf{a}))^2 = (\mathsf{a} : (\mathsf{a}^2 : \mathsf{a}))$ resultiert, also

$$\mathsf{a} = (\mathsf{a} : (\mathsf{a}^2 : \mathsf{a}))(\mathsf{a}^2 : \mathsf{a}) =: \mathsf{u} \cdot \mathsf{v}$$

mit idempotenten u und kürzbarem v. □

3. 4. 4 Proposition. *Für eine ring-artige komplementäre Halbgruppe $\mathfrak{S}$ mit der v-Ideal-Erweiterung $\mathfrak{A}$ sind die nachfolgenden Bedingungen paarweise äquivalent:*

(a) *$\mathfrak{A}$ hat die Noether-Eigenschaft und jedes $\mathsf{a} : \mathsf{b}$ ist eine Hauptideal.*
(b) *Jedes a ist Produkt von vollständig primen Hauptidealen aus $\mathfrak{S}$.*
(c) *Jedes $\mathfrak{a}$ ist ein Hauptideal.*

BEWEIS. (a)$\Longrightarrow$(b). Wegen der Noether-Eigenschaft zerfällt jedes a in halbprime Hauptideale.
In einer komplementäre Halbgruppe erfüllt aber jedes Halbprimelement p die Bedingung $\mathsf{p} \supseteq \mathsf{ab} \Longrightarrow (\mathsf{p} : \mathsf{b}) : \mathsf{a} = 1$, weshalb p sogar prim ist, and darüber hinaus gilt

$$\mathsf{p}^n \supseteq \mathsf{ab} \;\&\; \mathsf{p} \not\supseteq \mathsf{a} \Longrightarrow \mathsf{p}^n \supseteq \mathsf{p}^n + (\mathsf{a} + \mathsf{p})^n \mathsf{b} = \mathsf{p}^n + \mathsf{b} \supseteq \mathsf{b}\,,$$

weshalb p sogar vollständig prim ist.
(b)$\Longrightarrow$(c). Zunächst erhalten wir $\mathsf{p}^k \supseteq \mathsf{a} \;\&\; \mathsf{p}^{k+1} \not\supseteq \mathsf{a} \;\&\; \mathsf{p}^{k+\ell} \supseteq \mathsf{ax} \Longrightarrow \mathsf{p}^\ell \big| \mathsf{x}$, d.h. jedes a besitzt eine eindeutige unverkürzbare Primfaktorzerlegung. Sei nun $\mathsf{b} = \prod \mathsf{p}_i{}^{n_i}$ diese eindeutige Darstellung von b. Dann wählen wir zu jedem i den Exponenten ℓ_i im obigen Sinne und erhalten $\mathsf{b} : \mathsf{a} = \prod \mathsf{p}_i{}^{\ell_i}$. Daher ist $\mathfrak{S}$ komplementär. Als nächstes gilt wegen (3.116) die Gleichung

$$\mathsf{a} : (\mathsf{a} : \mathsf{b}) \vee \mathsf{b} : (\mathsf{b} : \mathsf{a}) = \mathsf{a} + \mathsf{b}\,, \tag{3.119}$$

man beachte

$$\mathsf{a} + \mathsf{b} \subseteq \mathsf{a} : (\mathsf{a} : \mathsf{b}) \vee \mathsf{b} : (\mathsf{b} : \mathsf{a})$$

und

$$\begin{aligned}(\mathsf{a} + \mathsf{b}) : \big(\mathsf{a} : (\mathsf{a} : \mathsf{b}) \vee \mathsf{b} : (\mathsf{b} : \mathsf{a})\big) &\supseteq \big(\mathsf{a} : (\mathsf{a} : (\mathsf{a} : \mathsf{b}))\big) + \big(\mathsf{b} : (\mathsf{b} : (\mathsf{b} : \mathsf{a}))\big) \\ &= \mathsf{a} : \mathsf{b} + \mathsf{b} : \mathsf{a} = 1\,.\end{aligned}$$

Es ist aber $\mathsf{a} : (\mathsf{a} : \mathsf{b}) \vee \mathsf{b} : (\mathsf{b} : \mathsf{a})$ 1-erzeugt. Folglich können wir schreiben: $\mathsf{a} + \mathsf{b} = \mathsf{a} \wedge \mathsf{b}\,.$

Sei nun $\mathsf{0} = \mathsf{p}_1^{n_1} \cdot \ldots \cdot \mathsf{p}_i^{n_i} \cdot \ldots \cdot \mathsf{p}_k^{n_k}$ die Zerlegung der $\mathsf{0}$. Dann dürfen wir annehmen, dass kein p_i eine anderes $\mathsf{p}_j \neq \mathsf{p}_i$, teilt und dass $\mathsf{1} \neq \mathsf{a} \supset \mathsf{p}_i \neq \mathsf{p}_i{}^2$ zu $\mathsf{a} = \mathsf{1}$ führt, da aus $a \neq 1$ die Implikation

$$\begin{aligned} \mathsf{p}^2 = \mathsf{p} \cdot (\mathsf{pa} + \mathsf{a}^*) \,\&\, \mathsf{p}^2 \not\supseteq \mathsf{p} &\Longrightarrow p \supseteq (pa + a^*) \\ &\Longrightarrow a \supseteq p \supseteq pa + a* \\ &\Longrightarrow 1 \neq a \supseteq a^*\,, \end{aligned}$$

resultieren würde, mit Widerspruch.
Weiterhin haben wir $\mathsf{au} = \mathsf{a} \supset \mathsf{p} \Longrightarrow \mathsf{au}^* = \mathsf{0} \Longrightarrow \mathsf{u} \supseteq \mathsf{p} \supseteq \mathsf{u}^* \Longrightarrow \mathsf{u} = \mathsf{1}$ und somit $\mathsf{ax} = \mathsf{ay} \supset \mathsf{p} \Longrightarrow \mathsf{a}(\mathsf{x}+\mathsf{y})\mathsf{x}' = \mathsf{a}(\mathsf{x}+\mathsf{y}) \Longrightarrow \mathsf{x}' = \mathsf{1}$, also das Kürzungsgesetz für die Menge aller $\mathsf{a} \supset \mathsf{p}$.
Dies führt dann schließlich zu einer direkten Zerlegung von $\mathfrak{S}$ durch die idempotenten Potenzen $\mathsf{u}_i := \mathsf{e}^{n_i}$ deren Faktoren in jedem Falle faktoriell sind und zudem primär oder kürzbar mit $\mathsf{0}$. Das zieht dann sie aufsteigende Kettenbedingung für Hauptideale nach sich und damit die Noether-Eigenschaft, zur Erinnerung

$$\mathfrak{a} \supset \mathfrak{b} \supseteq \mathsf{b} \,\&\, \mathfrak{a} \setminus \mathfrak{b} \supseteq \mathsf{a} \Longrightarrow \mathfrak{a} \setminus \mathfrak{b} \supseteq \mathsf{b} \wedge \mathsf{a} \supset \mathsf{b}\,.$$

Folglich ist jedes $\mathfrak{a}$ endlich erzeugt und wir haben schon oben gesehen, dass jedes endlich erzeugte Ideal ein Hauptideal ist.
Schließlich folgt (c)$\Longrightarrow$(a) *per definitionem.* □

3.5 Archimedizität und Vollständigkeit

3. 5. 1 Definition. Eine komplementäre Halbgruppe heiße vollständig, wenn jede nach oben beschränkte Menge nach oben begrenzt ist.
Eine komplementäre Halbgruppe heiße archimedisch, wenn sie dem Gesetz genügt:

$$a^n \,\big|\, b \ \ (\forall n \in \mathbf{N}) \Longrightarrow ab = b = ba$$

3. 5. 2 Proposition. *Jede vollständige komplementäre Halbgruppe ist archimedisch.*

BEWEIS. Sei $a^n \,\big|\, b$ $(\forall n \in \mathbf{N})$ und sei $b * ba = x$ sowie $\bigvee x^n = y$. Dann ist $x^n * x^{n+1} = x$ $(\forall n \in \mathbf{N})$ und folglich $y \leq x * y$, also $y = x * y$ und daher $yx = y$, woraus dann $ba = b(b * ba) = bx = b$ resultiert.

Dies liefert die Behauptung aus Gründen der Dualität. □

3. 5. 3 Proposition. *Ist $\mathfrak{S}$ eine archimedische komplementäre Halbgruppe, so ist auch die Halbgruppe der v-Ideale von $\mathfrak{S}$ archimedisch.*

BEWEIS. Sei $\mathfrak{a}^n \supseteq \{b\}$ erfüllt und gelte $c \,\big|\, \{b\} \cdot \mathfrak{a}$. Dann folgt $b * c \,\big|\, \mathfrak{a}$ und damit $(b * c)^n \,\big|\, \{b\}$ $(\forall n \in \mathbf{N})$, also $b(b * c) = b$, was $c \,\big|\, b$ und damit $\{b\} \cdot \mathfrak{a} = \{b\}$ bedeutet. □

3. 5. 4 Proposition. *Jede kommutative archimedische komplementäre Halbgruppe lässt sich einbetten in eine vollständige komplementäre Halbgruppe.*

Dieser Satz resultiert aus dem Divisoren-Lemma aus [39], das wir im folgenden kopieren:

3. 5. 5 Das Divisoren-Lemma. *Sei $\mathfrak{A}$ ein vollständiger, kommutativer, nicht notwendig algebraischer Multiplikationsverband.*
Sei weiter $A \supseteq B \supset A(A * B)$ und $S \supseteq A(A * B)$ erfüllt und sei $B * S$ ein Divisor. Dann folgt $(B * S)^n \,\big|\, B$ $(\forall\, n \in \mathbf{N})$.

BEWEIS. Setze $A * B := X$. Dann impliziert zunächst $S \supseteq AX$

$$Y := B * S \supseteq X * S \supseteq X * AX \supseteq A \supseteq B\,, \tag{3.120}$$

und damit weiter

$$Y^1 \,\big|\, A \quad \& \quad Y^1 \,\big|\, B\,. \tag{E(1)}$$

Sei hiernach

$$Y^n \,\big|\, A \;\text{ und }\; Y^n \,\big|\, B \tag{E(n)}$$

bereits bewiesen. Dann erhalten wir *via*

$$A_1 := Y^n * A \;\text{ und }\; B_1 := Y^n * B$$

zunächst
$$\begin{aligned} A_1 * B_1 &= (Y^n * A) * (Y^n * B) \\ &= A * B \\ &= X \end{aligned}$$

und damit weiter
$$B_1 \supseteq A_1 \cdot X\,.$$

Definiere nun:
$$S_1 := Y^n * S\,.$$

Dann folgt
$$\begin{aligned} S_1 &\supseteq Y^n * A \cdot X \\ &\supseteq (Y^n * A) \cdot X \\ &= A_1 \cdot X \\ &= A_1 \cdot (A_1 * B_1) \\ &\& \\ B_1 * S_1 &= (Y^n * B) * (Y^n * S) \\ &= B * S = Y\,. \end{aligned}$$

Folglich bleibt (3.120) sogar dann gültig, wenn wir A durch A_1 und B durch B_1 ersetzen, weshalb

$$Y \,\big|\, A_1 \rightsquigarrow Y \,\big|\, B_1$$

also
$$Y \,\big|\, Y^n * A \rightsquigarrow Y \,\big|\, Y^n * B$$

und folglich

(E($n+1$))
$$Y^{n+1} \,\big|\, A \;\;\&\;\; Y^{n+1} \,\big|\, B$$

eintritt.
Damit sind wir am Ziel. $\square$

In [39] wird gezeigt, dass jede archimedische d-Halbgruppe also auch die Halbgruppe der endlich erzeugten v-Ideale einer archimedischen komplementären Halbgruppe, kommutativ ist. Das liefert dann als Verschärfung von 3.5.4 das

3. 5. 6 Theorem. *Jede archimedische komplementäre Halbgruppe lässt sich einbetten in eine vollständige komplementäre Halbgruppe.*

3.6 Klassische Vertreter

In diesem Abschnitt engen wir die komplementäre Halbgruppe sukzessive ein zu den in der Einleitung erwähnten klassischen Strukturen.

3. 6. 1 Definition. $\mathfrak{S}$ heiße eine *Zerlegungshalbgruppe*, wenn $\mathfrak{S}$ ein Holoid ist, also ein *kommutatives Monoid* mit $a \,\big|\, b \;\&\; b \,\big|\, a \Longrightarrow a = b$, in dem jedes Element in Vollprimfaktoren zerfällt.

3. 6. 2 Proposition. *Eine Algebra* $\mathfrak{S} = (\mathfrak{S}, \cdot, *, :)$ *ist genau dann eine* Zerlegungshalbgruppe, *wenn sie den Bedingungen genügt:*

$$
\begin{array}{llcll}
\text{(A1)} & a(a*b) & = & b(b*a) & \text{(B1)} \\
\text{(A2)} & ab*c & = & b*(a*c) & \text{(B2)} \\
\text{(A3)} & a(b*b) & = & a & \text{(B3)} \\
\text{(A4)} & c:ab & = & (c:b):a & \text{(B10)} \\
\text{(A5)} & (a:a)(b:x)c & = & c(c*b)(a*a) & \text{(B11)} \\
\text{(Z)} & \big|\, S*a \,\big| & = & n \ \ (\exists n \in \mathbf{N}) & \text{(B14)}
\end{array}
$$

BEWEIS. (a) Seien zunächst die aufgestellten Bedingungen erfüllt. Dann lässt sich jedes nicht halbprime a zerlegen in $a = bc$ mit $b = a : c$ und $c = b * a$ sowie $b \neq a \neq c$. Zerlegt man $b * a$ entsprechend und setzt man das Verfahren fort, so gelangt man nach endlich vielen Schritten zu einer Zerlegung $a = b_1 \cdot p_1$ mit $b_1 = a : p_1$ und $p_1 = b_1 * a$ mit halbprimem p_1 und $b_1 < a$. Entsprechend lässt sich b_1 zerlegen in $b_1 = b_2 \cdot p_2$ mit $b_2 = b_1 : p_2$ und $p_2 = b_2 * b_1$. Hierin ist aufgrund der Konstruktion $p_2 \cdot p_1 = b_2 * a$, weil $b_2 \cdot p_2 \cdot p_1 \leq b_2 \cdot x$ zu $x = p_2 \cdot y$ führt und damit zu $b_2 \cdot p_2 \cdot p_1 \leq b_2 \cdot p_2 \cdot y$, also zu $p_2 \cdot p_1 \leq x$.
Wegen $b_1 = a : p_1$ und $b_1 > b_2 = b_1 : p_2$ muss aber $p_1 \cdot p_2 > p_1$ gelten. Das bedeutet, dass bei sukzessiver Anwendung des Verfahrens a schließlich in ein Produkt von Halbprimfaktoren zerfällt.

(b) Sei hiernach $\mathfrak{S}$ eine Zerlegungshalbgruppe. Dann ist $\mathfrak{S}$ kommutativ, da je zwei Halbprimelemente nach 3.3.9 kommutieren. Weiter gilt

$$(a = b) \iff \big(p^n \,\big|\, a \Leftrightarrow p^n \,\big|\, b\big) \ ,$$

weshalb jedes a eine eindeutig bestimmte unverkürzbare Zerlegung in Vollprimelemente besitzt. Hieraus leitet sich der Rest der Behauptung unter Berücksichtigung von $q < p$ & p halbprim $\Longrightarrow pq = q$ leicht her. □

Wir interessieren uns als nächstes für die Klasse der komplementären Halbgruppen, in denen zu je zwei Elementen $a \neq 1, b$ ein n mit $a^n \geq b$ existiert, auch bezeichnet als die Klasse der *streng archimedischen* komplementären Halbruppen, man konsultiere [39]. Streng archimedische komplementäre Halbgruppen sind *linear geordnet,* denn wegen $(a * b) * (b * a) = b * a$ muss nach (A2) gelten $a * b = 1 \vee 1 = b * a$. Das bedeutet weiter nach Hölder und CLIFFORD, dass sich jede streng archimedische komplementäre Halbgruppe entweder einbetten lässt in die additive Halbgruppe der nicht negativen reellen Zahlen – nämlich wenn $\mathfrak{S}$ kürzbar ist – oder aber in die Halbgruppe der reellen Zahlen x mit $0 \leq x \leq 1$ bezüglich der Verknüpfung $a \circ b = \min(a + b, 1)$.

3. 6. 3 Proposition. *Eine Algebra $\mathfrak{S} = (\mathfrak{S}, \cdot, *)$ ist genau dann eine streng archimedische komplementäre Halbgruppe, wenn sie den Bedingungen genügt:*

(A1)	$a(a * b) = b(b * a)$	(B15)
(A2)	$ab * c = b * (a * c)$	(B16)
(A3)	$a(b * b) = a$	(B17)
(AA)	$a \neq 1 \neq b \Rightarrow \exists n \in \mathbf{N} \ : \ a^n \,\big|\, b \ \& \ b \,\big|\, a^{n+1}$	(B10)

BEWEIS. Zunächst ist $\mathfrak{S}$ bezüglich $\leq$ trivialerweise *linear geordnet,* da $n = 0$ nach sich zieht $b \leq a$, während andernfalls $a \leq b$ erfüllt ist. Hieraus folgt weiter $a * b \leq b$, da sonst für alle n wegen $a * xy \geq a * x$ nach (A2) $a^n * b \geq b$ einträte. Somit ist jeder Rechtsteiler von c auch ein Linksteiler von c. Weiter gilt $au = a \Longrightarrow u = 1 \vee a^2 = a$, wegen $au = a \Longrightarrow au^n = a$, also im Falle $u \neq 1$ dann $a^2 = a$. Das bedeutet aber $b \leq a$ für alle b.
Ist hingegen $ax < v$, so gilt $ax = a(a * ax)\big((a * ax) * x\big) = ax\big((a * ax) * x\big)$, was $a * ax = x$ impliziert. Und hieraus folgt weiter $ax < ay < v \Longrightarrow x < y$. Wenden wir nun das auf HÖLDER zurückgehende Verfahren zum Nachweis der Kommutativität an, so sind wir fertig.
Es sei zunächst, falls ein solches existiert, x das kleinste von 1 verschiedene Element. Dann schöpfen die Potenzen von x das gesamte S aus, wegen

$$\begin{aligned} x^n \leq a < x^{n+1} &\Longrightarrow a = x^n(x^n * a) \\ &\Longrightarrow x^n * a < x \\ &\Longrightarrow x^n * a = 1 \\ &\Longrightarrow a = x^n\,. \end{aligned}$$

Gibt es aber kein kleinstes $x \neq 1$, so erhalten wir für $ab * ba \neq 1$ ein $x \neq 1$ mit $x^2 < ab * ba$, also auch mit $x^n \leq a \leq x^{n+1}$ und $x^m \leq b \leq x^{m+1}$, was $x^{n+m} \leq ab \leq x^{n+m+2} \leq abx^2 < ba$ impliziert, mit Widerspruch zu $x^{n+m+2} \geq ba$. □

Als nächstes studieren wir den kürzbaren Fall. Hier erhalten wir als Charakterisierung:

3. 6. 4 Proposition. *Eine Algebra $\mathfrak{S} = (\mathfrak{S}, \cdot, *, :)$ ist genau dann eine kürzbare komplementäre Halbgruppe, wenn sie den Bedingungen genügt:*

$$
\begin{array}{llcll}
\text{(A1)} & a(a*b) & = & b(b*a) & \text{(B1)} \\
\text{(A2)} & ab*c & = & b*(a*c) & \text{(B2)} \\
\text{(V1)} & a*ab & = & b & \text{(B3)} \\
\text{(V2)} & a(a*b) & = & (b:a)a & \text{(B18)} \\
\text{(A5)} & ba:a & = & a*ab & \text{(B19)}
\end{array}
$$

DENN: Wegen $ab = a(a*ab) = (ab:a)a = (ab:b)b = b(b*ab)$ gilt $aS = Sa$, weshalb das eindeutig bestimmte c mit $c \cdot a = b \vee a$ *Linkskomplement* von a bezüglich b ist. □

Hiernach kommen wir zu den *booleschen Verbänden*. Sie wurden in einem besonderen Abschnitt zur Verbandstheorie vorgestellt, und der Leser ist eingeladen, dort noch einmal hinzuschauen. Unser Interesse an dieser Stelle gilt der Auffassung boolescher Algebren als rechtskomplementärer Halbgruppen.

3. 6. 5 Proposition. *Eine Algebra $\mathfrak{S} = (\mathfrak{S}, \cdot, *, \circ)$ lässt sich genau dann auffassen als eine boolesche Algebra , wenn sie den Bedingungen genügt:*

$$
\begin{array}{llcll}
\text{(A1)} & a(a*b) & = & b(b*a) & \text{(B1)} \\
\text{(A2)} & ab*c & = & b*(a*c) & \text{(B2)} \\
\text{(A3)} & a(b*b) & = & a & \text{(B3)} \\
\text{(BA)} & b\big((a\circ a)*c\big) & = & (a*b)\big((a*b)*((a*(a\circ a))*b)\big) & \text{(B10)}
\end{array}
$$

BEWEIS. Zunächst folgt nach (BA) für $b = 1$, dass $(a\circ a)*c = 1$, also $c \,\Big|_{\ell}\, a\circ a$ für alle $c \in S$ erfüllt sein muss. Das bedeutet $a\circ a = b\circ b$, also mit $0 := a\circ a$ zu $a\cdot 0 \geq a\cdot(a*0) = 0$ und $0 \leq 0\cdot x \leq 0$ führt. Setzen wir nun $a' := a*0$, so folgt nach (BA) mit $b := a'$

$$
\begin{array}{rcl}
a*a' & = & (a*a')\big((a*a')*(a'*a')\big) \\
 & = & a' \\
 & \& & \\
a'*a & = & (a*a)\big((a*a)*\big(a'*a\big)\big)\ , \\
 & = & a \\
 & \rightsquigarrow & \\
aa' = 0 = a(a*a') & = & a'(a'*a) = 0 = a'a\,.
\end{array}
$$

Gilt nun weiter $a * b = b$ und $ab = 0 = ba$, so folgt $a' = b$ wegen

$$ax \geq 0 \Longrightarrow ax \geq b \implies x \geq a * b \Longrightarrow x \geq b\,,$$

und dies führt zu

$$a^2 \; = \; a\,,$$

denn es gelten:

$$\begin{array}{rcl} a^2 * a' & = & a * (a * a') = a * a' = a' \\ & \& & \\ a^2 \cdot a' = a(aa') = a(a'a) = & 0 & = (aa')a = (a'a)a = a' \cdot a^2\,. \end{array}$$

Wegen $0 * c = 1$ ergibt sich hieraus Axiom (I1), und aus Axiom (BA) folgt $a * b \,\big|_\ell\, b$ und damit nach (3.73) die $ab = ba$.
Zu zeigen bleibt, dass $\mathfrak{S}$ $\wedge$-abgeschlossen ist und $a \wedge a' = 1$ erfüllt. Hier gilt zunächst nach (BA)

$$c \leq a, a' \Longrightarrow c = (a * c)\big((a * c) * (a' * c)\big) = 1(1 * 1) = 1\,,$$

also $a \perp a'$, und es ist

$$a * b \leq a * 0 = a' \;\text{ und }\; b * a \leq a$$

erfüllt, woraus nach (3.3.16) die $\wedge$-Abgeschlossenheit von $\mathfrak{S}$ resultiert.

Es sei nun umgekehrt $\mathfrak{S}$ eine boolesche Algebra. Dann gilt $a * b = a' \wedge b$. Denn es ist $a \vee (a' \wedge b) = a \vee b$ und haben wir weiter $y < a' \wedge b$, so muss auch $a \vee y < a \vee b$ erfüllt sein – man schneide $a \vee y$ und $a \vee (a' \wedge b)$ jeweils mit a'. Hieraus ergibt sich für $a' \wedge b =: c$ zum einen $a \vee c \geq b$ und zum anderen die Implikation

$$\begin{array}{rcl} a \vee x \geq b & \Longrightarrow & a \vee b = a \vee (x \wedge c) \\ & \Longrightarrow & x \wedge c = c \\ & \Longrightarrow & c = a' \wedge b \leq x\,. \end{array}$$

Setzen wir noch $a \circ a = 0$ für alle a, b, so erhalten wir

$$\begin{array}{rcl} (a * b) \vee ((a * (a \circ a)) * b) & = & (a * b) \vee (a' * b) \\ & = & (a \wedge a') * b \\ & = & 1 * b = b \\ & = & b\big((a \circ a) * c\big)\,, \end{array}$$

also Axiom (BA). Damit sind wir am Ziel! □

Aus Satz 3.6.5 folgt unmittelbar

3. 6. 6 Proposition. *Eine Algebra $\mathfrak{S} = (\mathfrak{S}, \cdot, *)$ lässt sich genau dann auffassen als abschnittskomplementärer distributiver Verband, wenn sie den Bedingungen genügt:*

$$
\begin{array}{llcll}
\text{(A1)} & a(a*b) & = & b(b*a) & \text{(B1)} \\
\text{(A2)} & ab*c & = & b*(a*c) & \text{(B2)} \\
\text{(A3)} & a(b*b) & = & a & \text{(B3)} \\
\text{(BR)} & (a*b)\big((a*b)*((a*c)*b)\big) & = & b*b & \text{(B10)}
\end{array}
$$

BEWEIS. Setzt man $c = a^2$ und $b = a * a^2$, so erhält man $a * a^2 = 1$, also $a^2 = a(a * a^2) = a1 = a$. Daher bilden nach 3.6.5 die Teiler eines jeden a einen booleschen Verband bilden. Umgekehrt folgt die Bedingung (BR) aus $a \wedge (a * c) = 1$ aufgrund von Satz 3.3.5. □

Im Beweis zu 3.6.5 ergab sich, dass $a' \wedge b = a * b$ erfüllt ist, was bedeutet, dass in booleschen Ringen die Festsetzung $a+b = a*b \vee b*a$ eine assoziative Operation liefert. Wir zeigen, dass diese Eigenschaft sogar charakteristisch ist. Genauer gilt:

3. 6. 7 Proposition. *Eine Algebra $\mathfrak{S} = (\mathfrak{S}, \cdot, *)$ lässt sich genau dann auffassen als ein boolescher Ring, wenn sie mit $a + b := (a * b) \cdot (b * a)$ den Bedingungen genügt:*

$$
\begin{array}{llcll}
\text{(A1)} & a(a*b) & = & b(b*a) & \text{(B1)} \\
\text{(A2)} & ab*c & = & b*(a*c) & \text{(B2)} \\
\text{(A3)} & a(b*b) & = & a & \text{(B3)} \\
\text{(BR')} & a+(b+c) & = & (a+b)+c & \text{(B10)}
\end{array}
$$

BEWEIS. Zunächst gilt trivialerweise

$$a + a = 1\ ,\ 1 + a = a + 1 = a\ ,\ a + ab = ab + a = a * ab\,.$$

Das impliziert weiter:

$$
\begin{aligned}
a * a^2 = a * ((a + a^2) + a) &= a * \big((a * a^2) * a\big) \\
&\leq a * \big((a * a^2) * a^2\big) = 1 \rightsquigarrow a^2 = a
\end{aligned}
$$

also $\qquad a * b = a * (a * b) \leq a * (a * b)(b * a) \leq a + a + b = b\,,$

was $ab = ba$ bewirkt, wegen $a, b \leq a(a*b) = b(b*a) \rightsquigarrow ab = a \vee b = ba$. Endlich gilt $x \leq a, a*b \Longrightarrow x + (a*b) = x*(a*b) = ax*b = a*b$, also $x + (a*b) = a*b \rightsquigarrow x = 1$. $\square$

Wir wenden uns nun komplementären Halbgruppen zu, in denen jedes Element in ein Produkt eines *idempotenten* u mit einem *kürzbaren* v zerfällt. Zu ihnen gehören natürlich die direkten Produkte von *brouwerschen* und *kürzbaren* komplementären Halbgruppen.

3. 6. 8 Proposition. *Eine Algebra* $\mathfrak{S} = (\mathfrak{S}, \cdot, *, :)$ *ist multiplikativ genau dann subdirektes Produkt einer kürzbaren und einer idempotenten komplementären Halbgruppe, wenn sie den Bedingungen genügt:*

$$
\begin{array}{llcll}
\text{(A1)} & a(a*b) & = & b(b*a) & \text{(B1)} \\
\text{(A2)} & ab*c & = & b*(a*c) & \text{(B2)} \\
\text{(A3)} & a(b*b) & = & a & \text{(B3)} \\
\text{(A4)} & c:ab & = & (c:b):a & \text{(B10)} \\
\text{(A5)} & (a:a)(b:c)c & = & c(c*b)(a*a) & \text{(B11)} \\
\text{(IR)} & \multicolumn{3}{l}{\Big(\big((a*a^2)*(a*a^2)\big)\big(b(a*a^2):(a*a^2)\big)\Big)*b = b*b} & \text{(B23)}
\end{array}
$$

BEWEIS. Axiom (IR) gewährleistet, dass jedes $a*a^2$ kürzbar ist, und dies impliziert:

$$
\begin{array}{rrcl}
 & a^2 & = & (a*a^2)\big((a*a^2)*a\big)\big(a:(a*a^2)\big)(a*a^2) \\
 & & = & (a*a^2)\big((a*a^2)*a\big)(a*a^2) \\
\Longrightarrow & (\star)\quad a & = & (a*a^2)\big((a*a^2)*a\big) \\
 & & = & (a*a^2)\big((a*a^2)*a\big)\big(a:(a*a^2)\big) \\
 & & = & a\big(a:(a*a^2)\big) \\
\Longrightarrow & a*a^2 & = & \big(a:(a*a^2)\big)*(a*a^2) \\
\Longrightarrow & a & = & \big(a:(a*a^2)\big)\big((a:(a*a^2))*(a*a^2)\big) \\
 & & = & (a*a^2)\big((a*a^2)*(a:(a*a^2))\big) \\
\Longrightarrow & (a*a^2)*a & = & (a*a^2)*\big(a:(a*a^2)\big) \quad (\star\star) \\
 & & \leq & a:(a*a^2) \\
\Longrightarrow & a & \overset{(\star)}{=} & (a*a^2)\big((a*a^2)*a\big)\,\big(a:(a*a^2)\big) \\
 & & \overset{(\star\star)}{=} & (a*a^2)\big((a*a^2)*a\big)\big((a*a^2)*a\big) \\
\Longrightarrow & \big((a*a^2)*a\big)^2 & = & (a*a^2)*a\,,
\end{array}
$$

also die Idempotenz von $(a * a^2) * a$.
Ist umgekehrt jedes a in der gewünschten Weise *zerlegbar*, so erhalten wir $uv * (uv)^2 = uv * uv^2 = v * (u * uv^2) \leq v^2$ und damit die Behauptung. □

Da die *paarweise Orthogonalität* von kürzbaren und idempotenten Elementen gesichert ist, wenn jedes idempotente Element nur 1 als kürzbaren Teiler besitzt, und da diese Eigenschaft den direkten Produkten von booleschen Ringen mit Verbandsgruppenkegeln *a fortiori* zukommt, bieten sich nach 3.6.8 die beiden Korollare an:

3. 6. 9 Korollar. *Eine komplementäre Halbgruppe* $\mathfrak{S}$ *ist genau dann das direkte Produkt einer idempotenten und einer kürzbaren komplementären Halbgruppe, wenn sie neben* (IR) *das nachfolgende Axiom* (IV) *erfüllt:*

(IV) $$\big((a * a(ba : a)) * b\big)^2 \;=\; \big(a * a(ba : a)\big) * b\,.$$

DENN: Die Bedingung (IV) ist offenbar notwendig, und sie ist hinreichend wegen:

$$x \leq a = a^2 \Longrightarrow x = \big(a * a(a : a)\big) * x = \big(a * a(xa : a)\big) * x = x^2\,.$$ □

3. 6. 10 Korollar. *Eine komplementäre Halbgruppe* $\mathfrak{S}$ *ist genau dann das direkte Produkt eines booleschen Ringes und einer kürzbaren komplementären Halbgruppe, wenn sie neben* (IR) *das Axiom erfüllt:*

(BV) $$a : (b * a) \;=\; (b : a) * b\,.$$

BEWEIS. Die Bedingung (BV) ist notwendig, da in booleschen Ringen die Gleichung $(a * b) * b = \big((a \wedge b) * b\big) * b = a \wedge b$ erfüllt ist und Kürzbarkeit die Gleichung impliziert: $a = (a \wedge b)(b * a) = (a : b)(a \wedge b)$.
Umgekehrt folgt aus (BV) für kürzbare x die Implikation

$$x \leq a = a^2 \Longrightarrow x = a : (x * a) = a : (x * xa) = a : a = 1\,,$$

und weiter gilt:

$$a = a^2 \Longrightarrow a \wedge (a * c) = (a * c) : \big(a * (a * c)\big) = (a * c) : (a * c) = 1\,,$$

was zusammen mit 3.6.10 die Behauptung impliziert. □

Dass das um Axiom (IV) erweiterte Axiomensystem der komplementären Halbgruppe unabhängig ist, beweisen die Beispiele (B1), (B2), (B3), (B10), (B11), (B23).

Schließlich zeigen wir noch:

3. 6. 11 Proposition. *Eine komplementäre Halbgruppe ist genau dann das direkte Produkt eines booleschen Ringes mit einer kürzbaren komplementären Halbgruppe, wenn sie die Axiome* (IV) *und* (BV) *erfüllt.*

BEWEIS. Offenbar sind die beiden Bedingungen notwendig. Daher bleibt lediglich zu zeigen, dass sie die Bedingung (IR) implizieren.
Wie wir schon unter 3.6.10 sahen, gilt wegen (BV) auch $x \leq a = a^2 \Longrightarrow x = x^2$. Weiter ist das Element a – wie wir nun zeigen werden – genau dann kürzbar, wenn es lediglich 1 als idempotenten Teiler besitzt.
Denn ist a kürzbar, so muss jeder idempotente Teiler gleich 1 sein. Ist a hingegen nicht kürzbar, so gibt es ein Paar x, y mit (etwa) $xa = ya$ und $x * y \neq 1$. Dann gilt $x(x * y)a = (x \vee y)a = xa$, so dass entweder $(x \vee y) * (x \vee y)a < a$ gilt oder aber

$$x * xa = x * (x \vee a) = (x * (x \vee y)((x \vee y) * (x \vee y)a) = (x * y)a$$

und damit $a \geq x * xa \geq (x * y)a \geq a$, also $(x * y)a = a$ erfüllt ist.
Hieraus resultiert weiter $(x * y) * a < a$, wegen $a : \big((x * y) * a\big) = x * y \neq 1$ – man beachte die Voraussetzung.
Damit erhalten wir insgesamt ein z mit $z * za < a$, also nach Bedingung (IV) auch mit $1 \neq \big(z * z(az : z)\big) * a = u = u^2 \leq a$. Hieraus folgt dann Axiom (IR), da aus $x = x^2 \leq a * a^2$ die Implikation resultiert

$$\begin{aligned} x \leq a, a * a^2 \Longrightarrow x &= (a * a^2) : \big(x * (a * a^2)\big) \\ &= (a * a^2) : (ax * a^2) \\ &= (a * a^2) : (a * a^2) = 1\,. \end{aligned}$$

Dies liefert aus Gründen der Dualität den Beweis nach 3.6.10. □

Im Hinblick auf Koppelungsmöglichkeiten der Struktur der komplementären Halbgruppe mit der klassischen Struktur des Ringes sei noch erwähnt:

3. 6. 12 Zusatz. *Ist $\mathfrak{R}$ ein Ring mit $aR = Ra$ für alle $a \in R$ und $\mathfrak{S}$ die Halbgruppe der Hauptideale aus $\mathfrak{R}$, die wir bezeichnen wollen mit* $\mathrm{a}, \mathrm{b}\ldots$ *und betrachten wollen bezüglich* $\mathrm{ab} := \mathrm{a} \cdot \mathrm{b} = (a) \cdot (b) = (ab)$ *und bezüglich* $\mathrm{a} \vee \mathrm{b} := (a) \cap (b)$*, so gilt:*
Ist $\mathfrak{S}$ komplementär, so ist $\mathfrak{S}$ auch normal, und es ist unter dieser Voraussetzung Axiom (IR) *genau dann erfüllt, wenn $\mathfrak{R}$ semiprim ist, d.h. kein*

eigentliches nilpotentes Element, also kein $a \neq 0$ mit $a^n = 0$ $(\exists n \in \mathbf{N})$ besitzt.

BEWEIS. Zunächst besitzt $\mathfrak{S}$ eine *1* und damit auch $\mathfrak{R}$ eine 1. Denn ist u ein *Allteiler* aus $\mathfrak{R}$, so ist auch u^2 ein Allteiler, also mit geeignetem x dann $u(ux) = u$ und damit $(ux)(ux) = ux$ ein idempotenter Allteiler aus $\mathfrak{R}$. Unter dieser Bedingung können wir weiter schließen

$$\begin{aligned} \langle b\rangle : \langle a\rangle = \langle c\rangle \quad \& \quad & aef = a \;\&\; cef = c \\ \Longrightarrow\;\; & b \,|\, a(ef - 1 + c) \\ \Longrightarrow\;\; & e \,|\, c \,\Big|\, t(ef - 1 + c) \Longrightarrow e \,|\, 1\,. \end{aligned}$$

Damit folgt dann zum einen, dass $a * a^2$ keinen idempotenten Teiler enthalten kann und zum anderen, dass $\mathfrak{S}$ normal ist, wenn $\mathfrak{S}$ komplementär ist.
Gelte hiernach zusätzlich (IR) und sei $a = uv$ mit idempotentem u und kürzbarem v. Dann folgt die Implikation:

$$a^n = 0 \Longrightarrow (uv)^n = 0 \Longrightarrow uv^n = 0 \Longrightarrow u = 0 \Longrightarrow a = 0\,,$$

d. h., so ist $\mathfrak{R}$ frei von echten nilpotenten Elementen.
Sei nun umgekehrt $\mathfrak{R}$ frei von echten nilpotenten Elementen. Wir werden zeigen, dass dann jedes $a * a^2$ kürzbar ist, womit Axiom (IR) nachgewiesen wäre. Zunächst erhalten wir $b * 0 = 0 : b$ aus Gründen der Dualität wegen:

$$bc = 0 \Longrightarrow (bc)^2 = 0 = (c \vee b)^2 \Longrightarrow b \vee c = 0 = cb\,.$$

Sei hiernach $b \neq 0$. Dann folgt mit $c * 0 =: v \neq 0$ und $1 \neq v * 0 =: u \leq c$ also mit $u * 0 = ((u * 0) * 0) * 0 = (v * 0) * 0 = v$ die Implikation

$$\begin{gathered} u \wedge v = v * 0 \wedge u * 0 = (u \vee v) * 0 = 1 \\ \Longrightarrow \\ u \perp v \;\&\; u^2 \,\big|\, uv = 0 \Longrightarrow u = u^2 \leq c\,. \end{gathered}$$

Damit hätte im Falle $b \neq 0$ das Element c einen von *1* verschiedenen idempotenten Teiler.
Wäre nun $a * a^2$ ein Nullteiler, etwa $x \cdot (a * a)^2 = 0$, so müsste $a * a^2$ einen eigentlichen idempotenten Teiler besitzen, was, wie oben gezeigt, nicht möglich ist. Folglich ist $a * a^2$ kürzbar, d.h. Axiom (IR) erfüllt. □

Ist $\mathfrak{R}$ im vorauf gegangenen Beweis kommutativ, so ergibt sich die Idempotenz von $(a * a^2) * a$ natürlich fast unmittelbar.

Der soeben geführte Beweis ist im ersten Teil ringtheoretischer Natur, deshalb sei als rein idealtheoretische Variante mit $a, b, c, ... := \langle \mathrm{a} \rangle, \langle \mathrm{b} \rangle, \langle \mathrm{c} \rangle$ und $\langle u - 1 \rangle := u^*$ und $+$ als Addition i.S. der Idealtheorie noch nachgeliefert:

$$\begin{aligned} b : a = c \quad & \& \quad au = a \;\&\; cu = c \\ & \Longrightarrow \; b \,\big|\, a(u^* + c) \Longrightarrow u \,\big|\, c \,\Big|\, (u^* + c) \Longrightarrow u \,\big|\, u^* \Longrightarrow u = 1\,. \end{aligned}$$

3.7 Rechts-Kongruenzen

Wir stellen zunächst einige Sätze über Rechtskongruenzen rechtskomplementärer Halbgruppen vor, unter denen sich als wesentlichstes Resultat der Satz erweisen wird, dass in endlichen rechtskomplementären Halbgruppen jede Rechts-Kongruenz auch eine Links-Kongruenz ist.

3. 7. 1 Definition. Sei $\mathfrak{S}$ eine rechtskomplementäre Halbgruppe. Dann nennen wir eine Teilmenge H aus S ein *Rechtsideal* von $\mathfrak{S}$, wenn H den Bedingungen genügt:

$$(i) \qquad a \in S \;\&\; b \in H \Longrightarrow a * b \in H\,,$$

$$(ii) \qquad a \in H \;\&\; b \in H \Longrightarrow ab \in H\,,$$

$$(iii) \qquad ab \in H \Longrightarrow a \in H\,.$$

ähnlich wie in anderen Strukturen lassen sich auch in rechtskomplementären Halbgruppen die Kongruenzen durch spezielle Untermengen erfassen.

3. 7. 2 Proposition. *Sei $\mathfrak{S}$ eine rechtskomplementäre Halbgruppe. Dann entsprechen die Rechtskongruenzen von $\mathfrak{S}$ umkehrbar eindeutig den Rechtsidealen von $\mathfrak{S}$ via*

$$\theta \longrightarrow H \iff (a \equiv b \;\; (\theta) \Leftrightarrow a * b, b * a \in H)\,.$$

BEWEIS. Sei zunächst θ eine Rechtskongruenz und 1 das Einselement aus $\mathfrak{S}$. Dann erfüllt die Klasse $1\,\theta =: \overline{1}$ die Implikationen

$$(i) \qquad a \in S \;\&\; b \in \overline{1} \Longrightarrow a * b \equiv a * 1 \equiv 1 \in \overline{1}$$

$$(ii) \qquad a \in \overline{1} \;\&\; b \in \overline{1} \Longrightarrow ab \equiv a1 \equiv a \in \overline{1}$$

$$(iii) \qquad ab \in \overline{1} \Longrightarrow a \equiv a1 \equiv a(a * ab) \equiv ab \in \overline{1}$$

$$\begin{aligned}(iv) \qquad a \equiv b \;\; (\theta) &\Longrightarrow a * b \in \overline{1} \ni b * a \\ &\Longrightarrow a \equiv a(a * b) \equiv b(b * a) \equiv b \;\; (\theta)\end{aligned}$$

Sei hiernach H ein Rechtsideal. Dann erzeugt die Festsetzung

$$a \equiv b \;\; (H) \iff a * b, b * a \in H$$

eine Rechtskongruenz, denn die Bedingungen

$$R: \;\; a \equiv a \;\; (H) \;\; \text{und} \;\; S: \;\; a \equiv b \Longleftrightarrow b \equiv a \;\; (H)$$

sind evident,

$$T: \;\; a \equiv b \;\; (H) \quad \& \quad b \equiv c \;\; (H) \Longrightarrow a \equiv c \;\; (H)$$

folgt aus

$$\begin{aligned} a * c &\leq (a * b)((a * b) * (a * c)) \\ &= (a * b)(a(a * b) * c) \\ &= (a * b)(b(b * a) * c) \\ &= (a * b)((b * a) * (b * c)) \in H\,, \end{aligned}$$

und es gilt

$$\begin{array}{rcl} b & \equiv & b' \\ & \Longrightarrow & \\ ab * ab' & = & b * (a * ab') \\ & \leq & b * b' \in H \\ & \& & \\ (a * b) * (a * b') & = & a(a * b) * b' \\ & = & b(b * a) * b' \\ & = & (b * a) * (b * b') \in H\,. \end{array}$$

Damit ist wegen $a \in H \Longleftrightarrow 1 * a, a * 1 \in H$ alles bewiesen. □

3. 7. 3 Proposition. *Sei $\mathfrak{S}$ eine endliche rechtskomplementäre Halbgruppe. Dann entsprechen die Rechtskongruenzen umkehrbar eindeutig den Idempotenten u mit der Eigenschaft $au * u = 1 \;\; (a \in S)$ vermöge der Abbildung*

$$\theta \longrightarrow u \iff (a \equiv b \;\; (\theta) \Leftrightarrow au = bu).$$

BEWEIS. Ist u idempotent, so ist jeder Linksteiler von u auch ein Rechtsteiler von u wegen

$$\begin{array}{rcl} xy = u & \Longrightarrow & u \leq ux \leq uxy = u \\ & \Longrightarrow & ux = u\,. \end{array}$$

Für das weitere nehmen wir an, dass u zusätzlich $au * u = 1$ $(\forall a \in S)$ erfüllt. Dann erhalten wir

$$\begin{array}{rrcl} & a * u & \leq & u\,, \\ \text{wegen} & u * (a * u) & = & au * u = 1 \\ & & \& & \\ & au & = & au(au * u) \\ & & = & u(u * au)\,. \end{array}$$

Hieraus folgt, dass jeder Rechtsteiler y von u nicht nur auch ein Linksteiler von u ist, sondern zudem $yu = u$ erfüllt. Denn nach dem Gezeigten gilt:

$$\begin{array}{rcl} xy & = & u \\ & \Longrightarrow & \\ yu = uy' & = & xuy' \quad (\exists y' \in S) \\ & = & xyu = uu = u\,. \end{array}$$

Weiter erhalten wir unter der obigen Prämisse, dass die Menge H_u aller $h \leq u$ ein Rechtsideal bildet. Denn es gelten

$$a \in S \;\&\; b \leq u \;\Longrightarrow\; a * b \leq a * u \leq u \tag{3.159}$$

$$a \leq u \;\&\; b \leq u \;\Longrightarrow\; abu = au = u \Longrightarrow ab \leq u \tag{3.160}$$

$$ab \leq u \;\Longrightarrow\; a \leq u \tag{3.161}$$

Wir sind also am Hauptziel, wenn wir zeigen, dass jedes Rechtsideal vom Typ H_u ist. Sei hierzu H ein beliebiges Rechtsideal. Dann gilt $a, b \in H \Longrightarrow a * b \in H$, weshalb mit a und b auch $a \vee b$ zu H gehört. Somit existiert in H ein Maximum, nämlich $u = \bigvee h \ (h \in H)$, das seinerseits $uu = u$ und $a * u \in H \leadsto a * u \leq u \leadsto au * u = 1$ und daher $H = H_u$ erfüllt.
Bleibt zu zeigen, dass die den H_u entsprechenden Rechtskongruenzen vom Typ des Satzes sind. Dies folgt aber vermöge:

$$\begin{array}{rrcl} & au = bu & \Longrightarrow & a * b \leq a * bu = a * au \leq u \\ \& & a * b, b * a \leq u & \Longrightarrow & au = a(a * b)u = b(b * a)u = bu \end{array}$$

Fertig. $\square$

Als eine überraschende Folgerung des letzten Satzes erhalten wir:

3. 7. 4 Proposition. *Ist $\mathfrak{S}$ eine endliche rechtskomplementäre Halbgruppe, so ist jede Rechtskongruenz von $\mathfrak{S}$ sogar eine Kongruenz.*

BEWEIS. Es bleibt nach dem Bisherigen zu zeigen, dass für jedes idempotente u mit $xu * u = 1$ aus $a \equiv a'$ sowohl $ab \equiv a'b$ als auch $a * b \equiv a' * b$ folgt. Dies ergibt sich aber unter Annahme von $bu = uc$ aufgrund von

$$\begin{array}{rlrcl}
a \equiv a' & \Longrightarrow & au & = & a'u \\
 & \Longrightarrow & auc & = & a'uc \\
 & \Longrightarrow & abu & = & a'bu \\
 & \textbf{und} & & & \\
a \equiv a' & \Longrightarrow & au & = & a'u \\
 & \Longrightarrow & au * b & = & a'u * b \\
 & \Longrightarrow & u * (a * b) & = & u * (a' * b) \\
 & \Longrightarrow & u(u * (a * b)) & = & u(u * (a' * b)) \\
 & \Longrightarrow & (a * b)((a * b) * u) & = & (a' * b)((a' * b) * u) \\
 & \Longrightarrow & (a * b)((a * b) * u)u & = & (a' * b)((a' * b) * u)u \\
 & \Longrightarrow & (a * b)u & = & (a' * b)u\,.
\end{array}$$ $\square$

Mit dem soeben bewiesenen Sachverhalt gelingt es, ein Beispiel für eine rechtskomplementäre Halbgruppe zu konstruieren, deren Kongruenzklassen dem Chinesischen Restsatz – (vgl. [160]) –

$$\text{(CH)} \qquad \begin{array}{c} a\,\theta_1 \cap b\,\theta_2 \neq \emptyset \neq b\theta_2 \cap c\,\theta_3 \neq \emptyset \neq c\,\theta_3 \cap a\,\theta_1 \\ \Longrightarrow \qquad a\,\theta_1 \cap b\,\theta_2 \cap c\,\theta_3 \neq \emptyset \end{array}$$

nicht genügen und deren Kongruenzen nicht vertauschbar sind. Denn man unterwerfe die freie Halbgruppe $F(1, u, v, w, x, y, z)$ den definierenden Relationen:

$$\begin{array}{l}
1a = a = a1\ ; \quad \text{für alle erzeugenden Elemente.} \\
uu = u\ ; \qquad uv = vu\ ; \qquad ux = vx = wx = x\ ; \\
vv = v\ ; \qquad vw = wv\ ; \qquad uy = vy = wy = y\ ; \\
ww = w\ ; \qquad wu = uw\ ; \qquad uz = vz = wz = z\ ; \\
xx = yy = zz = xy = yx = yz = zy = zx = xz = \\
xxx = yyy = zzz = xuvw = yuvw = zuvw := 0
\end{array}$$

$$\text{und:} \qquad xvw = yvw\ ; \qquad yuv = zuv\ ; \qquad zwu = xwu\ .$$

Dann gilt für die Klassen X von x modulo vw, Y von y modulo uv und Z von z modulo wu : $X \cap Y = \{y, yv\}$, $Y \cap Z = \{z, zu\}$, $Z \cap X = \{x, xw\}$, aber $X \cap Y \cap Z = \emptyset$.
Und setzen wir $vw = a$ und $uv = b$, so folgt $xa = ya$ & $yb = zb$, doch lässt sich kein Element s finden mit der Eigenschaft $xb = sb$ & $sa = za$, da aus $xb = sb$ resultieren würde, dass s gleich x, xu, xv oder xuv wäre, obwohl $zvw \neq xvw$ und $zvw \neq xuvw$, in jedem Falle also $xb = sb \Longrightarrow sa \neq za$ erfüllt ist.

3.8 Kongruenzen

3. 8. 1 Definition. Sei $\mathfrak{S}$ eine komplementäre Halbgruppe. Dann nennen wir eine nicht leere Teilmenge I aus S ein *Halbideal*, wenn sie der Bedingung genügt:

(i) $\qquad ab \in I \Longleftrightarrow a, b \in I$

Erfüllt $I \subseteq S$ zudem die Bedingung

(ii) $\qquad (a * a')(a' * a)(b * b')(b' * b) \in I \Longrightarrow (a * b) * (a' * b') \in I$,

so nennen wir I ein $*$-*Ideal*. Gilt über (i) hinaus die Bedingung

(iii) $\qquad a * b \in I \Longleftrightarrow b : a \in I$

so nennen wir I ein *Vollideal*.

3. 8. 2 Lemma. *Jedes $*$-Ideal ist ein Rechtsideal in Bezug auf $(S, *)$.*

DENN:
$$\begin{aligned} b \in I &\Longrightarrow (a * a)(a * a)(1 * b)(b * 1) \in I \\ &\Longrightarrow (a * 1) * (a * b) \in I \\ &\Longrightarrow 1 * (a * b) \in I \\ &\Longrightarrow a * b \in I \end{aligned}$$
$$\begin{aligned} \text{und} \quad ab \in I &\Longrightarrow (ab * 1)(1 * ab)(ab * a)(a * ab) \in I \\ &\Longrightarrow (ab * ab) * (1 * a) \in I \\ &\Longrightarrow 1 * (1 * a) \in I \\ &\Longrightarrow 1 * a = a \in I\,. \end{aligned}$$
□

3. 8. 3 Lemma. *Eine Teilmenge A aus S ist schon dann ein $*$-Ideal, wenn sie neben (ii) die Implikation erfüllt:*

(3.163) $$a, b \in I \Longrightarrow ab \in I$$

DENN:
$$\begin{aligned} ab \in I &\Longrightarrow (a*1)(1*a)(1*b)(b*1) \in I \\ &\Longrightarrow (a*1)*(1*b) \in I \\ &\Longrightarrow 1*(1*b) \in I \\ &\Longrightarrow 1*b = b \in I \ , \end{aligned}$$

fertig. □

3. 8. 4 Lemma. *Ist $\equiv$ eine Kongruenzrelation in $\mathfrak{S}$ bezüglich $\cdot$ und $*$, so bildet die Klasse $[1]$ ein $*$-Ideal, und es gilt $a \equiv b \Longleftrightarrow (a*b)(b*a) \in \big(1\big)$.*

BEWEIS. Zunächst haben wir die Implikationen

$$a \equiv 1 \equiv b \ \Longrightarrow \ ab \equiv 1 \cdot 1 \equiv 1$$

und

$$\begin{array}{rcl} ab & \equiv & 1 \\ & \Longrightarrow & \\ a \equiv 1*a \equiv ab*a & \equiv & b*(a*a) \equiv b*1 \equiv 1 \\ & \Longrightarrow & \\ b \equiv 1b & \equiv & ab \equiv 1 \, . \end{array}$$

Hieraus folgt dann weiter:

$$\begin{array}{rcl} (a*a')(a'*a)(b*b')(b'*b) \equiv 1 & \Longrightarrow & a*a' \equiv a'*a \equiv b*b' \equiv b'*b \equiv 1 \\ & \Longrightarrow & \\ a \equiv a(a*a') \equiv a'(a'*a) \equiv a' & \& & b \equiv b(b*b') \equiv b'(b'*b) \equiv b' \\ & \Longrightarrow & \\ (a*b)*(a'*b') & \equiv & (a*b)*(a*b) \equiv 1*1 \equiv 1 \ . \end{array}$$

Schließlich haben wir
$$\begin{aligned} a \equiv b &\Longrightarrow (a*b)(b*a) \equiv 1 \\ &\Longrightarrow a*b \equiv 1 \equiv b*a \\ &\Longrightarrow a \equiv a(a*b) \equiv b(b*a) \equiv b \ . \end{aligned}$$
□

3. 8. 5 Lemma. *Ist I ein $*$-Ideal aus $\mathfrak{S}$, so ist I auch ein Rechtsideal.*
DENN: Man beachte die Definition. □

3. 8. 6 Proposition. *Ist I ein $*$-Ideal, so liefert die Festsetzung*

$$a \equiv b \ :\Longleftrightarrow \ (a*b)(b*a) \in I$$

eine Kongruenzrelation in $\mathfrak{S}$ bezüglich $\cdot$ und $*$ mit $\big(1\big) = I$.

BEWEIS. Nach 3.8.5 ist I ein Rechtsideal. Folglich ist die oben definierte Relation eine Rechtskongruenz.
Zu zeigen bleibt, dass sie sogar eine Kongruenz ist. Dies folgt aber aus:

$$\begin{aligned} a \equiv a' \ \&\ b \equiv b' &\Longrightarrow (a * a')(a' * a)(b * b')(b' * b) \in I \\ &\Longrightarrow (a * b) * (a' * b') \in I \end{aligned}$$

und

$$\begin{array}{rcl} a & \equiv & a' \\ & \Longrightarrow & \\ ab * a'b \equiv b * (a * a'b) & \equiv & b * (a' * a'b) \equiv a'b * a'b \equiv 1 \in I\,. \end{array}$$

Der Rest resultiert aus 3.7.1 mittels

$$\begin{aligned} a \in I &\Longleftrightarrow (1 * a)(a * 1) \in I \\ &\Longleftrightarrow a \equiv 1\,. \end{aligned} \qquad \square$$

Zusätzlich erhalten wir:

3. 8. 7 Lemma. *Sei $\mathfrak{S}$ komplementär. Ist dann $\equiv$ eine Kongruenzrelation bezüglich der Operationen $\cdot$, $*$ und $:$, so ist die Klasse $[1]$ sowohl ein $*-$ als auch ein $:-$Ideal. Darüber hinaus gilt $a * b \in [1] \Longleftrightarrow b : a \in [1]$.*

DENN: Der erste Teil ist klar, der zweite folgt vermöge:

$$\begin{aligned} a * b \equiv 1 &\Longrightarrow a(a * b) \equiv a \\ &\Longrightarrow (b : a)a \equiv a \\ &\Longrightarrow b : a \equiv 1\,. \end{aligned} \qquad \square$$

Unmittelbar klar ist nach dem bisherigen auch

3. 8. 8 Proposition. *In einer komplementären Halbgruppe entsprechen die Kongruenzen umkehrbar eindeutig den Vollidealen vermöge:*

$$\theta \longrightarrow H \iff a \equiv b\ (\theta) \Leftrightarrow (a * b)(b * a) \in H\,.$$

Weiter haben wir

3. 8. 9 Proposition. *Eine Teilmenge I aus S ist genau dann ein Vollideal, wenn sie den beiden Bedingungen genügt:*

(i) $ab \in I \Longleftrightarrow a, b \in I$

(iii) $a \cdot I = I \cdot a$.

BEWEIS. Gelten (i) und (iii), so folgt für $x \in I$

$$ax = a(a * ax) = (ax : a)a \text{ mit } ax : a \in I\,,$$

also $aI \subseteq Ia$ und es ergibt sich dual $aI \supseteq Ia$.
Sind umgekehrt (i) und (iv) erfüllt, so gilt

$$a * b \in I \Longrightarrow a(a * b) = xa = (b : a)a \text{ mit } x \in I \Longrightarrow b : a \in I\,,$$

und wir erhalten dual $b : a \in I \Longrightarrow a * b \in I$. □

Neben den Kongruenzen werden im weiteren *Rechtskongruenzen* eine große Rolle spielen.

3. 8. 10 Lemma. *In einer rechtskomplementären Halbgruppe, die der Bedingung* $a*(b*a) = 1$ *genügt, entsprechen die Rechtskongruenzen umkehrbar eindeutig den Halbidealen vermöge*

$$a \equiv b \quad (I) \iff (a * b)(b * a) \in I\,,$$

und es gilt auch hierbei $I = [1]$.

BEWEIS. Man beachte 3.7.2 und

$$\begin{aligned}(a * b) * (a * b') &= (a(a * b) * b' \\ &= b(b * a) * b' \\ &= (b * a) * (b * b') \\ &\leq b * b' \in I\,.\end{aligned}$$

□

Vor dem Hauptsatz dieses Paragraphen erwähnen wir noch eine Charakterisierung der Kongruenzen und Rechtskongruenzen, die später von Bedeutung sein wird.

3. 8. 11 Lemma. *Ist* $\mathfrak{S}$ *eine komplementäre Halbgruppe und* $\equiv$ *von* I erzeugt,*so ist* $a \equiv b$ *gleichbedeutend mit* $a \,\big|\, be_1$ & $b \,\big|\, ae_2$ *für mindestens ein* e_1, e_2 *aus* I.

DENN: Wir haben $a \equiv b \Longrightarrow a \,\big|\, b(b * a)$ & $b \,\big|\, a(a * b)$ mit $a * b, b * a \in I$ und $a \,\big|\, be \Longrightarrow be * a = e * (b * a) = 1 \Longrightarrow b * a \leq e$. □

Ferner sei noch darauf hingewiesen, dass jede von einem Halbideal erzeugte Rechtskongruenz auch treu ist bezüglich $\vee$, was *a fortiori* gilt, und gegebenenfalls bezüglich $\wedge$, was aus

$$(a \wedge b) * (a \wedge b') = a * (a \wedge b') \vee b * (a \wedge b')$$

resultiert. Zusammenfassend formulieren wir

3. 8. 12 Proposition. *Ist $\mathfrak{S}$ eine rechtskomplementäre Halbgruppe, so lassen sich die Rechts-Kongruenzen bezüglich $\cdot$ und $*$ umkehrbar eindeutig den Halb-Idealen zuordnen, die jeweils der Klasse* [1] *entsprechen.*
Analog lassen sich in komplementären Halbgruppen die Kongruenzen bezüglich $\cdot, *$ und $:$ umkehrbar eindeutig den Vollidealen zuordnen.
Dabei ist das erzeugende Prinzip stets $a \equiv b \quad (I) \Longleftrightarrow (a * b)(b * a) \in I$.

Für das folgende ist noch ein Ergebnis wichtig, das wir mit Hilfe der *Rees-Ideale*, kurz *r-Ideale,* erzielen. Diese sind definiert *via* $SRS \subseteq R$. Sie bilden in komplementären Halbgruppen ihrerseits eine Halbgruppe bezüglich der Komplexmultiplikation und erfüllen auch die übrigen Idealeigenschaften, doch ist das hier nicht wesentlich. Von Bedeutung ist hingegen die so genannte *Rees-Kongruenz.* Ist R ein r-Ideal, so wird sie geliefert durch

$$a \equiv b \ \ (R) \iff a = b \vee a, b \in R\,.$$

Das homomorphe Bild ist dabei nicht notwendig komplementär, doch gilt

3. 8. 13 Proposition. *Ist $\mathfrak{S}$ eine komplementäre Halbgruppe, I ein Halbideal und $R = S - I$, so liefert die Rees-Kongruenz nach R einen Homomorphismus bezüglich der Multiplikation auf eine komplementäre Halbgruppe $\overline{S}$, und es gilt für die a und b außerhalb von R die Gleichung $\overline{a} \,\overline{*}\, \overline{b} = \overline{a * b}$ und ganz entsprechend $\overline{a} \,\overline{:}\, \overline{b} = \overline{a : b}$.*

BEWEIS. Der erste Teil ist fast evident. Dass $\overline{\mathfrak{S}}$ komplementär ist, folgt für die Restmengen von Halbidealen daraus, dass Halbideale operativ abgeschlossen sind, so dass mit $\overline{0} := R$ in $\overline{\mathfrak{S}}$ die Gleichung $\overline{0} = \overline{a} \,\overline{*}\, \overline{0} = \overline{0} \,\overline{:}\, \overline{a} = \overline{0}$ erfüllt ist. □

Ferner können wir zeigen

3. 8. 14 Proposition. *Ist $\mathfrak{S}$ eine $\wedge$-abgeschlossene komplementäre Halbgruppe und u ein idempotentes Element aus $\mathfrak{S}$, so liefert die Äquivalenz $a \equiv b :\Longleftrightarrow u \wedge a = u \wedge b$ eine $\vee$- und $\wedge$-treue Kongruenzrelation bezüglich der Multiplikation auf die komplementäre Halbgruppe der Teiler von u.*

DENN: Offenbar ist $\equiv$ eine Äquivalenzrelation. Ferner gilt nach 3.3.3

$$\begin{aligned}(u \wedge a)(u \wedge b) &= u \wedge ub \wedge au \wedge ab \\ &= u(1 \wedge a \wedge b) \wedge ab = u \wedge ab\end{aligned}$$

und

$$(u \wedge a) \vee (u \wedge b) = u \wedge (a \vee b)$$

sowie *a fortiori*

$$(u \wedge a) \wedge (u \wedge b) \;=\; u \wedge (a \wedge b)\,. \qquad \Box$$

Wir gehen jetzt noch ein auf einige allgemein-algebraische Aspekte.

3. 8. 15 Proposition. *Komplementäre Halbgruppen bilden eine arithmetische Varietät.*

BEWEIS. Zunächst ist der Kongruenzverband einer jeden komplementären Halbgruppe distributiv – wegen $c \le ab \Longrightarrow (c:b)\big((c:b)*c\big)$ mit $c:b \le a$ und $(c:b)*c \le b$, da dies $I_1 \vee I_2 = I_1 \cdot I_2$ bedeutet und die Implikation liefert:

$$\begin{aligned} d \in AB \wedge AC &\Longrightarrow d \le ab, ac \;\; (a \in A,\ b \in B,\ c \in C) \\ &\Longrightarrow d:(a*d) \in A \;\&\; a*d \in B \wedge C\,. \end{aligned}$$

Gilt weiter $\qquad a = x \;\; (I_1) \quad \& \quad x \equiv b \;\; (I_2)\,,$

so existieren wegen $I_1 \cdot I_2 = I_2 \cdot I_1$ Elemente e_1, f_1 in I_1 und e_2, f_2 in I_2 mit

$$ae_1e_2 \ge b \quad \& \quad bf_2f_1 \ge a\,,$$

woraus mit $\qquad y = \big(ae_1(bf_2 * ae_1)\big) \;\vee\; \big(bf_2 : (ae_1 * bf_2)\big)$

die zweite Behauptung aus Dualitätsgründen folgt, wegen

$$y \le ae_1 \;\Longrightarrow\; a * y \le e_1$$

und

$$\begin{aligned} y * a &\le \big(ae_1 : (bf_2 * ae_1)\big) * a \\ &\le bf_2 * ae_1 \le f_2e_1\,. \end{aligned}$$

$\Box$

3.9 Repräsentierbarkeit

Wir gehen kurz auf die Frage ein, unter welchen Bedingungen eine komplementäre Halbgruppe *repräsentierbar* ist, also subdirekt zerfällt in linear geordnete *Komponenten.* Die Antwort ist leicht gegeben. Denn ist $\mathfrak{S}$ subdirekt irreduzibel, so darf es natürlich kein Paar von 1-disjunkten Vollidealen geben. Andererseits bilden in linear geordneten komplementären Halbgruppen die *Polaren* $U^\perp := \{x \,|\, u \perp x \;\; (\forall u \in U)\}$ jeweils ein Vollideal. Daher ist notwendig und hinreichend die in [15] formulierte Forderung

$$(0^c) \qquad (c*(b*a)c \vee c(b*a):c)*x \vee (a*b)*x \;=\; x\,.$$

Denn: Setzt man hier $c = 1$, so erhalten wir nach 3.3.6 die Normalität $a * b \wedge b * a = 1$ und damit die $\wedge$-Abgeschlossenheit, also erneut nach 3.3.6 $a * b \perp c * (b * a)c$ und $a * b \perp c(b * a) : c$ und damit, da $x \perp y$ zu $x = y * x$ und $y = x * y$ führt, die Gleichung $c \cdot a^\perp = a^\perp \cdot c$. Denn, man beachte

$a \perp b \Longrightarrow bc = c(c*bc)\ \ (a \perp c*bc)$ und $a \perp b \Longrightarrow cb = (cb : c)c\ \ (a \perp cb : c)$.

Wir hätten also im Falle der Unvergleichbarkeit zweier Elemente a, b die Vollideale $U := (a * b)^\perp$ und $V := U^\perp$ mit $U \neq \{1\} \neq V$ und $U \cap V = \{1\}$, ein Widerspruch zur subdirekten Irreduzibilität von $\mathfrak{S}$!

3.10 Polynome

Im vorangehenden Abschnitt haben wir gezeigt, dass die Kongruenzen einer jeden komplementären Halbgruppe *vertauschbar* sind, einen *distributiven* Verband bilden und durch ihre 1-*Klassen* charakterisiert werden.
Insbesondere folgt aus den beiden ersten Eigenschaften, dass die Kongruenzen komplementärer Halbgruppen den *Chinesischen Restsatz* erfüllen, der besagt:

> *Der Durchschnitt endlich vieler Kongruenzklassen ist leer gdw. es unter diesen endlich vielen Klassen zwei disjunkte gibt.*

Somit müssen, man konsultiere etwa [47],
ein Malzew-Polynom $p(x, y, z)$ mit

$$p(x, x, z) = \ z\ = p(z, x, x)\,,$$

ein Pixley-Polynom $q(x, y, z)$ mit

$$q(x, x, z) = \ q(x, z, x)\ = q(z, x, x) = x$$

und eine Wille-Kette $p_1(x, y), \ldots, p_n(x, y)$, $r(x, y, x_1, \ldots, x_n)$ mit

$$\begin{aligned} p_v(x,x)1 \ \&\ r(x, y, 1, \ldots, 1) &= x \\ r(x, y, p_1(x, y), \ldots, p_n(x, y)) &= y \end{aligned}$$

existieren. Nichts ist indessen gesagt über die Form solcher Polynome.

3. 10. 1 Proposition. *Sei $\mathfrak{S}$ eine komplementäre Halbgruppe. Definieren wir dann $h(x, y, z) := x : (z * y)$, so liefern uns*

$p(x,y,z) = h(x,y,z) \vee h(z,y,x)$ *ein* MALZEW-*Polynom,*

$q(x,y,z) = h(x,x,y) \vee h(y,y,z) \vee h(z,z,x)$ *ein* PIXLEY-*Polynom,*

und

$p_1(x,y) = y * x, \quad p_2(x,y) = (x : (y * x)) * y, \quad p_3(x,y,w,z) = (x : w)z$
eine WILLE-*Kette.*

Nach dem Beispiel des letzten Paragraphen kann zu beliebigen rechtskomplementären Halbgruppen weder ein MALZEW- noch ein PIXLEY-Polynom existieren, da die Existenz des einen Polynoms äquivalent ist mit der Vertauschbarkeit der Kongruenzrelationen, die Existenz des anderen äquivalent ist mit dem Chinesischen Restsatz.
Es gelten jedoch zwei Abschwächungen von weittragender Konsequenz (vgl. [160] und [108]), nämlich:

3. 10. 2 Proposition. *Ist $\mathfrak{S}$ eine rechtskomplementäre Halbgruppe, so existiert ein Paar von Polynomen*

$$\begin{array}{rcl} p_1(w,x,y,z) & , & p_2(w,x,y,z) \\ & \textit{mit} & \\ p_1(x,y,y,z) = x;\; p_1(x,x,y,y) & = & p_2(x,x,y,y);\; p_2(x,y,y,z) = z \end{array}$$

sowie ein Paar von Polynomen

$$\begin{array}{rcl} q_1(x,y,z) & , & q_2(x,y,z) \\ & \textit{mit} & \\ x = q_1(x,x,z);\; q_1(x,z,z) & = & q_2(x,z,z);\; q_2(x,x,z) = z \\ \textit{und} \qquad q_1(x,y,x) = & x & = q_2(x,y,x)\,. \end{array}$$

DENN: Man betrachte die Paare

$$\begin{array}{rcl} p_1(w,x,y,z) = w(x * y) & , & p_2(w,x,y,z) = z(y * x) \\ & \text{und} & \\ q_1(x,y,z) = x(x(y * z) * z) & , & q_2(x,y,z) = z(z(z * y) * x). \end{array}$$

□

Dass es sich bei den aufgezeigten Gegebenheiten um Abschwächungen der MALZEW - bzw. PIXLEY-Bedingung handelt, folgt daraus, dass bei Existenz eines Malzew-Polynoms $p(x,y,z)$ das Paar $p(w,p(x,y,z),z), z$ den

Forderungen an p_1, p_2 genügt, und bei Existenz eines PIXLEY-Polynoms das Paar $q(x,y,z), z$ den Forderungen an q_1, q_2.
Dass für beliebige rechtskomplementäre Halbgruppen eine WILLE-Kette nicht unbedingt existieren muss, hat natürlich damit zu tun, dass in ihren Existenznachweis die Vertauschbarkeit eingeht.

Insbesondere gewährleistet das Polynompaar q_1 , q_2, siehe etwa [47]

Rechtskomplementäre Halbgruppen sind kongruenzdistributiv!

Folglich greift

Jónsson's celebrated Lemma!

3.11 States

In [133] wird eine Klasse von beschränkten $R\ell$-Monoiden untersucht. Leider übersehen die Autoren dort aber, dass diese Strukturen nichts anderes sind als beschränkte komplementäre Halbgruppen.
Der zentrale Begriff in [133] ist der eines normalen Filters, der zudem – als Filter – maximal ist und folglich ein homomorphes Bild erzeugt, das zu einem State führt, man konsultiere [83], [68] und [133].
In diesem Abschnitt zeigen wir, dass das von einem maximalen Filter, der zudem normal ist, erzeugte homomorphe Bild nicht nur eine linear geordnete MVA-Algebra ist, sondern zudem bezüglich der Operationen max, min, und $\oplus$, definiert mittels $a \oplus b = \min(1, a+b)$ in das reelle Einheitsintervall $[0,1]$ eingebettet werden kann.
Zu diesem Zweck betrachten wir eine beschränkte komplementäre Halbgruppe, also eine solche mit einer 0, die zudem $a^n = 1$ $(\forall a \neq 0\ \exists n \in N)$ erfüllt – in anderen Zusammenhängen auch als stark archimedisch bezeichnet. Hier folgt sofort $au = a \Longrightarrow u = 0$ und folglich $a * b + b * a = 0$, $(a \wedge b)(a * b + b * a) = a \wedge b$. s gilt aber $x \wedge y = 1 \Longrightarrow x = 1 \vee y = 1$, zur Erinnerung

$$a^n = 1 = b^m \Longrightarrow (a \wedge b)^{m+n} = 1\,. \tag{3.165}$$

Folglich ist $\mathfrak{S}$ linear geordnet, erfüllt zudem $a^n = 1$ für alle a bezüglich einem geeigneten (privaten) n und darüber hinaus $au = a \Longrightarrow u = 0$.
Dies bedeutet, dass $\mathfrak{S}$ eine Unterstruktur von $(E, \oplus, \min)$ ist, wie in [54] gezeigt wird. Wir möchten hier aber die Chance nutzen einen alternativen Beweis auf der Grundlage von 6.3.3 zu geben.

Skizze: Wir weisen zunächst auf die herkömmliche Art nach, dass eine stark archimedische komplementäre Halbgruppe kommutativ ist, und betten sie hiernach ein in ihren v-Idealbereich – für *outsider* in die Habgruppe ihrer Dedekindschnitte ein.

Auf diese Weise erhalten wir ein vollständiges total geordnetes d-Monoid, in dem folglich jedes $a > 0$ eine eindeutige *Quadratwurzel* und demzufolge eine *Bisektion* erzeugt, also jedes a eine eindeutige *Binärdarstellung* besitzt.

3.12 Quotienten

Die komplementäre Halbgruppe erweckt den Eindruck einer gewissen Enge, insofern sie *a fortiori* eine *positive* Halbverbandshalbgruppe darstellt. Tatsächlich lässt sich aber zu jeder komplementären Halbgruppe mit nichttrivialem kürzbaren Anteil C eine echte *partial geordnete Quotientenerweiterung* $\mathfrak{Q}$ konstruieren, in der jedes $b \in C$ und darüber hinaus jedes kürzbare Element *invertierbar* ist. Genauer:

3. 12. 1 Proposition. *Zu jeder komplementären Halbgruppe $\mathfrak{S}$ existiert eine Quotientenhülle, d.h. eine eindeutig bestimmte Oberhalbgruppe $\mathfrak{Q}$, in der sich jedes α darstellen lässt als Produkt ab^{-1} mit $a, b \in S$ und in der jedes kürzbare Element aus $\mathfrak{S}$ und darüber hinaus auch alle übrigen kürzbaren Elemente aus $\mathfrak{Q}$ invertierbar sind.*

3. 12. 2 Lemma. *Ist $\mathfrak{S}$ eine komplementäre Halbgruppe, so bildet die Menge R aller Paare mit positivem a und* linkskürzbarem *b bezüglich der Operation $a.b \circ c.d := a(b * c).d(c * b)$ ein Monoid.*

BEWEIS. Es ist $a.b = a.1 \circ 1.b$. Hieraus folgen zunächst die beiden Gleichungen:

$$\begin{aligned}(a.b \circ x.1) \circ c.d &= a(b * x).(x * b) \circ c.d \\ &= a(b * x)((x * b) * c).d(c * (x * b)) \\ &= a(b * xc).d(xc * b) \\ &= a.b \circ xc.d \\ &= a.b \circ (x.1 \circ c.d)\end{aligned}$$

$$
\begin{aligned}
\text{und} \qquad (a.b \circ 1.y) \circ c.d &= a.yb \circ c.d \\
&= a(yb * c).d(c * yb) \\
&= a(b * (y * c)).d(c * y)((y * c) * b) \\
&= a.b \circ (y * c).d(c * y) \\
&= a.b \circ (1.y \circ c.d)\ ,
\end{aligned}
$$

woraus die allgemeine Assoziativität resultiert vermöge der Herleitung

$$
\begin{aligned}
(a.b \circ x.y) \circ c.d &= (a.b \circ (x.1 \circ 1.y)) \circ c.d \\
&= ((a.b \circ x.1) \circ 1.y) \circ c.d \\
&= (a.b \circ x.1) \circ (1.y \circ c.d) \\
&= \ \dots \\
&= a.b \circ (x.y \circ c.d)\ .
\end{aligned}
$$

Da,it sind wir am Ziel. □

Man beachte an dieser Stelle, dass der voraufgegangene Beweis schon gültig ist für rechtskomplementäre Halbgruppen. Hierauf werden wir später zurückkommen.

3. 12. 3 Lemma. *In R liefert die Festsetzung*

$$a.b \equiv c.d :\Longleftrightarrow \exists\, x, y\ : ax = cy\ \&\ bx = dy$$

eine Kongruenzrelation (bezüglich $\circ$*).*

BEWEIS. Seien x, y kürzbar. Dann liefert die Gleichungskette:

$$
\begin{aligned}
ax.bx \circ c.d &\equiv ax(bx * c).d(c * bx) \\
&\equiv ax(x * (b * c)).d(c * b)((b * c) * x) \\
&\equiv a(b * c)((b * c) * x).d(c * b)((b * c) * x) \\
&\equiv a(b * c).d(c * b) \\
&\equiv a.b \circ c.d \\
&\equiv a.b \circ c.d \\
&\equiv a(b * c).d(c * b) \\
&\equiv a(b * c)((c * b) * x).d(c * b)((c * b) * x) \\
&\equiv a(b * c)((c * b) * x).dy(x * (c * b)) \\
&\equiv a(b * cx).dy(cx * b) \\
&\equiv a.b \circ cx.dx\ ,
\end{aligned}
$$

das Gewünschte, wie der aufmerksame Leser leicht bestätigt. $\square$

Erneut haben wir lediglich auf die Rechtskomplementarität zurückgegriffen. Ist $\mathfrak{S}$ sogar komplementär, so gilt zusätzlich:

$$a.b \equiv c.d \iff a : b = c : d \;\&\; b : a = d : c$$

DENN: $ax.by$ erfüllt $ax : bx = (ax : x) : b$ und aus

$$a : b = c : d \;\&\; b : a = d : c\,,$$

resultiert

$$a.b = (a : b)(a \wedge b).(b : a)(a \wedge b) \equiv (a : b).(b : a) = (c : d).(d : c) \equiv c.d\,.$$

Es erzeugt $\equiv$ also ein *homomorphes Bild* zu $(R, \circ)$, das im weiteren mit $\mathfrak{Q}$ bezeichnet sei. Die Elemente von $\mathfrak{Q}$ sind demnach die $\equiv$ - *Klassen* von R, die wir im allgemeinen mit griechischen Buchstaben benennen. Offenbar bildet nun die Menge aller Klassen, die von Paaren der Form $a.1$ repräsentiert werden, eine zu $\mathfrak{P}$ *isomorphe* Unterhalbgruppe von $\mathfrak{Q}$, wegen

$$a.1 \circ b.1 \equiv ab.1 \quad \text{und} \quad a.1 \equiv b.1 \Longleftrightarrow a = a : 1 = b : 1 = b\,.$$

Ebenso bildet die Menge aller Klassen, die von Paaren der Form $1.b$ erzeugt werden, eine zu $C \cap P$ *antiisomorphe* Unterhalbgruppe von $\mathfrak{Q}$, denn:

$$1.b \circ 1.d = 1.db \quad \text{und} \quad 1.b \equiv 1.d \Longleftrightarrow \; b = b : 1 = d : 1 = d\,.$$

Schließlich folgt für kürzbare b :

$$1.b \circ b.1 \equiv 1.1 \equiv b.b \equiv b.1 \circ 1.b \quad \text{und} \quad 1.1 \circ a.b \equiv a.b \equiv a.b \circ 1.1\,.$$

Aus diesem Grund können wir die abkürzende Bezeichnung a für die von $a.1$ erzeugte Klasse und b^{-1} für die von $1.b$ erzeugte Klasse einführen, so dass wir für die Klasse von $a.b$ auch ab^{-1} und für das Produkt $ab^{-1} \circ cd^{-1}$ auch $ab^{-1}.cd^{-1}$ setzen können, ohne dass dies zu Komplikationen führt.
Insbesondere dürfen wir in ab^{-1} den Sonderfall $a \wedge b = 1$ annehmen, denn es gilt ja nach (3.84) $a.b \equiv (b : a).(a : b)$, und es ist $\{a : b, b : a\}$ ein idempotenter Teiler von b, also gleich $\{1\}$. Denn mit $b \cdot \{a : b, b : a\} = b$ gilt natürlich auch $bx = b$ für alle $x \leq a : b, b : a$.
Weiter ist jedes $b^{-1}a$ ein cb^{-1} – und umgekehrt, beachte – etwa – $ab = by \Longrightarrow b^{-1}a = yb^{-1}$. Sei von nun an $\mathfrak{S}$ mit $\mathfrak{Q}$ fest gewählt.

3. 12. 4 Proposition. *In $\mathfrak{Q}$ liefert die Festsetzung $\alpha \leq \beta \Longleftrightarrow \alpha x = \beta\ (\exists x \in S)$ eine $\vee$-abgeschlossene* isotone Partialordnung. *Ist $\mathfrak{S}$ gar $\wedge$-abgeschlossen, so ist auch $\mathfrak{Q}$ $\wedge$-abgeschlossen.*

BEWEIS.

$$\begin{array}{rrcll} & ab^{-1} \cdot x & = & a \cdot y \cdot b^{-1} & (y \in S) \\ & & = & z \cdot ab^{-1} & (z \in S) \\ \text{und:} & yab^{-1} & = & azb^{-1} & (z \in S) \\ & & = & w \cdot ab^{-1} & (w \in S) \end{array}$$

Daher ist die Existenz eines x mit $\alpha x = \beta$ gleichbedeutend mit der Existenz eines y mit $y\alpha = \beta$. Hieraus folgt unmittelbar, dass $\leq$ reflexiv, transitiv und *isoton* ist. , d.h., $\alpha \leq \beta \Longrightarrow \alpha\gamma \leq \beta\gamma\ \&\ \gamma\beta$.
Gilt weiter $xy\alpha = \alpha$, so folgt für $\alpha = ab^{-1}$ die Implikation $xya = a \rightsquigarrow xa = a$, was die Antisymmetrie sicher stellt. Zu zeigen bleibt somit nur noch, dass Q $\vee$-abgeschlossen ist. Hierzu seien ab^{-1} und cd^{-1} zwei Elemente mit $a \wedge b = 1 = c \wedge d$ und $ab^{-1} \leq cd^{-1}$. Dann folgt $ad \leq bc$ und damit $a \leq c$ und $d \leq b \rightsquigarrow b^{-1} \leq d^{-1}$. Haben wir umgekehrt $a \leq c$ und $b^{-1} \leq d^{-1}$, so gilt *a fortiori* $ab^{-1} \leq cd^{-1}$. Das bedeutet insgesamt $(a \vee c)(b \wedge d)^{-1} = ab^{-1} \vee cd^{-1}$, da mit $a \wedge b = 1 = c \wedge d$ auch $(a \vee c) \wedge (b \wedge d) = 1$ erfüllt ist. Insbesondere ist $\mathfrak{Q}$ demnach $\vee$-treu, d. h. in $\mathfrak{S}$ stimmen die Partialordnungen von $\mathfrak{S}$ und $\mathfrak{Q}$ überein.
Analog verfährt man bezüglich $\wedge$. □

Nach 3.12.4 ist $(Q\,, \leq)$ ein Halbverband. Die nächste Gleichung stellt eine Beziehung zwischen Multiplikation und Vereinigung in Q her. Es gilt:

$$\alpha(\beta \vee \gamma)\delta = \alpha\beta\delta \vee \alpha\gamma\delta\,. \tag{3.166}$$

BEWEIS. Zur Herleitung zeigen wir schrittweise:

$$\begin{array}{lrcl} (i) & \gamma & \geq & ax^{-1} \vee \beta x^{-1} \\ \Longleftrightarrow & \gamma x & \geq & \alpha \vee \beta \\ \Longleftrightarrow & \gamma & \geq & (\alpha \vee \beta)x^{-1} \end{array}$$

$$\begin{array}{lrcll} (ii) & \gamma & \geq & x^{-1}\alpha \vee x^{-1}\beta & \\ \Longleftrightarrow & \gamma & \geq & x^{-1}(\alpha \vee \beta) & (i) \end{array}$$

$$\begin{array}{lrcl}
(iii) & yab^{-1} \vee ycb^{-1} & = & (ya \vee yc)b^{-1} \\
& & = & y(a \vee c)b^{-1} \\
& & = & y(ab^{-1} \vee cb^{-1}) \\[1ex]
(iv) & ab^{-1}y \vee cb^{-1}y & = & a(b*y)(y*b)^{-1} \vee c(b*y)(y*b)^{-1} \\
& & = & \big(a(b*y) \vee c(b*y)\big)(y*b)^{-1} \\
& & = & (a \vee c)(b*y)(y*b)^{-1} \\
& & = & (a \vee c)b^{-1}y \\
& & = & (ab^{-1} \vee cb^{-1})y \\[1ex]
(v) & ab^{-1} & = & a(b*d)(b*d)^{-1}b^{-1} \qquad (\forall\ d \in C) \\
& & = & a(b*d)(b \vee d)^{-1}.
\end{array}$$

Beachten wir nun, dass aufgrund von (v) je zwei Elemente aus Q *gleichnamig* gemacht werden können, so ist nach dem Bisherigen alles gezeigt. □

Ohne Ausführung sei noch erwähnt, dass sich im Falle eines $\wedge$-abgeschlossenen $\mathfrak{S}$ dual die Gleichung

$$\alpha(\beta \wedge \gamma)\delta \;=\; \alpha\beta\delta \wedge \alpha\gamma\delta\,. \tag{3.167}$$

ergibt, wie der Leser leicht bestätigt. Darüber hinaus erhalten wir für $\wedge$-abgeschlossene $\mathfrak{S}$ noch die Gleichung:

$$\alpha \wedge (\beta \vee \gamma)\delta \;=\; (\alpha \wedge \beta) \vee (\alpha \wedge \beta)\,. \tag{3.168}$$

d. h. in diesem Fall ist $(Q, \wedge, \vee)$ distributiv.

BEWEIS. Wie schon betont, folgt die $\wedge$-Abgeschlossenheit analog der $\vee$-Abgeschlossenheit, und es gilt für $a \wedge b = 1 = c \wedge d$ die Gleichung

$$ab^{-1} \wedge cd^{-1} = (a \wedge c)(b \vee d)^{-1}\,.$$

Hieraus ergibt sich weiter unter Berücksichtigung von $a \wedge b = 1 = c \wedge d \Longrightarrow (a \wedge c) \wedge (b \vee d) = 1$ für $a \wedge b = 1 = c \wedge d = 1 = g \wedge k$ die Gleichungskette:

$$\begin{array}{rcl}
ab^{-1} \wedge (cd^{-1} \vee gk^{-1}) & = & ab^{-1} \wedge (c \vee g)(d \wedge k)^{-1} \\
& = & \big(a \wedge (c \vee g)\big)\big(b \vee (d \wedge k)\big)^{-1} \\
& = & \big((a \wedge c) \vee (a \wedge g)\big)\big((b \vee d) \wedge (b \vee k)\big)^{-1} \\
& = & (a \wedge c)(b \vee d)^{-1} \vee (a \wedge g)(b \vee k)^{-1} \\
& = & (ab^{-1} \wedge cd^{-1}) \vee (ab^{-1} \wedge gk^{-1})\,.
\end{array}$$

Damit sind wir am Ziel. □

Wir sahen, dass die Quotientenhülle bis auf Isomorphie von $\mathfrak{S}$ eindeutig bestimmt ist. Der nächste Hilfssatz wird zeigen, dass dies auch für die homomorphen Bilder gilt.

3. 12. 5 Lemma. *Ist $\equiv$ eine Kongruenzrelation in $\mathfrak{S}$ bezüglich $\cdot, *$ und $:$, so lässt sich $\equiv$ eindeutig ausdehnen auf $\mathfrak{Q}$ bezüglich $\cdot, \vee$ und - gegebenenfalls - bezüglich $\wedge$. Entsprechendes gilt für die Rechtskongruenzen.*
Ist S/I sogar linear geordnet, so gibt es keine anderen Klassen bezüglich $\equiv$ als die von den $a \in S$ und den b^{-1} mit $b \in C$ erzeugten.

BEWEIS. Es sei I das $\equiv$ erzeugende (Voll-) Ideal. Setzen wir dann $\alpha \equiv \beta$ gdw. ein $x, y \in S$ und ein $e_1,\ e_2 \in I$ existiert mit $\alpha x = \beta e_1$ und $\beta y = \alpha e_2$, so ist diese Relation in $\mathfrak{Q}$ transitiv und wegen $1 \in I$ eine Äquivalenzrelation, denn

$$\begin{array}{rcl} \alpha x = \beta e_1 & \& & \beta y = \gamma e_2 \\ & \Longrightarrow & \\ ax(e_1 * y) & = & \gamma e_2(y * e_1)\,. \end{array}$$

Ferner ist die erklärte Relation *a fortiori* rechtskongruent und, falls I ein Vollideal ist, sogar kongruent bezüglich $\cdot$, da dann für $b \in C$ aus $be_1 = e_2 b \Longleftrightarrow e_1 b^{-1} = b^{-1} e_2$ für alle $a \in Q$ die Gleichung $aI = Ia$ resultiert.
Weiter ist $\equiv$ auch eine Kongruenzrelation bezüglich $\vee$, denn wir dürfen analog (3.166 , v) annehmen, dass $\alpha = x^{-1}a,\ \beta = x^{-1}b$ und $\beta\,' = x^{-1}b\,'$ und damit die Implikation $\beta \equiv \beta\,' \Longrightarrow b \equiv b\,'$ erfüllt ist, was nach sich zieht:

$$\begin{array}{rcl} \alpha \vee \beta & = & x^{-1}a \vee x^{-1}b \\ & = & x^{-1}(a \vee b) \\ & = & x^{-1}(a \vee b\,') \\ & = & x^{-1}a \vee x^{-1}b\,' \\ & = & \alpha \vee \beta'\,. \end{array}$$

Analog beweisen wir die Behauptung für $\wedge$, falls $\mathfrak{S}$ $\wedge$-abgeschlossen ist.
Ist schließlich S/I linear geordnet, so folgt aus $b^{-1}a = (a * b)^{-1}(b * a) = (b * a)(a * b)^{-1}$, dass jedes α ein a oder ein b^{-1} ist. Also ist in diesem Falle auch $\mathfrak{Q}/I$ linear geordnet ist bezüglich

$$(\alpha) \leq (\beta) \iff (\beta) = (ax)\,.$$

Schließlich zeigt die Äquivalenz

$$\begin{aligned} a^{-1}b = c^{-1}d &\iff (a:c)^{-1}b = (c:a)^{-1}d \\ &\iff (c:a)b = (a:c)d\,, \end{aligned}$$

schon für den Fall einer Rechtskongruenz, dass es keine weitere Ausdehnung von $\equiv$ auf Q gibt. □

3.12.5 liefert für Verbandsgruppen:

3. 12. 6 Korollar. *Es gibt keine anderen Rechtskongruenzen in Verbandsgruppen bezüglich $\cdot$ und $\vee$ als die Ausdehnung der $(\cdot, *)$-Rechtskongruenzen ihres Kegels.*

DENN: Dies folgt aus 3.12.5 und

$$\begin{aligned} ax \geq b \Longleftrightarrow x \geq a^{-1}b &\iff x \geq 1 \vee a^{-1}b \\ &\iff a * b = 1 \vee a^{-1}b\,, \end{aligned}$$

woraus die Rechtskongruenz bezüglich $*$ in $\mathfrak{S}$ resultiert. □

Durch die Quotientenhülle $\mathfrak{Q}$ ist $\mathfrak{S}$ eingebettet in eine sehr spezielle Halbverbandshalbgruppe. Diese ist offenbar *a fortiori* kommutativ gdw. $\mathfrak{S}$ kommutativ ist, $\wedge$-abgeschlossen gdw. $\mathfrak{S}$ $\wedge$-abgeschlossen ist, und keineswegs notwendig vom Typ

$$\forall\ \alpha, \beta \in Q\ \exists\, \alpha * \beta\ :\ \alpha\gamma \geq \beta \Longleftrightarrow \gamma \geq \alpha * \beta\,.$$

Umgekehrt ist der positive Kegel der DLR-*Semigruppe* von Swamy, siehe [147], [148], [149], komplementär, und es bestimmt dieser Kegel die Struktur der Halbgruppe vollständig, aufgrund von $\alpha = \alpha(\alpha \wedge 1)^{-1} \cdot (\alpha \wedge 1)$ und der Herleitung

$$\begin{aligned} \alpha(\alpha \wedge 1)^{-1} \wedge 1 &= \alpha(\alpha \wedge 1)^{-1} \wedge (\alpha \wedge 1)(\alpha \wedge 1)^{-1} \\ &= (a \wedge \alpha \wedge 1)(\alpha \wedge 1)^{-1} \\ &= (\alpha \wedge 1)(\alpha \wedge 1)^{-1} = 1\ , \end{aligned}$$

man beachte, dass jedes α von der Form $a \cdot b^{-1}$ ist.

3.13 Halbgruppenerweiterungen

Ist $\mathfrak{S}$ lediglich rechtskomplementär, so können wir mit einer Quotientenhülle nicht rechnen. Es zeigt sich aber verblüffenderweise, dass die links

kürzbare, rechtskomplementäre Halbgruppe mit einer inversen Halbgruppe korrespondiert.
Eine Halbgruppe heißt *regulär,* wenn zu jedem a ein a' existiert mit $a \cdot a' \cdot a = a$ und $a' \cdot a \cdot a' = a'$. In diesem Fall sind offenbar die Elemente aa' und $a'a$ *idempotent.* Tatsächlich genügt schon die erste Forderung der Regularität, denn aus $aa'a = a$ folgt ja mit $a^* := a'aa'$ zum einen $a \cdot a^* \cdot a = a$ und zum anderen $a^* \cdot a \cdot a^* = a^*$.
Existiert zudem zu jedem a exakt ein a' der beschriebenen Art, so heißt $\mathfrak{S}$ *invers,* und wir bezeichnen dieses eindeutig bestimmte a' mit a^{-1}. Unmittelbar klar ist dann $(a^{-1})^{-1} = a$. Insbesondere ist damit jedes idempotente u ein Inverses seiner selbst.
Für die Inversität gilt die wichtige

3. 13. 1 Proposition. *Ein Halbgruppe ist genau dann invers, wenn sie regulär ist und je zwei Idempotente kommutieren.*

BEWEIS. Kommutieren je zwei Idempotente und erfüllen a', a^* beide gemeinsam die Bedingungen der Regularität für das Element a, so folgt, man beachte die Dualität:

$$a' = a'a(a^*a)a' = (a^*a)(a'aa') = a^*aa' = a'aa^* = a^* .$$

Seien jetzt die exisitierenden a' eindeutig bestimmt. Wir werden zeigen, dass mit je zwei idempotenten Elementen u und v auch deren Produkt idempotent ist. Das bedeutet dann, dass uv und vu zugleich ein Inverses zu uv sind und damit dass $uv = vu$ erfüllt ist.
Sei nach diesen Vorbetrachtungen $w = (uv)^{-1}$. Dann folgt zunächst $w = vwu$, wegen

$$uv \cdot vwu \cdot uv = uv \quad \& \quad vwu \cdot uv \cdot vwu = v \cdot wuvw \cdot u = vwu .$$

Hieraus ergibt als nächstes:

$$w^2 = vwu \cdot uv \cdot vwu = vwu = w$$

und damit weiter, aufgrund von

$$uv \cdot w \cdot uv = uv \;\&\; w \cdot w \cdot w = w \;\&\; w \cdot uv \cdot w = w$$

wegen der Eindeutigkeit der Inversen $uv = w$ die Idempotenz von uv. □

Wir können also festhalten:

3. 13. 2 Korollar. *In inversen Halbgruppen gelten die wichtigen Invertierbarkeitsregeln:*

$$(a^{-1})^{-1} = a \quad und \quad (ab)^{-1} = b^{-1}a^{-1} \tag{3.169}$$

Schließlich beachten wir noch $u^2 = u \Longrightarrow au = (aua^{-1})a$ mit idempotentem (aua^{-1}). Dies bedeutet

$$\begin{aligned} b = au \ (\exists u = u^2) &\iff b = va \ (\exists v = v^2) \\ &\iff b = sat \ (\exists s = s^2, t = t^2) \end{aligned} \tag{3.170}$$

Nach diesen Vorbereitungen lässt sich nun beweisen:

3. 13. 3 Der Homomorphiesatz. *Ist $\mathfrak{S}$ invers, dann ist jeder Halbgruppen-Homomorphismus auch ein Inversen-Homomorphismus.*

BEWEIS. Sei $\sum$ ein inverses Urbild von $\mathfrak{S}$ unter ϕ. Natürlich ist $\mathfrak{S}$ dann regulär. Wir werden zeigen, dass jedes idempotente a zumindest ein idempotentes Urbild besitzt.
Zu diesem Zweck nehmen wir an, es sei $a = a^2 = \phi(\alpha)$ und $x = \phi(\alpha^{-1})$. Dann kommutieren ax und xa, da $\alpha\alpha^{-1}$ und $\alpha^{-1}\alpha$ kommutieren. Also haben wir:

$$\begin{array}{rcl} x = xax = xa \cdot ax &=& (xa \cdot ax)^2 = x^2 \\ & \rightsquigarrow & \\ x = xax = xa \cdot ax &=& ax \cdot xa = axa = a \end{array}$$

und damit

$$a = ax = \phi(\alpha)\phi(\alpha^{-1}) = \phi(\alpha\alpha^{-1}) .$$

Also ist a Bild des idempotenten Urbildes $\alpha\alpha^{-1}$. □

Der Vollständigkeit halber sei noch erwähnt:

3. 13. 4 Korollar. *Eine reguläre Halbgruppe ist genau dann invers, wenn ihre Idempotenten jeweils exakt ein Inverses besitzen.*

BEWEIS. Sei $axa = a$ & $xax = x$ & $aya = a$ & $yay = y$. Dann verhalten sich ax und ay sowie xa und ya jeweils invers zueinander. Und das bedeutet $ax = ay$ & $xa = ya$. Das aber führt dann zu $x = xax = yay = y$. □

Wir kommen nun zu

3. 13. 5 Proposition. *Ist $\mathfrak{S}$ eine inverse Halbgruppe, so erzeugt die Festsetzung $a \equiv b :\Longleftrightarrow au = bu \ (\exists : u = u^2)$ das engste homomorphe Gruppenbild von $\mathfrak{S}$.*

DENN: $\equiv$ im obigen Sinne ist offenbar eine Kongruenzrelation wegen der beiden Implikationen:

$$\begin{array}{rrcl} & au = bu & \Longrightarrow & (sa)u = (sb)v \\ \& & au = bu & \Longrightarrow & a(ss^{-1})u = bss^{-1}u \\ & & \Longrightarrow & \\ (as)(s^{-1}u)(s^{-1}u)^{-1} & & = & (bs)(s^{-1}u)(s^{-1}u)^{-1} \end{array}$$ □

Eine inverse Halbgruppe heißt *e-unitär,* wenn gilt:

$$\begin{array}{rlcl} & a^2 = a \ \& \ (ae)^2 = ae & \Longrightarrow & e^2 = e \\ \& & a^2 = a \ \& \ (ea)^2 = ea & \Longrightarrow & e^2 = e\,. \end{array}$$

Tatsächlich genügt schon eine der beiden Forderungen, denn gilt beispielsweise die erste der beiden Zeilen, so folgt aus $a^2 = a \ \& \ (ea)^2 = ea$ die Implikation:

$$eaea = ea \rightsquigarrow eae = (eae)^2 \rightsquigarrow e^2 = e$$

Als ein wichtiger Struktursatz sei ohne Beweis erwähnt:

3. 13. 6 Proposition. *e-unitäre inverse Halbgruppen sind* semidirekt *zerlegbar in einen Halbverband $\mathfrak{H}$ und seine Automorphismengruppe $\mathfrak{G}$, d. h. sie sind einbettbar in das* kartesische Produkt *der Trägermengen von $\mathfrak{H}$ und $\mathfrak{G}$, betrachtet bezüglich $(\alpha.b) \circ (\beta.b) := (\alpha \vee a\beta.ab)$.*

3.14 Quotienten im links-komplementären Fall

Dieser Abschnitt bietet einen alternativen Zugang vom Verbandsgruppenkegel zu seiner Quotientenerweiterung, ausgehend von einer rechtskomplementären Halbgruppe, fast Wort für Wort übernommen aus [43].

3. 14. 1 Proposition. *Sei $\mathfrak{S}$ rechtskomplementär. Wir bezeichnen $S \times S$ mit Σ. Dann sind paarweise äquivalent*

(LC) $\mathfrak{S}$ *erfüllt* $\quad a * bc = (a * b)((b * a) * c)$

(CL) $\mathfrak{S}$ *is links-kürzbar, d.h.* $\quad ab = ac \Longrightarrow b = c$

(MC) Σ *bildet eine Monoid unter* $\quad a.b \circ c.d = a(b * c) \,.\, d(c * b).$

BEWEIS. (LC)$\Longrightarrow$(CL) , denn

$$\begin{aligned} ab = ac &\Longrightarrow a * ab = a * ac \\ &\Longrightarrow (a*a)((a*a)*b) = (a*a)((a*a)*c) \\ &\Longrightarrow b = c. \end{aligned}$$

(CL)$\Longrightarrow$(LC) , denn $a(a*b)((b*a)*c) = b(b*a)((b*a)*c) \geq bc$ and

$$\begin{aligned} ax \geq bc &\Longrightarrow ax \geq b \\ &\Longrightarrow x \geq a * b \\ &\Longrightarrow x = (a*b)y \\ &\Longrightarrow a(a*b)y \geq bc \\ &\Longrightarrow b(b*a)y \geq bc \\ &\overset{\text{(CL)}}{\Longrightarrow} (b*a)y \geq c \\ &\Longrightarrow y \geq (b*a)*c \\ &\Longrightarrow x \geq (a*b)((b*a)*c)\,. \end{aligned}$$

(LC)$\Longrightarrow$(MC) , wegen

$$\begin{aligned} (a.b \circ x.e) \circ c.d &= a(b*x)\,.\,(x*b) \circ c.d \\ &= a(b*x)((x*b)*c)\,.\,d(c*(x*b)) \\ &= a(b*xc)\,.\,d(xc*b) \\ &= a.b \circ xc.d \\ &= a.b \circ (x.e \circ c.d) \end{aligned}$$

und

$$\begin{aligned} (a.b \circ e.y) \circ c.d &= a.yb \circ c.d \\ &= a(yb*c)\,.\,d(c*yb) \\ &= a(b*(y*c))\,.\,d(c*y)((y*c)*b) \\ &= a.b \circ (y*c)\,.\,d(c*y) \\ &= a.b \circ (e.y \circ c.d)\ , \end{aligned}$$

woraus die allgemeine Assoziativität folgt vermöge

$$\begin{aligned} (a.b \circ x.y) \circ c.d &= (a.b \circ (x.e \circ e.y)) \circ c.d \\ &= ((a.b \circ x.e) \circ e.y) \circ c.d \\ &= (a.b \circ x.e) \circ (e.y \circ c.d) \\ &= \ \ldots \\ &= a.b \circ (x.y \circ c.d)\ . \end{aligned}$$

Schließlich erhalten wir $a.b \circ e.e = a.b = e.e \circ a.b$, weshalb Σ sogar ein Monoid bezüglich $\circ$ bildet.

(MC)$\Longrightarrow$(LC) . Der Vergleich der Zeilen 2 und 3 im Beweis von

$$(a.b \circ x.e) \circ c.d \;=\; a.b \circ (x.e \circ c.d)$$

führt zu

$$a((b * x)((x * b) * c) \;=\; a(b * xc)$$

das ist Bedingung (LC) – man setze $a = e$. □

3. 14. 2 Proposition. *Erfüllt* $\mathfrak{S}$ *eine der obigen Bedingungen* (LC), (CL), (MC)*, so ist* $\sum := (\Sigma, \circ)$ *sogar bisimpel und invers mit Einselement* $e.e. =: \varepsilon$ *mit 1-elementigen Untergruppen. Darüber hinaus sind die Elemente vom Typ* $a \circ \beta$ *worin* α *eine Rechts-Einsteiler und* β *eine Links-Einsteiler ist.*

Weiterhin *ist* $\sum$ *e-unitär gdw.* $\mathfrak{S}$ *kürzbar ist* [2]*, und in diesem Falle trennt die feinste Gruppenkongruenz* $a.b \equiv c.d \Longleftrightarrow a.b \circ u.u = c.d \circ u.u \;\; (\exists u.u)$ *jedes Paar* $a.e \neq b.e$ *.*

Schließlich *definiert in jedem Falle*

(PO) $$a.b \leq c.d \;\;:\Longleftrightarrow\;\; a \leq c \;\&\; b \geq d$$

eine Partialordnung mit

(LD) $$a.b \leq c.d \Longrightarrow a.b \,\big|_{\ell}\, c.d$$

und erfüllt $\mathfrak{S}$ *darüber hinaus*

(RL) $$a * (b * a) \;=\; e \;,$$

d.h. gilt $\big|_{\ell} \supseteq \big|_{r}$*, so ist die Partialordnung zusätzlich verträglich mit der Multiplikation.*

BEWEIS. Wir betrachten das Monoid $\sum := (\Sigma, \circ)$ der Proposition 3.14. 1. Dort ist jedes $a.b$ gleich $a.e \circ e.b$, und es gilt $e.a \circ a.e = e.e$. Daher ist

[2] als ein Beispiel, das die Verbandsgruppenkegelbedingungen nicht erfüllt, sei Beispiel 18 erwähnt.

jedes Element aus Σ vom Typ $\alpha \circ \beta$ mit $\alpha\big|_r \varepsilon$ and $\beta\big|_\ell \varepsilon$.
Als nächstes ist $\sum$ regulär wegen $a.b \circ b.a \circ a.b = a.b$. Darüber hinaus erhalten wir

$$\begin{aligned}(a.b)^2 = a.b &\Longrightarrow a = a(b * a) \;\&\; b = b(a * b)\\ &\Longrightarrow b * a = e = a * b\\ &\Longrightarrow a = b\,.\end{aligned}$$

Folglich sind die Produkte von Idempotenten offenbar idempotent. Somit ist die betrachtete Ausdehnung nicht nur regulär, sondern sogar invers mit

$$(a.b)^{-1} \;=\; b.a\,.$$

Ferner gilt

$$x.y \circ y.x = y.x \circ x.y \Longrightarrow x = y\;. \tag{3.174}$$

Somit sind alle Untergruppen 1-elementig.
Endlich ist $\sum$ bisimpel, d.h. für jedes Paar (von Paaren) $a.b\,, c.d$ existiert ein $x.y$ derart dass $a.b$ und $x.y$ einander von links teilen und derart, dass $x.y$ und $c.d$ einander von rechts teilen.
Zur Erinnerung: $a.x \circ x.y = a.y$, d.h. es ist $a.x$ Linksteiler eines jeden $a.y$ und dual ist $u.b$ Rechts-Teiler eines jeden $v.b$, weshalb $a.d$ die Behauptung bezüglich $a.b\,, c.d$ erfüllt.

Weiterhin, ist $\mathfrak{S}$ kürzbar, wie etwa im kommutativen Fall oder auch im Verbandsgruppenkegel-Fall und ist zudem $a.a \circ x.y = a(a * x).y(x * a)$ idempotent, so resultiert

$$x(x * a) = y(x * a) \rightsquigarrow x = y\,, \tag{3.175}$$

also ist $\sum$ in diesem Fall e-unitär, und ist umgekehrt $\sum$ e-unitär, so resultiert aus $ac = bc$

$$\begin{aligned} ac.ac \circ b.a &= ac(ac * b)\,.\,a(b * ac)\\ &= ac(bc * b)\,.\,a(b * bc)\\ &= ac\,.\,ac\\ &\overset{(3.175)}{\rightsquigarrow} a = b\;. \end{aligned} \tag{3.176}$$

Darüber hinaus erzeugt die oben definierte Relation $\equiv$ die feinste Gruppen-Kongruenz. Daher bleibt nur noch zu zeigen, dass im Falle eines kürzbaren $\mathfrak{S}$ die im Falle $a \neq b$ die Elemente $a.e$, $b.e$ getrennt werden. Dies aber folgt aus

$$a.e \circ u.u = b.e \circ u.u \Longrightarrow au.u = bu.u \Longrightarrow au = bu \Longrightarrow a = b \ . \tag{3.177}$$

Schließlich erhalten wir mit Blick auf Ordnungsprobleme, dass

$$a.b \leq c.d \Longrightarrow a.b \circ b(a * c)\,.\,d = c.d \Longrightarrow a.b\big|_\ell\, c.d \tag{3.178}$$

erfüllt ist und darüber hinaus die Bedingung (RL) die Implikation

$$v \leq w \Longrightarrow u * v \leq u * w \ \& \ u \leq v \Longrightarrow u * w \geq v * w \tag{3.179}$$

nach sich zieht. Das führt dann zu

$$\begin{array}{rcl} a.b & \leq & c.d \\ & \Longrightarrow & \\ a.b \circ x.y & = & a(b * x)\,.\,y(x * b) \\ & \leq & c(d * x)\,.\,y(x * d) \\ & = & c.d \circ x.y \end{array} \tag{3.180}$$

und zu

$$\begin{array}{rcl} a.b & \leq & c.d \\ & \Longrightarrow & \\ x.y \circ a.b & = & x(y * a)\,.\,b(a * y) \\ & \leq & x(y * c)\,.\,d(c * y) \\ & = & x.y \circ c.d \ . \end{array} \tag{3.181}$$

Wir symbolisieren nun die $\equiv$-Klasse von $a.b$ mittels $\overline{a.b}$. Dann definiert

$$\begin{array}{ccc} \overline{a\,.\,b} & \overline{\leq} & \overline{c\,.\,d} \\ & :\Longleftrightarrow & \\ a.b \circ x.y & \leq & c.d \circ x.y \ \ (\exists\ x.y) \\ & \Longleftrightarrow & \\ a.b \circ u.u & \leq & c.d \circ u.u \ \ (\exists\ u.u) \end{array}$$

eine PO auf $\overline{\Sigma}$, wie man leicht bestätigt. Und es ist PO $\circ$-verträglich.

Dies ist linksseitig evident und folgt rechtsseitig *via*

$$\begin{array}{rcl} a.b \circ u.u & \leq & c.d \circ u.u \\ & \Longrightarrow & \\ (a.b \circ x.y) \circ (y.x \circ u.u) & \leq & (c.d \circ x.y) \circ (y.x \circ u.u) \end{array} \qquad \square$$

Hiernach wenden wir uns den Verbandsgruppenkegeln zu. Sie erfüllen

$$a.b \equiv cd \Longleftrightarrow \exists x, y : ax = cy \ \& \ bx = dy \tag{3.182}$$

DENN:

$$\begin{array}{rl} & a.b \equiv c.d \\ \Longrightarrow & a.b \circ u.u = c.d \circ u.u \ \ (\exists u \in S) \\ \Longrightarrow & a(b * u).u(u * b) = c(d * u).u(u * d) \\ \Longrightarrow & a(b * u).b(b * u) = c(d * u).d(d * u) \end{array}$$

UND

$$\begin{array}{rl} & ax.bx = cy.dy \\ \Longrightarrow & a.b \circ bx.bx = c.d \circ dy.dy \\ \Longrightarrow & a.b \circ bx.bx \circ dy.dy = c.d \circ dy.dy \circ bx.bx \\ \Longrightarrow & a.b \equiv c.d\,. \end{array}$$

Damit sind wir in der Lage zu zeigen:

3. 14. 3 Proposition. *Sei $\mathfrak{S}$ ein Verbandsgruppenkegel. Dann liefert der Beweis von 3.14.2 eine alternative Methode für die Einbettung von $\mathfrak{S}$ in seine Quotientengruppe.*

BEWEIS. Ist $\mathfrak{S}$ eine Verbandsgruppenkegel (3.182) so folgt

$$a.b = (a : b)(a \wedge b).(b : a)(a \wedge b) \equiv (a : b).(b : a) \tag{3.183}$$

Dies liefert weiter

$$a.b \equiv c.d \Longrightarrow a : b = c : d \ \& \ b : a = d : c\,, \tag{3.184}$$

wegen

$$\begin{array}{rcl} a \bot b \ \& \ c \bot d \ \& \ a.b \equiv c.d & \Longrightarrow & e.b \circ a.e \equiv c.e \circ e.d \\ & \Longrightarrow & b.b \circ a.e \circ d.e \equiv b.e \circ c.e \\ & \Longrightarrow & b.b \circ ad.e \equiv bc.e \\ & \Longrightarrow & ad.e \equiv bc.e \\ & \overset{(3.107)}{\Longrightarrow} & a = c \ \& \ b = d\,. \end{array}$$

Das bedeutet aber: Jede Klasse $\overline{a.b}$ enthält ein eindeutig bestimmtes orthogonales Paar $A.B$ und alle anderen Paare dieser Klasse sind vom Typ $Ax.Bx$.

Wir betrachten nun die Menge G aller orthogonalen Paare $a.b$. Nach den Regeln der Arithmetik resultiert fast unmittelbar

$$a \perp b \;\&\; c \perp d \Longrightarrow (a \vee c) \perp (b \wedge d)\,, \tag{3.185}$$

weshalb G abgeschlossen ist unter

$$a\,.\,b\,\nabla\,c\,.\,d \;:=\; (a \vee c)\,.\,(b \wedge d) \tag{3.186}$$

$$a\,.\,b\,\Delta\,c\,.\,d \;:=\; (a \wedge c)\,.\,(b \vee d)\,. \tag{3.187}$$

Weiterhin erhalten wir nach (3.97),(3.98), (3.184) und den Kürzungsregeln, dass G auch abgeschlossen ist bezüglich $\circ$, wegen

$$\begin{array}{rcl}
a \perp b & \& & c \perp d \\
& \Longrightarrow & \\
a.b \circ c.d & = & a(b * c)\,.\,d(c * b) \\
& \equiv & a(b * c) : d(c * b)\,.\,d(c * b) : a(b * c) \\
& = & (a : ((c * b) : (b * c)))((b * c) : (c * b)) : d \\
& . & (d : ((b * c) : (c * b)))((c * b) : (b * c)) : a \\
& \overset{(3.98)}{=} & (a : (c * b))(b * c) : d \;.\; (d : (b * c))(c * b) : a \\
& \overset{(3.98)}{=} & a(b * c) : d \;.\; d(c * b) : a \\
& = & (a : d)(b * c)\,.\,(d : a)(c * b)\,.
\end{array}$$

Folglich bildet $\overline{\Sigma}$ eine *po*-Gruppe bezüglich $\circ$ und $\overline{\leq}$, und es bleibt nur noch zu zeigen, dass $\overline{\leq}$ einen Halbverband definiert.

Um dies zu bestätigen verifizieren wir $\overline{A.B} \;\overline{\leq}\; \overline{C.D} \Longrightarrow A \leq C \;\&\; B \geq D$ und beweisen so $\overline{A \vee C\,.\,B \wedge D} = \sup(\overline{A.B}\,,\,\overline{C.D})$, was weiter mit $E := e$ zu

$$\begin{array}{rl}
& \overline{A.B} \;\overline{\leq}\; \overline{C.D} \\
\Longrightarrow & (\exists\, U.U) \quad U.U \circ A.B \leq U.U \circ C.D \\
\Longrightarrow & U.U \circ A.E \circ E.B \leq U.U \circ C.E \circ E.D \\
\Longrightarrow & U.U \circ A.E \circ E.B \circ D.E \leq U.U \circ C.E \\
\overset{(3.170)}{\Longrightarrow} & (\exists V.V) \quad A.E \circ E.B \circ D.E \circ V.V \leq C.E \circ V.V \\
\overset{(3.170)}{\Longrightarrow} & E.B \circ A.E \circ D.E \circ V.V \leq C.E \circ V.V
\end{array}$$

$$
\begin{aligned}
&\Longrightarrow && B.B \circ A.E \circ D.E \circ V.V \leq B.E \circ C.E \circ V.V\\
&\overset{(3.170)}{\Longrightarrow} && (\exists\, W.W) A.E \circ D.E \circ W.E \circ E.W \leq B.E \circ C.E \circ W.E \circ E.W\\
&\Longrightarrow && ADV \leq BCV\\
&\overset{(RC)}{\Longrightarrow} && AD \leq BC\\
&\overset{(3.107)}{\Longrightarrow} && A \leq C \;\&\; D \leq B\,.
\end{aligned}
$$

führt und den Beweis abschließt. □

Eine historische Anmerkung. Üblicherweise wählt man als Einbettungsmethode ORE's klassisches Einbettungsresultat, doch die spezielle Verbandsgruppensituation gibt Anlass nach einer speziellen Einbettungsmethode zu suchen, wie oben geschehen.
Eine ähnliche Methode werden wir später bei der Einbettung von *Verbandsloopkegeln* in *Verbandsloops* wählen und mittels der Definition

$$a.b \circ c.d \;:=\; (a:d)(b*c)\,.\,(d:a)(c*b) \tag{3.188}$$

$$a\,.\,b \bigvee c\,.\,d \;:=\; (a \vee c)\,.\,(b \wedge d) \tag{3.189}$$

ein Problem von J. VON NEUMANN lösen. Es ist nicht schwierig zu sehen, dass die Menge der orthogonalen Paare $A\,.\,B$, $C\,.\,D$,...,$U\,.\,V$ abgeschlossen ist bezüglich $\circ$ und $\bigvee$ und dass $A.B \leq C.D :\Longleftrightarrow A \leq C \;\&\; B \geq D$ eine verträgliche PO definiert. Doch der Beweis, dass im gegebenen Fall auch die Assoziativität mit geht, ist sehr technisch, im Gegensatz zu dem obigen Beweis, der ganz beträchtlich von den Struktureigenschaften von $\sum$ profitiert.

3.15 Wann ist $\mathfrak{Q}$ invers?

Wir kehren zurück zur komplementären Halbgruppe $\mathfrak{S}$ mit Quotientenhülle $\mathfrak{Q}$. Ist $\mathfrak{S}$ idempotent, so haben wir grob gesprochen $\mathfrak{S} = \mathfrak{Q}$, ist $\mathfrak{S}$ sogar kürzbar, so ist $\mathfrak{Q}$ natürlich eine Verbandsgruppe. Ist $\mathfrak{S}$ Produkt einer kürzbaren und einer idempotenten komplementären Halbgruppe, so ist $\mathfrak{Q}$, wie man leicht sieht, invers.
Frage: Sind dies schon alle komplementären Halbgruppen mit inverser Hülle $\mathfrak{Q}$? Antwort: Es gilt in der Tat:

3. 15. 1 Proposition. *Die Quotientenhülle $\mathfrak{Q}$ einer komplementären Halbgruppe $\mathfrak{S}$ ist genau dann invers, wenn $\mathfrak{S}$ Produkt eines brouwerschen Halbverbandes mit einem Verbandsgruppenkegel ist.*

BEWEIS. Sei Q invers und sei $a \perp b$ sowie ab^{-1} idempotent. Dann folgt:

$$\begin{array}{rrcll} & ab^{-1} & = & (ab^{-1})^2 & \\ & & = & a^2b^{-1}b^{-1} & \\ \Longrightarrow & a & = & a^2b^{-1} & \\ \Longrightarrow & a^2 & = & ab & \\ \Longrightarrow & a^2 & = & a & (a\perp b) \\ \Longrightarrow & ab^{-1} & = & ab^{-1}b^{-1} & \\ \Longrightarrow & a & = & ab^{-1} \in S\,. & (\star) \end{array}$$

Sei nun $x \perp y$ und gelte

$$\begin{array}{rcl} a & = & a \cdot (x^{-1}y) \cdot a \\ & \& & \\ x^{-1}y & = & (x^{-1}y) \cdot a \cdot (x^{-1}y) \end{array}$$

dann folgt weiter

$$\begin{array}{rrcll} & x^{-1}ya & = & (x^{-1}ya)^2 \in S & (\star) \\ \rightsquigarrow & ya & \geq & x & \\ \rightsquigarrow & x & \leq & a & \\ \rightsquigarrow & a' & := & ax^{-1} \in S & \\ \rightsquigarrow & ya'y & = & y & \\ \rightsquigarrow & y & = & y^2\,. & \end{array}$$

Wir zeigen nun, dass $y = ax^{-1}$ erfüllt ist, was dann bedeutet, dass $a = (ax^{-1}) \cdot x$ mit idempotentem $ax^{-1} \in S$ und kürzbarem $x \in C \cap S$ eine Zerlegung der gewünschten Art darstellt. Es gilt:

$$\begin{array}{rrcl} & a \cdot x^{-1}y \cdot a & = & a \\ \rightsquigarrow & a'ya & = & a \\ \rightsquigarrow & ya & = & a \\ \rightsquigarrow & yay & = & a \\ \rightsquigarrow & y & = & ya'y \\ & & = & yax^{-1}y \\ & & = & ya \cdot yx^{-1} \\ & & = & a \cdot x^{-1}\,. \end{array}$$

Sei hiernach umgekehrt die Bedingung des Satzes erfüllt. Dann lässt sich a zerlegen in uv mit idempotentem u und kürzbarem v, und es gilt:

$$\begin{aligned} uv &= (uv)\cdot(uv^{-1})\cdot(uv) \\ uv^{-1} &= (uv^{-1})\cdot(uv)\cdot(uv^{-1}) \end{aligned}$$

Ferner liegen die Idempotenten von $\mathfrak{Q}$, wie oben gezeigt, in $\mathfrak{S}$, also im Zentrum von $\mathfrak{S}$ und damit auch im Zentrum von $\mathfrak{Q}$. □

3.16 Der idempotente Fall

Grob gesprochen haben wir rechtskomplementären Halbgruppen eine spezielle Halbgruppenerweiterung zugeordnet, von der aus Rückschlüsse auf die Ausgangsstruktur möglich wurden. Abhängig war diese Erweiterung von der Existenz kürzbarer Elemente. Wir wenden uns nun einer alternativen Erweiterung zu, die idempotente komplementäre Halbgruppen – also browersche Halbverbände – in eine Erweiterungshalbgruppe einbettet.

3. 16. 1 Proposition. *Eine rechtskomplementäre Halbgruppe $\mathfrak{S} = (S, \cdot, *)$ ist ein brouwerscher Halbverband, gdw. $H := S \times S$ bezüglich*

$$(a\,.\,b \circ c\,.\,d := a(a * b)\,.\,bd) \tag{3.190}$$

eine Halbgruppe bildet.

BEWEIS. Aufgrund der Definition erhalten wir:

$$\begin{aligned} (a\,.\,b \circ c\,.\,d) \circ u\,.\,v &= (a(b * c)\,.\,bd) \\ &= a(b*c)(bd*u)\,.\,bdv \\ \text{und} \qquad a\,.\,b \circ (c\,.\,d \circ u\,.\,v) &= a\,.\,b \circ (c(d*u)\,.\,dv) \\ &= a(b*c(d*u))\,.\,bdv\,. \end{aligned}$$

Ist $\mathfrak{S}$ nun brouwersch, so folgt weiter:

$$\begin{aligned} a(b*c(d*u) &= a(b*c)(b*(d*u)) \\ &= a(b*c)(bd*u)\,. \end{aligned}$$

Folglich ist $\circ$ in diesem Falle assoziativ, $\mathfrak{H}$ also eine Halbgruppe.
Sei hiernach $\mathfrak{H}$ eine Halbgruppe. Dann erhalten wir:

$$a(b*c(d*u)) = a(b*c)(bd*u)\,.$$

Wir setzen zunächst $a = 1 = c$. Dann folgt:

$$b * cu \;=\; (b * c)(b * u)\,.$$

und damit

$$\begin{aligned} a * a^2 &= (a * a)(a * a) = 1 \\ \rightsquigarrow \quad a &= a^2\,. \end{aligned}$$

Also ist $\mathfrak{S}$ idempotent. Und setzen wir weiter $a = 1 = c$, so erhalten wir:

$$bd * u \;=\; b * (d * u)\,,$$

weshalb $\mathfrak{S}$ auch kommutativ, insgesamt also brouwersch sein muss. □

Erwähnt sei noch die evidente Tatsache, dass die soeben zum brouwerschen Halbverband konstruierte Erweiterung natürlich in der Regel nicht kommutativ, sehr wohl aber immer idempotent ist. Dies könnte Anregung geben zur Konstruktion von idempotenten Halbgruppen.

3.17 Beispiele

Beispiel 1: Es sei $\mathfrak{S}$ die Halbgruppe der Elemente $1, a, b$ mit $1x = x = x1$, $ab = aa = a$ und $ba = bb = b$, sowie $x * y = 1 = y : x$.

Beispiel 2: Es sei $\mathfrak{S}$ der Verband der Elemente $1, a, b, c, 0$ mit $1 \leq a \leq b \leq 0,\ 1 \leq c \leq 0,\ 1 * x = x,\ 0 * x = x * x = x * 1 = 1,\ a * 0 = b * 0 = c,\ c * 0 = a,\ a * b = c * b = b,\ a * c = b * c = c,\ c * a = a,\ b * a = 1$ sowie $b : a = a * b$ und $a \circ a = 0$. Man betrachte $\mathfrak{S}$ bezüglich $\vee$.

Beispiel 3: Es sei $\mathfrak{S}$ eine nicht kommutative Halbgruppe mit 0, betrachtet bezüglich $a * b = b : a = 0$.

Beispiel 4: Es sei $\mathfrak{S}$ eine Menge von mindestens zwei Elementen a, b, betrachtet bezüglich $ab = b = a * b$.

Beispiel 5: Es sei $\mathfrak{S}$ eine kommutative Halbgruppe mit 1 und mindestens zwei verschiedenen Elementen a, b, betrachtet bezüglich $a * b = 1$, falls $a = b$, und $a * b = b$, falls $a \neq b$ gilt.

Beispiel 6: Es sei $\mathfrak{S}$ ein Halbverband mit mindestens zwei verschiedenen Elementen. Man setze $a * b = b$.

Beispiel 7: Es sei $\mathfrak{S}$ die Menge aus Beispiel 4, betrachtet bezüglich $ab = b$ und $a * b = \mathit{const.}$

Beispiel 8: Es sei $\mathfrak{S}$ eine abelsche Gruppe mit $a * b = b : a = a^{-1} \cdot b$.

Beispiel 9: Es sei $\mathfrak{S}$ die Halbgruppe der Zahlen $1, 2, 4, 6, \ldots$ mit der üblichen Multiplikation. Man setze $a*b = b : a = b/a$, falls $a \,\big|\, b$, $a*b = b : a = 1$, falls $b \,\big|\, a$, und $a * b = b : a = b$ im letzten Fall.

Beispiel 10: Es sei $\mathfrak{S}$ eine Halbgruppe der Elemente $1, a, b, 0$ mit der Multiplikation $1x = x = x1,\ 0x = 0 = x0,\ ab = aa = a,\ ba = bb = b$. Diese Halbgruppe ist rechtskomplementär. Man erkläre $a : b$ so, dass $a : a = 1$ sowie $(x : y)y = y(y * x)$ ist und setze $a \circ a = 0$.

Beispiel 11: Es sei $\mathfrak{S}$ die Halbgruppe aus Beispiel 10 mit $x : y = x$.

Beispiel 12: Es sei $\mathfrak{S}$ die Halbgruppe, die aus Beispiel 10 durch Spiegelung an der Diagonalen hervorgeht. Man setze $x * y = y : x$.

Beispiel 13: Es sei $\mathfrak{S}$ ein Halbverband mit 1 und 0. Man setze $a * b = 1$, falls $a \geq b$, und $a * b = b$ sonst.

Beispiel 14: Es sei $\mathfrak{S}$ eine unendliche boolesche Algebra mit $\vee$ als $\cdot$.

Beispiel 15: Es sei $\mathfrak{S}$ der Bereich der reellen Zahlen des abgeschlossenen Intervalls $[\,0, 1\,]$. Man setze $ab = a + b$, falls $a + b \leq 1$ ist, und $ab = \infty$, falls $a + b > 1$ ist, sowie $a * b = 0$.

Beispiel 16: Es sei $\mathfrak{S}$ der Bereich aus Beispiel 15, diesmal mit $a * b = 0$, falls $a = b$ gilt, und $a * b = b$, falls $a \neq b$ ist.

Beispiel 17: Es sei $\mathfrak{S}$ der Bereich aus Beispiel 15 mit $a * b = 1$.

Beispiel 18: Es sei $\mathfrak{S}$ die Halbgruppe der Paare $(a \,|\, b)$ nicht negativer ganzer Zahlen bezüglich $(a \,|\, b)(c \,|\, d) = (a + c \,|\, 2^c b + d)$. $\mathfrak{S}$ ist rechtskomplementär. Man erkläre $a : b$ so, dass $ba : a = b$ ist.

Beispiel 19: Es sei $\mathfrak{S}$ die Halbgruppe der Ordnungsisomorphismen von $\mathbf{R}$ auf Enden von $\mathbf{R}$ mit $r \leq \varphi(r)$. Erklärt man in dieser Halbgruppe $a \circ b$ als ba, so ist $\mathfrak{S}$ bezüglich $\circ$ rechtskomplementär und es gilt $a \Big|_{\ell}\, b \Longleftrightarrow a \Big|_{r}\, b$. Man setze $b : a$ so fest, dass $(b : a) \circ a = a \vee b$ wird.

Beispiel 20: Es sei $\mathfrak{S}$ eine Menge von mindestens zwei Elementen. Man setze $ab = a$ und $a * b = b$.

Beispiel 21: Es sei $\mathfrak{S}$ eine kommutative Halbgruppe mit 1. Man setze $a * b = 1$, falls $a = b$ ist, man setze $a * b = b$, falls $a \neq b$ gilt.

Beispiel 22: Man betrachte die Elemente $1, a, b, 0$ bezüglich der Verknüpfungen $x1 = x$ und $xy = 1$, falls $y \neq 1$, sowie $x * x = 1$ und $x * y = 0$, falls $y \neq x$.

Beispiel 23: Es sei $\mathfrak{S}$ die Menge der reellen Zahlen aus $[\,0, 1\,]$, betrachtet bezüglich $ab = \min(a + b, 1)$.

Kapitel 4

Gleichungsbasen

Vom allgemein theoretischen Standpunkt aus gesehen, mag der Leser dieses Kapitel auslassen. Doch scheint der Inhalt von einem gewissen Reiz für Liebhaber. Gezeigt wird im einzelnen:

1. *Jede Klasse rechtskomplementärer Halbgruppen, die sich mit endlich vielen Gleichungen beschreiben lässt, lässt sich auch mit zwei Gleichungen beschreiben.*

2. *Jede Klasse komplementärer Halbgruppen, die sich mit endlich vielen Gleichungen beschreiben lässt, lässt sich auch mit einer (einzigen) Gleichung beschreiben.*

3. *Es gibt eine „common structured fundamental equation", zu deutsch vielleicht eine „Muttergleichung" für den Verbandsgruppenkegel, den Verbandsloopkegel, die boolesche Algebra, die Verbandsgruppe, die Verbandsloop – UND (!) – die abelsche Gruppe.*

4.1 Zur rechtskomplementären Halbgruppe

4. 1. 1 Proposition. *Eine Algebra $(S, \cdot, *)$ ist genau dann eine rechtskomplementäre Halbgruppe, wenn sie den beiden Axiomen genügt:*

$$\text{(A1)} \qquad a(b * b) = a\,,$$

$$\text{(B2)} \qquad u(u * (ab * c)) = (b * (a * c))((ab * c) * u)\,.$$

BEWEIS. Setzen wir $u = ab * c$, so erhalten wir

$$\text{(A2)} \qquad ab * c = b * (a * c)$$

Zu zeigen bleibt (A3), was wir über eine Kette von Zwischenschritten leisten. Zunächst setzen wir hierzu $b = x * x$ und erhalten

$$u(u * (a * c)) = (a * c)((a * c) * u)\,, \tag{4.4}$$

womit wir weiter zeigen können

$$\begin{aligned}
v * v &= (v * v)(a * a) && (4.5)\\
&= (v * v)(a(v * v) * a)\\
&\overset{(4.4)}{=} (a * a)((a * a) * (v * v)) && (4.6)\\
&= a * a\\
&:= e\,.
\end{aligned}$$

Hiernach folgen sukzessive:

$$\begin{aligned}
(e * a) * e &= (e * a) * (e * e)\\
&= e(e * a) * e && \text{(A2)}\\
&= (a * e) * e && (4.4)\\
&= (a * e) * (a * e)\\
&= e
\end{aligned}$$

$$\begin{aligned}
e * a &= (e * a)((e * a) * e) && (4.6)\\
&= e(e * (e * a)) && (4.4)\\
&= e(e * a)
\end{aligned} \tag{4.7}$$

$$\begin{aligned}
(e * a) * a &= e(e * a) * a && (4.7)\\
&= (e * a) * (e * a) && (4.4)\\
&= e
\end{aligned} \tag{4.8}$$

$$\begin{aligned}
e * a &= (e * a)((e * a) * a) && (4.8)\\
&= a(a * (e * a)) && (4.4)\\
&= a(ea * a)
\end{aligned} \tag{4.9}$$

(4.10)
$$\begin{aligned} e * ea &= (ea)(e(ea) * ea) \\ &= (ea)(ea * (e * ea)) \\ &= (ea)(a * (e * (e * ea))) \\ &= (ea)(a * (e * ea)) \\ &= (ea)(ea * ea) \\ &= ea \end{aligned}$$

(4.11)
$$\begin{aligned} a(a * eb) &= a(a * (e * eb)) && (4.10) \\ &= (e * eb)((e * eb) * a) \\ &= (eb)(eb * a) \end{aligned}$$

(4.12)
$$\begin{aligned} e(bc) &= (e(bc))((eb)c * (eb)c) \\ &= (e(bc))(c * (eb * (eb)c)) \\ &= (e(bc))(c * (b * (e * (eb)c))) \\ &= (e(bc))(bc * (e * (eb)c)) \\ &= (e(bc))(e(bc) * (eb)c) \\ &= ((eb)c)((eb)c * e(bc)) && (4.11) \\ &= ((eb)c)(c * (eb * e(bc))) \\ &= ((eb)c)(c * (b * (e * e(c)))) \\ &= ((eb)c)(bc * (e * e(bc))) \\ &= ((eb)c)(e(bc) * e(bc)) \\ &= (eb)c \end{aligned}$$

(4.13)
$$\begin{aligned} ea &= ea(ea * ea) \\ &= ea(a * (e * ea)) \\ &= e(a(a * ea)) && (4.10) \\ &= e(ea(ea * a)) && (4.11) \\ &= (ee)(a(ea * a)) && (4.12) \\ &= e(e * a) && (4.9) \\ &= e * a && (4.7) \end{aligned}$$

(4.14)
$$\begin{aligned} ea &= e * a && (4.13)\\ &= a(ea * a) && (4.9)\\ &= a((e * a) * a) \\ &= ae = a && (4.8) \end{aligned}$$

(4.15)
$$\begin{aligned} e * a = \ a &= ea \\ a * e &= (e * a) * e \\ &= e\ . && (4.4) \end{aligned}$$

Damit sind wir am Ziel. □

Als Korollar sei schließlich festgehalten:

(A3)
$$\begin{aligned} a(a * b) &= a(a * (e * b)) \\ &= (e * b)((e * b) * a) \\ &= b(b * a) \end{aligned}$$

Aus Satz 4.1.1 ergibt sich fast unmittelbar

4. 1. 2 Proposition. *Sei $\mathfrak{A}$ Varietät, die sich mit endlich vielen Gleichungen vermöge der Operationen $\circ_\nu$ beschreiben lässt. Lassen sich dann die Axiome* (A1), (A2), (A3) *bezüglich zweier aus den $\circ_\nu$ abgeleiteter Operationen verifizieren, so ist $\mathfrak{A}$ zweibasig.*

BEWEIS. Zunächst gilt $ab = e \Longrightarrow b = e$ und $a = b \Longleftrightarrow (a*b)(b*a) = 1$. Hieraus resultiert weiter, dass jedes endliche System von Gleichungen

(4.17)
$$f_\nu \ = \ g_\nu \ \ (\nu = 1, \ldots, n)$$

„komprimiert" werden kann zu einer einzigen Gleichung

(G)
$$p \ := \ \prod_1^n \Big((f_\nu * g_\nu) \cdot (g_\nu * f_\nu)\Big) = e\,,$$

wobei diese Identität gleichwertig ist mit $x * p = e$. Daher können wir (B2) durch Juxtaposition von $v * p$ spezialisieren zu

(B2')
$$u(u * (ab * c))(v * p) \ = \ ((b * (a * c))((ab * c) * u))\,.$$

Somit sind wir am Ziel, denn wir erhalten (B2) aus 4.1.1 und (A1) durch Ersetzung von v mittels p und die Gleichung $p = e$ mittels $u = v = a = b = c = e$. □

Es ist klar, dass Gleichung (B2') in Sonderfällen bezüglich seiner Länge und der Anzahl ihrer Variablen reduziert werden kann. Von besonderem Interesse ist diesbezüglich natürlich die kommutative komplementäre Halbgruppe. Hier können wir zeigen:

4. 1. 3 Proposition. *Eine Algebra $S(\cdot, *)$ ist genau dann eine kommutative komplementäre Halbgruppe, wenn sie den beiden Axiomen genügt:*

$$\text{(B1)} \qquad a(b*b) = a\,,$$

$$\text{(BK)} \qquad (ab*c)((u(u*v))) = (v(v*u))(b*(a*c))\,.$$

BEWEIS. Setzen wir $b = a*a$ und $c = a$, so erhalten wir

$$\text{(4.22)} \qquad (a*a)(u(u*v)) = v(v*u)\,,$$

und es folgt für $u = w*w = v$ die Gleichung:

$$\text{(4.23)} \qquad a*a = w*w = e\,.$$

Setzen wir nun in (4.22) $u = v$, so erhalten wir

$$\text{(4.24)} \qquad eu = u\,,$$

woraus mit $a = b = c = e$ in (BK) die Gleichung

$$\text{(4.25)} \qquad u(u*v) = v(v*u)$$

und mit $u = v = e$ in (BK) die Gleichung

$$\text{(4.26)} \qquad ab*c = b*(a*c)$$

resultiert. Setzen wir schließlich in (BK) $a = b = e$ und $u = v$, so ergibt sich hieraus die Kommutativität. □

Durch eine leichte Abänderung des Systems (A1), (BK) – nämlich bei Ersetzung von $ab*c$ durch $ab*c^2$ – erhält man ein Axiomensystem für den *brouwerschen Halbverband.* Ein System für den *abelschen Verbandsgruppenkegel* liefert (B2) zusammen mit der Forderung $a * ba = b$. Auf einen Beweis sei hier verzichtet, zumal wir auf den abelschen Verbandsgruppenkegel und andere Strukturen mit Kürzungsregel am Ende diese Kapitels noch zurückkommen werden.

4.2 Zur komplementären Halbgruppe

In Anlehnung an McKenzie [122] werden wir im folgenden zeigen:

4. 2. 1 Proposition. *Jede Klasse $\mathfrak{A}$ komplementärer Halbgruppen, die sich mit endlich vielen Gleichungen beschreiben lässt, ist einbasig.*

Zunächst gilt offenbar:

4. 2. 2 Lemma. *Sind f und g zwei Funktionen auf M und ist $f \circ g \circ f$ eine Permutation, so sind auch f und g Permutationen.*

Das liefert weiter fast unmittelbar

4. 2. 3 Lemma. *Seien $f_1, \ldots, f_m$ Funktionen auf der Menge M mit*

$$f_1 \circ f_2 \circ \ldots \circ f_{m-1} \circ f_m \circ f_{m-1} \circ \ldots \circ f_2 \circ f_1(a) = a\,. \tag{4.27}$$

Dann sind alle f_i $(1 \leq i \leq n)$ Permutationen, und es resultiert:

$$f_n \circ f_{n+1} \circ \ldots \circ f_m \circ \ldots \circ f_{n+1} \circ f_n \circ f_{n-1} \circ \ldots \circ f_1 \circ f_1 \circ \ldots \circ f_{n-1}(a) = a$$

$$f_{n-1} \circ \ldots \circ f_1 \circ f_1 \circ \ldots \circ f_{n-1} \ \circ \ f_n \ \circ \ f_{n+1} \circ \ldots \circ f_m \circ \ldots \circ f_{n+1} \circ f_n(a) \ = \ a\,.$$

DENN: Man beachte $fg = id \Longrightarrow gf = id\,.$ □

Insbesondere haben wir damit:

$$f_\nu(b) = f_\nu(c) \implies b = c\,. \tag{4.28}$$

Als nächstes kürzen wir ab:

$$\begin{aligned} a \vee b \ &:= \ a(a * b)\,, \\ a \wedge b \ &:= \ (b : (a * b))((b : (a * b)) * (a : (b * a))) \end{aligned}$$

und bilden hiernach die Polynome:

$$
\begin{aligned}
p_1 &= (x_1 \wedge x) \vee (x \wedge x)\,, \\
p_2 &= ((x \vee x) \wedge x_2) \vee (x \wedge x)\,, \\
p_3 &= ((x \vee x) \wedge (x \vee x)) \vee (x_3 \wedge x)\,, \\
p_4 &= ((x \vee x) \wedge (x \vee x)) \vee ((x \vee x) \wedge x_4)\,, \\
p_5 &= (x_5 \vee x) \wedge (x \vee x)\,, \\
p_6 &= ((x \wedge x) \vee x_6) \wedge (x \vee x)\,, \\
p_7 &= ((x \wedge x) \vee (x \wedge x)) \wedge (x_7 \vee x)\,, \\
p_8 &= ((x \wedge x) \vee (x \wedge x)) \wedge ((x \wedge x) \vee x_8)\,. \\
p_9 &= ((x_9 \wedge x) \vee (x \wedge y_9)) \vee x\,, \\
p_{10} &= x(x_{10} * x_{10})\,, \\
p_{11} &= (x_{11} * x_{11})x\,, \\
p_{12} &= (x((x_{12}y_{12} * z_{12}) * (y_{12} * (x_{12} * z_{12})))) \\
&\quad \cdot ((v_{12} * (u_{12} * w_{12})) * (u_{12}v_{12} * w_{12}))\,, \\
p_{13} &= xf(w_{13,1} \ldots w_{13,m} \text{ mit } f \text{ gleich } p \text{ aus (B2')}\,.
\end{aligned}
$$

Es ist klar, dass die angeführten Polynome alle als Polynome in den Operationen $*, :$ und $\cdot$ und den Variablen

$$x\,,\, x_1\,,\, \ldots\,,\, x_{12}\,,\, y_{12}\,,\, z_{12}\,,\, u_{12}\,,\, v_{12}\,,\, w_{13,1}\ \ldots\,,\, w_{13,m}$$

aufgefasst werden können und dass p_1 bis p_{13} übergehen in Funktionen f_1 bis f_{13}, wenn man in p_ν jeweils $x_1\,, \ldots\ldots, w_{13,m}$ mit Konstanten $u_\nu\,, \ldots$ $\ldots\,, w_{m\nu}$ belegt. Geht man nun weiter hin und belegt p_ν einmal mit $\overline{u}_\nu\,, \ldots$ $\ldots, \overline{w}_{m\nu}$ zu $\overline{f}\nu$ und ein anderes Mal mit $\overline{\overline{u}}_\nu\,, \ldots\ldots, \overline{\overline{w}}_{m\nu}$ zu $\overline{\overline{f}}_\nu$, so erhält man durch Vor- und Einschachteln aus

$$
\begin{aligned}
& f_1 \circ \ldots \circ \overline{f}_\nu \circ \ldots \circ f_{13} \circ \ldots \circ f_\nu \circ \ldots \circ f_1(a) \\
& = \quad a \quad = \\
& f_1 \circ \ldots \circ \overline{\overline{f}}_\nu \circ \ldots \circ f_{13} \circ \ldots \circ f_\nu \circ \ldots \circ f_1(a)
\end{aligned}
$$

die Gleichung

$$\overline{f}_\nu(a) = \overline{\overline{f}}_\nu(a)\,. \tag{4.29}$$

Dies ist der Schlüssel zum Beweis. Denn die Forderung

$$\overline{f}_1 \circ \ldots \circ \overline{f}_{12} \circ f_{13} \circ \overline{\overline{f}}_{12} \circ \ldots \circ \overline{\overline{f}}_1(a) = a \tag{A}$$

ist offenbar notwendig. Sie reicht aber auch hin:
DENN: Da (A) die Unabhängigkeit der Polynomwerte von den indizierten Variablen impliziert, gilt zunächst

$$f_1(a) = f_2(a) = f_3(a) = f_4(a) = f_1(a \vee a) \quad , \tag{4.31}$$

also nach 4.2.3

$$a \vee a \;=\; a\,. \tag{4.32}$$

Analog erhalten wir

$$a \wedge a \;=\; a \tag{4.33}$$

und damit

$$f_1(a) = \ldots\ldots\ldots\ldots\ldots = f_9(a) = a\,. \tag{4.34}$$

Aufgrund dieses letzten Sachverhalts gewinnen wir:

$$\begin{array}{rcl}
(a \vee b) \vee (b \vee a) & = & ((a \wedge (b \vee a)) \vee ((b \wedge a) \wedge b)) \\
& \vee & (b \vee a) \\
& = & b \vee a \\
& \Longrightarrow & \\
a \vee b & = & (a \vee b) \wedge ((a \vee b) \vee (b \vee a)) \\
& = & b \vee a\,.
\end{array}$$

Diese Kommutativität (bezüglich $\vee$) sichert uns als nächstes die Gleichung

$$a(a * b) \;=\; b(b * a)\,. \tag{A1}$$

Weiter gilt wegen $\overline{f}_{10}(a) = \overline{\overline{f}}_{10}(a)$ die Gleichung $a(b * b) = a(a * a)$, also

$$a(b * b) \;=\; a\,. \tag{A3}$$

Damit folgt aber wegen $\overline{f}_{10}(a) = \overline{\overline{f}}_{10}(a)$ und $\overline{f}_{11}(a) = \overline{\overline{f}}_{11}(a)$

$$a * a = (a * a)(b * b) \;=\; (b * b)(b * b) = b * b\,, \tag{4.37}$$

so dass mit $a * a = b * b := e$ die Gleichung

$$e \cdot e = \quad e \quad = e * e \tag{4.38}$$

erfüllt ist und damit:

$$\begin{array}{rcl} a & = & a((xy * z) * (y * (x * z))) \\ & \& & \\ a & = & a((y * (x * z)) * (xy * z)) \,. \end{array}$$

DENN: Wählen wir in $f_{12}(a)$ zunächst $u_{12} = v_{12} = w_{12} = x_{12} = y_{12} = z_{12} = e$, so erhalten wir a. Wählen wir weiter $u_{12} = v_{12} = w_{12} = e$ und $x_{12} = x$, $y_{12} = y$ sowie $z_{12} = z$, so erhalten wir die erste Zeile. Und setzen wir schließlich $x_{12} = y_{12} = z_{12} = e$ und $u_{12} = x$, $v_{12} = y$ sowie $z_{12} = z$, so erhalten wir die zweite Zeile.
Damit folgt für $f = xy * z$ und $g = y * (x * z)$ die Gleichung

$$f = f(f * g) \;\; = \;\; g(g * f) = g \,. \tag{4.39}$$

Dies sichert das Axiom

$$ab * c \;\; = \;\; b * (a * c) \tag{A3}$$

Hieraus ergibt sich $(b * b)a = a$ und damit $f_{10}(a) = a$, so dass unsere Ausgangsgleichung zusammen schrumpft zu

$$f_{13}(a) \;\; = \;\; a \,. \tag{4.41}$$

Damit ist alles gezeigt. □

Aus Satz 4.2.1 ergeben sich mehrere Korollare. Unter ihnen als das wesentlichste, das alle übrigen umfasst:

4. 2. 4 Korollar. *Sei $\mathfrak{A}$ eine Klasse von Algebren, die sich mit endlich vielen Gleichungen beschreiben lässt. Lassen sich dann bezüglich zweier aus den definierenden Operationen ableitbarer Operationen die Axiome der komplementären Halbgruppe herleiten, so ist es möglich, die Klasse $\mathfrak{A}$ mit einer einzigen Gleichung zu charakterisieren.*

Der Beweis verläuft analog zu dem soeben geführten. Insbesondere gelten demnach:

4. 2. 5 Korollar. *Die kommutative komplementäre Halbgruppe besitzt eine Fundamentalgleichung.*

4. 2. 6 Korollar. *Der boolesche Ring und der Verbandsgruppenkegel besitzen jeweils eine Fundamentalgleichung.*

4. 2. 7 Korollar. *Der brouwersche* (*Halb-*) *Verband besitzt eine Fundamentalgleichung.*

4. 2. 8 Korollar. *Der* (*abelsche*) *Verbandsgruppenkegel besitzt eine Fundamentalgleichung.*

4. 2. 9 Korollar. *Die normale komplementäre Halbgruppe besitzt eine Fundamentalgleichung.*

Insbesondere ergibt sich aus Satz 4.1.2 noch der auf GRÄTZER zurückgehende Satz von B. H. NEUMANN [128]:

4. 2. 10 Korollar. *Gehört eine universelle Algebra A zu einer Klasse $\mathfrak{A}$, die sich mit endlich vielen Gleichungen beschreiben lässt, so lässt sich A durch Hinzunahme zweier weiterer Operationen einengen zu einer Algebra, deren zugehörige Klasse sich mit einer einzigen Gleichung definieren lässt.*

DENN, man ordne A so an, dass ein minimales Element in A existiert. Dann bildet A einen brouwerschen Halbverband bezüglich der gewählten Anordnung.
Schließlich können wir Satz 4.2.1 verschärfen zu

4. 2. 11 Proposition. *Eine Klasse rechtskomplementärer Halbgruppen lässt sich immer dann mittels einer Fundamentalgleichung beschreiben, wenn sich eine Operation $\wedge$ angeben lässt, bezüglich der die Polynome p_1 bis p_8 den Wert a annehmen.*

Aufgrund von Satz 4.1.2 ist die Existenz von Fundamentalgleichungen nachgewiesen, nichts ist hingegen gesagt über ihre *Länge.* Dass es sehr viel kürzere Gleichungen in weniger Variablen als die von uns konstruierten geben dürfte, scheint evident. So liefert beispielsweise

(BR) $$((x+y)+z)+((x+z)+h(t,u,v,w)) = y$$

mit

$$h = ((tt + t(u(vw) + w(uv))) + t) + (u(v+w) + (uv + wu))$$

eine *Kurzform* für die boolesche Algebra, was hier nicht ausgeführt werden soll, doch werden wir später auf Sonderfälle zurückkommen, siehe 3.6.7 und 3.6.4.

4.3 Eine „Muttergleichung“

Im folgenden präsentieren wir eine „common structured fundamental equation“ für idempotente Ringe und Verbandsgruppenkegel, die zudem auch noch greift im Falle eines Verbandsloopkegels, der Verbandsgruppe, der Verbandsloop, ja sogar der abelschen Gruppe.

Wir weisen vorweg hin auf an die Charakterisierung des booleschen Ringes unter 3.6.7 und des Verbandsgruppenkegels unter 3.6.4.

Grundgedanke ist dann: Definieren wir

$$a \,\Delta\, b := \begin{cases} (a * b)(b * a) & \text{im booleschen Fall} \\ a : b & \text{im Kegelfall} \end{cases}$$

und

$$a \circ b := \begin{cases} (a * b)(b * a) & \text{im booleschen Fall} \\ ab & \text{im Kegelfall ,} \end{cases}$$

so können wir sowohl den idempotenten Ring als auch den Verbandsgruppenkegel betrachten als Algebra $(S, \cdot, *, \,\Delta\,, \circ)$ vom Typ $(2, 2, 2, 2)$. Damit kommt die Frage nach einer gemeinsamen Grundlegung dieser beiden Strukturen auf. Insbesondere stellt sich die Frage nach einer Fundamentalgleichung von gemeinsamer Struktur.

Es ist wohlbekannt nach [19] und [130], dass es Fundamentalgleichungen gibt, doch sind die bekannten Gleichungen von „astronomischer“ Länge. Dies zu überwinden ist unser nächstes Ziel.

Dabei werden wir zu einem zufrieden stellendem Ansatz gelangen, der über den hier betrachteten Fall auch von allgemein algebraischer Bedeutung sein dürfte. Wir beginnen mit einer Serie von Gleichungen, die in den betrachteten Algebren gemeinsam gelten.

$$(a * a) \circ a = a \tag{4.43}$$
$$(b \circ (b * a))\, \Delta\, (a * b) = a \tag{4.44}$$
$$(a \circ b)\, \Delta\, b = a \tag{4.45}$$
$$a \circ (a * b) = (b\, \Delta\, a)a \tag{4.46}$$
$$a \circ (b \circ c) = (a \circ b) \circ c \tag{4.47}$$
$$(b^2\, \Delta\, b) * (b^2\, \Delta\, b)a = a\,. \tag{4.48}$$

Diese Gleichungen sind leicht zu verifizieren im Kegelfall.
Wir betrachten den Fall des idempotenten Ringes. Hier gilt $a^2 = a$ und damit unter Berücksichtigung von $(a*b)*b = (b*a)*a$ die Gleichungskette:

$$\begin{aligned}
(a * b) * a &= ((a * b) * (a * a)) * ((a * b) * a)\\
&= (a * ((a * b) * a)) * ((a * b) * a)\\
&= ((((a * b) * a) * a) * a)\\
&= ((a * (a * b)) * (a * b)) * a\\
&= ((a^2 * b) * (a * b)) * a\\
&= a\,,
\end{aligned}$$

also insgesamt $a * (a * b) = a * b$ und $(a * b) * a = a$. Hiernach verifiziert der Leser die notierten Gleichungen (4.43) bis (4.48) ohne Probleme.
Schließlich erwähnen wir

$$\text{Es gibt eine } 0 \text{ mit } 0^2 = 0 \text{ und } 0 * ((a * a^2) * a) = 1\,, \tag{4.49}$$

man wähle im Kegelfall etwa die 1 als 0.
Wir starten nun von einer Algebra $(S\,,\,\cdot\,,\,*\,,\,\Delta\,,\,\circ)$ des Typs (2, 2, 2, 2), die den Gleichungen (4.43) bis (4.48) genügen möge – tatsächlich genügt weniger – und zwei disjunkten Mengen von Variablen $\{x_0, \ldots, x_n\}$, $\{y_0, \ldots, y_n\}$. Weiterhin sei f eine *algebraische Funktion* in n *Variablen* über S. Wir bezeichnen dann mit f_x den Term $f(x_1, \ldots, x_n)$ und mit f_y den Term $f(y_1, \ldots, y_n)$. Schließlich erfülle f in beiden Klassen die Bedingung $f \circ a = a = a \circ f$.
Dann gilt, wenn $\circ$ stärker binden soll als $*$ und $*$ stärker als Δ :

$$f_x \circ \Big\{\Big(\big(f_y \circ (a \circ (a * b)\, \Delta\, (b * a))\big) \circ c\Big)\, \Delta\, c\Big\} = b\,. \tag{F}$$

wo Δ beispielsweise agieren mag als $(a * b)(b * a)$ in dem einen Fall und als : in dem anderen Fall.

Ist auf der anderen Seite (F) erfüllt, so lässt sich zeigen, dass $\circ$ rechtskürzbar, $*$ *identitiv* und f konstant ist. Darüber hinaus lässt sich aus diesen Regeln ein zweites Kürzungsgesetz herleiten, nämlich

$$1 \circ (1 * a) = 1 \circ (1 * b) \Longrightarrow a = b\,.$$

Der Rest „degeneriert“ dann zur Routine.

4. 3. 1 Lemma. *Gilt die Gleichung* (F), *so erhalten wir*

$$f_x \circ \Big\{\Big(\big(f_y \circ (u \circ c\,\Delta\, c)\big) \circ w\Big)\,\Delta\, w\Big\} = u\,.$$

DENN: In der Tat, setze $a = b = f_x \circ \big(v \circ (v * u)\,\Delta\,(u * v)\big)$. Dann folgt

$$\text{(F 1)} \qquad f_x \circ \big((u \circ c)\,\Delta\, c\big) = f_x \circ \big(v \circ (v * u)\,\Delta\,(u * v)\big)$$

und hieraus resultiert

$$\text{(F 2)} \qquad f_y \circ \Big\{\Big(\big(f_x \circ (u \circ c\,\Delta\, c)\big) \circ w\Big)\,\Delta\, w\Big\} = u\,.$$

□

Damit haben wir insbesondere:

$$a \circ c = b \circ c \overset{(F2)}{\Longrightarrow} a = b\,. \tag{4.53}$$

$$a * b = b * a \overset{(F2,F1)}{\Longrightarrow} a = b\,. \tag{4.54}$$

Sei f nun von der Form $(\ldots(g_1 \circ g_2) \circ \ldots \circ g_m)$ und seien die Variablen von g_ν und g_μ verschieden für alle Paare $\nu \neq \mu$ sowie

$$g_1 \;=\; x_0 * (x_1 * x_1)\,.$$

Dann ist g_1, wie sich durch Kürzung nach (4.53) erweist, konstant, also $(a * a) * (b * b) = (b * b) * (a * a)$, woraus

$$a * a = b * b =: 1$$

resultiert, und hieraus folgt unmittelbar

$$x_0 * (x_1 * x_1) = 1 * (1 * 1) = 1 * 1 = 1 \rightsquigarrow a * 1 = 1\,.$$

Damit erhalten wir für $a = 1$ in (F) die angekündigte zweite Kürzungsregel:

$$1 \circ (1 * u) = 1 \circ (1 * v) \;\Longrightarrow\; u = v\,. \tag{4.55}$$

Wir definieren nun weiter:

$$\begin{aligned} g_2 &:= x_2 * ((x_2 * x_2) \circ (x_2 * x_2)) \\ g_3 &:= x_3 * ((x_3 * x_3) \cdot (x_3 * x_3)) \\ g_4 &:= x_4 * ((x_4 * x_4) \,\Delta\, (x_4 * x_4)) \,. \end{aligned}$$

Da $g_1 \circ g_2$ konstant ist, erhalten wir hiermit

$$\begin{aligned} g_1 \circ g_2 &= 1 \circ (x_2 * (1 \circ 1)) &&= 1 \circ (1 * (1 \circ 1)) \\ &= 1 \circ ((1 \circ 1) * (1 \circ 1)) &&= 1 \circ (1 * 1)\,, \end{aligned}$$

also $1 \circ (1 * (1 \circ 1)) = 1 \circ (1 * 1)$ und folglich nach (4.55)

$$1 \circ 1 = 1$$

und damit

$$g_1 \circ g_2 = 1 \circ 1 = 1\,.$$

Fahren wir in dieser Weise fort, so resultiert nach ähnlichem Muster

$$1 * 1 = 1 \text{ und } 1 \cdot 1 = 1 \text{ und } 1 \,\Delta\, 1 = 1\,.$$

Sei nun $g_\nu, g_{\nu+1}$ vom Typ

$$\begin{aligned} g_\nu &:= x_\nu * (p\,(y_1, \ldots, y_r) * q\,(y_1, \ldots, y_r)) \\ g_{\nu+1} &:= x_{\nu+1} * (q\,(z_1, \ldots, z_r) * p\,(z_1, \ldots, z_r)) \end{aligned}$$

und außerdem $\qquad (\ldots (g_1 \circ g_2) \circ \ldots g_{\nu-1}) = 1\,.$

Dann erhalten wir nach der soeben vorgestellten Methode

$$\begin{aligned} 1 &= p\,(z_1, \ldots, z_r) * q\,(z_1, \ldots, z_r) \\ 1 &= q\,(z_1, \ldots, z_r) * p\,(z_1, \ldots, z_r) \end{aligned}$$

und folglich $\qquad p\,(z_1, \ldots, z_r) = q\,(z_1, \ldots, z_r)\,.$

Das liefert aber

(K1) $$a \cdot (a * b) = b \cdot (b * a)$$

mittels $\qquad g_5 := x_5 * ((z_5 \cdot (z_5 * z_{51})) * (z_{51} \cdot (z_{51} * z_5)))\,,$

da wir z_5 and z_{51} vertauschen dürfen,

(K2) $$ab * c = b * (a * c)$$

mittels

$$\begin{aligned} g_6 &:= x_6 * ((z_6 z_{61} * z_{62}) * (z_{61} * (z_6 * z_{62}))) \\ g_7 &:= x_7 * ((z_{71} * ((z_7 * z_{72})) * (z_7 z_{71} * z_{72}))) \end{aligned}$$

und schließlich

$$\text{(K3)} \qquad a(b * b) \ = \ a$$

vermöge

$$\text{(4.59)} \qquad g_8 \ := \ x_8 * x_8(z_{81} * z_{81}),$$

da diese Definition zu

$$a * a(b * b) \ = \ 1$$

führt und (K2) dann weiter zu

$$a(b * b) * a \ = \ (b * b) * (a * a) = 1 .$$

Sicher zu stellen bleiben hiernach noch über den vorgegebenen Mechanismus die Gleichungen:

$$\begin{aligned} a \circ (b \circ c) &= (a \circ b) \circ c \\ a \circ (a * b) &= (b \,\Delta\, a)a \\ (b^2 \,\Delta\, b) * (b^2 \,\Delta\, b)a &= a \\ (a \circ b) \,\Delta\, b &= a . \end{aligned}$$

Schließlich haben wir eine Konstante 0 im Sinne von (11) einzufügen, wenn wir den booleschen Ring erfassen wollen. Damit ist gezeigt:

4. 3. 2 Theorem. *Sei* $(S\,,\,\cdot\,,\,*\,,\,\Delta\,,\,\circ)$ *eine Algebra, in der die Gleichung* (F) *erfüllt ist mit* f_x *im obigen Sinne.*
Dann ist $(S\,,\,\cdot\,,\,*\,,\,\Delta\,,\,\circ)$ *ein Verbandsgruppenkegel, wenn auf dem Wege über* f_x $a \,\Delta\, b = a : b$ *gesichert ist.*
Und es ist $(S, \cdot, *, \,\Delta\,, \circ)$ *ein idempotenter Ring, wenn auf dem Wege über* f_x *die Gleichung* $a \,\Delta\, b = a \circ b = (a * b)(b * a)$ *gewährleistet ist.*

Natürlich lässt sich (F) im Sonderfall vereinfachen. Diesem Aspekt gilt der nächste Abschnitt.

4.4 Der boolesche Sonderfall

Wir erinnern zunächst an 3.6.7, d. h. daran, dass sich eine Algebra $\mathfrak{S} = (\mathfrak{S}, \cdot, *)$ genau dann auffassen als ein idempotenter Ring auffassen lässt, wenn sie mit $a + b := (a * b)(b * a)$ den Bedingungen genügt:

$$\text{(A1)} \qquad a(a*b) = b(b*a) \qquad \text{(B1)}$$

$$\text{(A2)} \qquad ab*c = b*(a*c) \qquad \text{(B2)}$$

$$\text{(A3)} \qquad a(b*b) = a \qquad \text{(B3)}$$

$$\text{(BR')} \qquad a+(b+c) = (a+b)+c \qquad \text{(B10)}$$

Dies im Blick, zeigen wir:

4. 4. 1 Proposition. *Eine Algebra $\mathfrak{B} = (B, \circ, *)$ ist eine boolesche Algebra gdw. sie für ein geeignetes, von a, b, c, freies f_u der Gleichung genügt:*

$$\text{(B)} \qquad ((a \circ b) \circ c) \circ ((a \circ c) \circ f_u) = b\,.$$

BEWEIS. Zunächst erhalten wir die Kürzungsregel

$$(4.65) \qquad x \circ y = x \circ z \implies y = z\,.$$

Wir setzen nun $a = x \circ y, b = z, c = (x \circ y) \circ f_u$. Dann folgt weiter:

$$\begin{aligned} z &= \Big(((x \circ y) \circ z) \circ ((x \circ y) \circ f_u)\Big) \circ \Big(((x \circ y) \circ ((x \circ y) \circ f_u))) \circ f_u\Big) \\ &= y \circ \Big(((x \circ y) \circ ((x \circ y) \circ f_u)) \circ f_u\Big) \\ &\leadsto \end{aligned}$$

$$(4.66) \qquad y \,\Big|_{\ell}\, z \quad \text{setze} \quad z = y \cdot y_z.$$

Hiernach können wir den Beweis wie folgt abschließen:
Zunächst ist y_z nach (4.65) eindeutig bestimmt, also konstant. Folglich können wir etwa von x_x sprechen, und es resultiert

$$(4.67) \qquad a_a = b_b$$

aus $\quad a_a = ((a \circ a_a) \circ b) \circ ((a \circ b) \circ f_u) = (a \circ b) \circ ((a \circ b) \circ f_u)$

Wir bezeichnen nun $a_a = b_b$ als 1. Dann folgt $1 \circ 1 = 1$ und damit weiter vermöge (4.65) und (4.67):

$$1 \circ (1 \circ f_u) = 1 \Longrightarrow 1 \circ f_u = 1 \Longrightarrow f_u = 1 \tag{4.68}$$

sowie vermöge (4.68) und (4.69):

$$((a \circ b) \circ c) \circ (a \circ c) = b \tag{4.69}$$

$$a \circ a = (a \circ 1) \circ (a \circ 1) = 1 \tag{4.70}$$

$$1 \circ a = ((a \circ a) \circ a) \circ (a \circ a) = a \tag{4.71}$$

$$(a \circ b) \circ c = (((a \circ b) \circ c) \circ (a \circ c)) \circ (a \circ c) = b \circ (a \circ c) \tag{BR'}$$

Weiter erhalten wir hiernach

$$a \circ b = (a \circ b) \circ 1 = b \circ (a \circ 1) = b \circ a\,, \tag{4.73}$$

beachte (BR'), und schließlich

$$a \circ b = 1 \Longleftrightarrow a = b\,. \tag{4.74}$$

Hier stoppen wir die Entwicklung und überlassen dem Leser den Abschluss auf der Grundlage von Proposition 3.6.7 □

Wir gehen hier nicht ein auf die Erfassung des booleschen Verbandes, auch sie darf natürlich dem Leser überlassen bleiben.

4.5 Der Kegel-Sonderfall

Wir erinnern auch hier zunächst an ein früheres Theorem, nämlich an 3.6.4. Es besagte, dass eine Algebra $\mathfrak{S} = (\mathfrak{S}, \cdot, *, :)$ eine kürzbare komplementäre Halbgruppe genau dann ist, wenn sie den Bedingungen genügt:

$$\begin{array}{lrcl}
\text{(A1)} & a(a * b) & = & b(b * a) \\
\text{(A2)} & ab * c & = & b * (a * c) \\
\text{(V1)} & a * ab & = & b \\
\text{(V2)} & a(a * b) & = & (b : a)a \\
\text{(A5)} & ba : a & = & a * ab
\end{array}$$

4. 5. 1 Proposition. (F) *ist Fundamentalgleichung des Kegels, wenn wir* $\circ$ *als* $\cdot$ *auffassen und* Δ *als* : *sowie*

$$f_x := (\ldots(g_1 \circ g_2) \circ \ldots \circ g_7)$$

setzen mit

$$\begin{aligned}
g_1 &:= x_1 * (x_0 * x_0)\\
g_2 &:= x_2 * ((x_{21}x_{22} * x_{23}) * (x_{22} * (x_{21} * x_{23})))\\
g_3 &:= x_3 * ((x_{32} * (x_{31} * x_{33})) * (x_{31} * x_{32} * x_{33}))\\
g_4 &:= x_4 * (x_{41}(x_{41} * x_{42}) * x_{42}(x_{42} * x_{41}))\\
g_5 &:= x_5 * ((x_{51} * x_{51}x_{52}) * x_{52})\\
g_6 &:= x_6 * ((x_{61} : x_{62})x_{62} * x_{62}(x_{62} * x_{61}))\\
g_7 &:= x_7 * (x_{71}(x_{71} * x_{72}) * (x_{71} : x_{72})x_{72}) .
\end{aligned}$$

BEWEIS. Mittels g_1 erhalten wir zunächst die beiden Gleichungen:

$$a * a = b * b = 1 \tag{4.80}$$

$$a * 1 = 1 . \tag{4.81}$$

Weiter folgt mittels g_1, g_2

$$ab * c = b * (a * c) . \tag{A3}$$

Als nächstes liefert g_4

$$a(a * b) = b(b * a) , \tag{A2}$$

und es folgt $(a * ab) * b = 1$ vermöge g_5 – und $b * (a * ab) = ab * ab = 1$ vermöge (4.81). Das liefert weiter:

$$a * ab = b \tag{V1}$$

Damit haben wir auch $a1 = a = 1a$, man konsultiere den Abschnitt zur Axiomatik, und wir erhalten$(a : b)b * a(a * b) = 1$ – durch Fortfahren. Leichte Probleme bekommen wir lediglich mit g_7. Hier belegen wir x_7 mit $1 : 1$ und alle anderen Variablen mit 1. Dies führt zu

$$(b(b * a) : (a * b)) : 1 = a \Longrightarrow (a : 1) : 1 = a \Longrightarrow (1 : 1) : 1 = 1 ,$$

und bei Belegung aller Variablen aus g_1 bis g_7 mit 1 resultiert

$$\begin{aligned}
& 1 \cdot (1 * (x_{71} * x_{72}) * (x_{71} : x_{72}))\\
= {} & 1 \cdot (1 * (1(1 * (1 : 1)) * ((1 : 1) : 1)1)\\
= {} & 1(1 * 1)\\
\leadsto {} & \\
g_7 = {} & x_{71}(x_{71} * x_{72}) * (x_{72} : x_{71})x_{71} = 1 .
\end{aligned}$$

Dies impliziert dann weiter

$$\text{(V2)} \qquad a(a*b) \;=\; (a:b)b\,,$$

und damit $a:1=(a:1)1=a(a*1)=a$. Folglich können wir den Beweis abschließen, indem wir in (F2) alle von u und c verschiedenen Variablen mit 1 belegen, denn dies liefert $uc:c=u$ und damit das Axiom

$$\text{(A5)} \qquad ab:b \;=\; a$$

Damit sind wir am Ziel. □

Wir wenden uns nun dem abelschen Fall zu – der Vollständigkeit halber. Wir erinnern zunächst an 3.2.4, also den Satz, dass ein Gruppoid $\mathfrak{G}$ eine abelsche kürzbare komplementäre Halbgruppe ist gdw. es bezüglich einer weiteren Operation $*$ den Axiomen genügt:

$$\text{(A1)} \qquad a(a*b) \;=\; b(b*a)$$

$$\text{(A2)} \qquad ab*c \;=\; b*(a*c)$$

$$\text{(VA)} \qquad a*ba \;=\; b$$

Auf dieser Grundlage werden wir beweisen:

4. 5. 2 Proposition. (F) *wird zur Fundamentalgleichung des abelschen Verbandsgruppenkegels, wenn wir einerseits die Operationen $a\circ b$ und ab identifizieren sowie andererseits die Operationen $a\Delta b$ und $b{*}a$ und hiernach definieren:*

$$\begin{aligned} f_x \;&:=\; f(x_1,\ldots,x_6) \\ &:=\; (x_1x_2{*}x_2x_1)(((x_3{*}x_4){*}(x_3{*}x_5)){*}((x_4{*}x_3){*}(x_4{*}x_5))) \end{aligned}$$

BEWEIS. Es ist also zu zeigen, dass (A1), (A2), (AV) aus

$$\text{(FA)} \qquad f_x\cdot\Big\{c*(f_y\cdot((a*b)*(b\cdot(b*a)))\cdot c\Big\}=a$$

folgen. Wieder erhalten wir

$$ac=bc\Longrightarrow a=b$$

und $a*b=b*a\Longrightarrow a=b$ und – da $x_1x_2*x_2x_1=x_2x_1*x_1x_2$ wegen der Kürzungsregel konstant ist

$$\text{(4.91)} \qquad ab \;=\; ba\,.$$

Als nächstes folgt wegen der Kommutativität

$$(a * b) * (a * c) \;=\; (b * a) * (b * c)\,, \tag{4.92}$$

da $((x_3 * x_4) * (x_3 * x_5)) * ((x_4 * x_3) * (x_4 * x_5))$ konstant ist, man beachte die Symmetrie in x_3, x_4.
Wir schreiben nun a in der Form $f_x(c * (f_y((a * b) * b(b * a)))c) = f_x \cdot g_a$ und b als $f_x \cdot g_b$. Dann folgt aus der Kommutativität

$$a * a \;=\; b * b =: 1\,. \tag{4.93}$$

Dies führt zu $f_x = 1 \cdot 1 =: e$. Hiernach zeigen wir

$$a * 1 \;=\; 1\,. \tag{4.94}$$

Dazu beachten wir in einem ersten Schritt, dass aus (F) und (V1) die Herleitung liefern:

$$\begin{aligned} & ea &=&\; e\big\{e * (e(ea * b) * b(b * ea)))e\big\} \\ \rightsquigarrow\quad & a &=&\; e * (e((ea * b) * b(b * ea)))e \\ & &=:&\; e * d\,, \end{aligned} \tag{4.95}$$

woraus – wie gewünscht – resultiert:

$$a * 1 = (e * d) * (e * e) \;=\; (d * e) * (d * e) = 1\,.$$

Wir setzen nun in (FA) $a = b = e((r * s) * s(s * r))$. Dann folgt

$$e(c * rc) \;=\; e((r * s) * s(s * r))\,,$$

also nach Kürzung

$$c * rc \;=\; (r * s) * s(s * r) \tag{4.96}$$

Anwendung von (4.96) auf (FA) führt als nächstes zu

$$1 * a1 = 1 * b1 \Longrightarrow a = b\,, \tag{4.97}$$

was wegen

$$\begin{aligned} 1 * a1 &= (a * 1) * 1(1 * a) \\ &= 1 * 1(1 * a) = 1 * (1 * a)1 \end{aligned} \tag{4.98}$$

die Gleichung

$$1 * a \;=\; a\,. \tag{4.99}$$

impliziert. Im weiteren bezeichnen wir mit u das eindeutig existierende Element x mit $ex = e$. Dann erhalten wir sofort mittels (4.99) und (4.96)

$$1u = 1 * 1u \;=\; e * eu = e * e = 1$$

und hiermit unter Berücksichtigung von (4.96) zunächst

$$e \;=\; 1 \cdot 1 = 1\,, \tag{4.100}$$

wegen $\quad 1 \cdot 1 = 1 * 1 \cdot 1 \;=\; u * 1u = u * 1 = 1$

und weiter erneut wegen (4.99)

$$a * 1a \;=\; 1\,, \tag{4.101}$$

wegen

$$a * 1a = (1 * 1) * 1(1 * 1) \;=\; 1 * 1 \cdot 1 = 1 * 1 = 1\,.$$

Als nächstes erhalten wir mittels (4.101) die Gleichung

$$a \cdot 1 \;=\; a\,. \tag{4.102}$$

Hierzu genügt es wegen $a * a1 = 1$ zu zeigen, dass $a1 * a = 1$ erfüllt ist. Dazu zeigen wir vorab mittels (4.98) und (4.99)

$$\begin{aligned} 1a = 1 * a1 \;&=\; (a * 1a) * (1a)(1a * a) \\ &=\; 1 * (1a)(1a * a) \\ &=\; (1a)(1a * a)\,. \end{aligned} \tag{4.103}$$

Nun sind wir in der Lage $a1 * a = 1$ herzuleiten, vermöge:

$$\begin{array}{rcl} 1a * 1a & = & 1b * 1b \\ & \overset{(4.103)}{\rightsquigarrow} & \\ 1a * (1a * a)(1a) & = & 1b * (1b * b)(1b) \\ & \overset{(4.96)}{\rightsquigarrow} & \\ 1 * (1a * a)1 & = & 1 * (1b * b)1 \\ & \overset{(4.92,4.99)}{\rightsquigarrow} & \\ 1(1a * a) & = & 1(1b * b) \\ & \overset{(4.53)}{\rightsquigarrow} & \\ 1a * a & = & 1b * b \\ & \overset{(4.92)}{\rightsquigarrow} & \end{array}$$

$$\begin{array}{rcl} a \cdot 1 * a & = & 1 \cdot 1 * 1 \\ & \rightsquigarrow & \\ a1 * a & = & 1 \end{array}$$

Setzen wir nun in (FA) alle von $a$und c verschiedenen Variablen gleich 1, so erhalten wir

(VA) $$a * ba = b\,,$$

Weiter folgt

(4.105) $$(a * b) * b = (b * a) * a\,,$$

wegen

$$(a * b) * b = (a * b) * (a * ab) = (b * a) * (b * ab) = (b * a) * a\,.$$

Nun zeigen wir

(4.106) $$ab * a = 1\,.$$

Hierzu setzen wir vorab in (FA) alle von a, b verschiedenen Variablen gleich 1. Dies liefert zunächst:

(4.107) $$(a * b) * b(b * a) = a$$

und damit weiter

$$\begin{array}{rcl} (ab * a) * ab & \overset{(4.107)}{=} & (ab * a) * a(a * ab) = ab \\ & \rightsquigarrow & \\ ab * a & = & ((ab * a) * ab) * ((a * ab) * ab) \\ & = & ((ab * a) * ab) * ((ab * a) * a) \\ & = & (ab * (ab * a)) * (ab * a) \\ & = & ((ab * a) * ab) * ab \\ & = & ab * ab = 1\,, \end{array}$$

also die Gleichung (4.106).

Hiernach sind wir fast am Ziel, denn

(A2) $$ab * c = b * (a * c)$$

folgt aus

$$\begin{aligned} ab * c &= (ab * a) * (ab * c) \\ &= (a * ab) * (a * ac) \\ &= b * (a * c)\,, \end{aligned}$$

und es ergibt sich

(A3) $$a(a * b) = b(b * a)$$

via $$\begin{aligned} a(a * b) * b(b * a) &= (a * b) * (a * (b(b * a)) \\ &\overset{(4.92)}{=} (b * a) * (b * b(b * a)) \\ &= (b * a) * (b * a) = 1\,. \end{aligned}$$

□

4.6 Ausblick

Die hier angebotene „Mechanik“ ist weit relevanter, als es auf den ersten Blick scheinen mag. So lassen sich zum einen der *Verbandsloopkegel* – vergleiche das Kapitel über *Verbandsloops* – und zum anderen „ℓ-group“ und „ℓ-loop“ erfassen.
Interessant ist vor allem, dass mit der Varietät der abelschen Gruppen eine Varietät von unserem „Muster“ erfasst wird, die zwar *kongruenz-vertauschbar* und *kongruenz-modular,* nicht aber *kongruenz-distributiv* ist. Hierzu führen wir aus:
Sei $\mathfrak{G} := (G, \cdot, ^{-1})$ eine abelsche Gruppe. Wie setzen $a * b := ab^2$ und $a\Delta b := ab^{-1}$. Dann gilt $a(a * b) = b(b * a)$, also $a(a * b)\Delta(b * a) = b$ und $a * b = b * a \Longrightarrow a = b$, das letzte wegen $ab^2 = ba^2 \Longrightarrow a = b$.
Ein Problem bereitet allerdings der Umstand, dass aus $a * b = b * a$ hier nicht folgt $a * b = e = b * a$ mit $ae = a = ea$.
Es gelingt aber die Erfassung der Varietät *via* $aa^{-1} = bb^{-1} =: 1$ und $1c = c = c1$, was sich wie folgt ergibt:

Setze $$g_1 := uu^{-1}$$

$$g_2 := (vw)(wv)^{-1}$$

$$g_3 := ((rp)q)((pq)r)^{-1}$$

und hiernach $$f_x := \big(g_1 \circ g_2^{-1}\big) \circ g_3^{-1}.$$

Dann resultieren bei „Verfremdung“ von f_x und f_y nacheinander: $aa^{-1} = bb^{-1} =: 1$, insbesondere also auch $1 \cdot 1^{-1} = 1$, und es gilt wegen $ab^{-1} = 1 \Longrightarrow a = b$, beachte $ab^{-1} = bb^{-1} \Longrightarrow a = b$.
Weiter erhalten wir $g_2 = 1$, also $1 \cdot g_2^{-1} = g_2 \cdot g_2^{-1} \rightsquigarrow g_2 = 1$ und damit das Kommutativgesetz, und es ergibt sich analog das Assoziativgesetz vermöge g_3. Insbesondere haben wir zusätzlich – am Wege – $f_x = 1$ erhalten. Somit ist auch jedes u Teiler eines jeden b und demzufolge $\mathfrak{G}$ eine Gruppe.
Dem Leser wird ohne Schwierigkeiten klar, wie sich beliebige Gleichungsforderungen als $g_4, \ldots, g_n$ einbauen lassen, man beachte $1 \cdot 1 = 1 = 1^{-1}$.
Allerdings: die soeben hergeleitete Charakterisierung benutzt lediglich den Anteil $a * a \circ b = b$, weshalb unserer Herleitung vorrangig ein methodischer Wert zukommt.
Für eine kürzere Darstellung eignet sich $a * b = a^{-1}b$ eher, und auch im nicht kommutativen Fall gelangen wir zu einer 1-basigen Beschreibung, etwa vermöge:

$$\text{(G)} \qquad f \cdot \big((g_1 \cdot (g_2 \cdot g_3))\big) \ = \ b$$

mit

$$\begin{aligned} f &:= (a * ab) \\ g_1 &:= \big((xy)z)^{-1} \cdot x(yz)\big)^{-1} \\ g_2 &:= \big((u(v^{-1}v))^{-1} \cdot ((v^{-1}v)u)\big)^{-1} \\ g_3 &:= w^{-1}w \end{aligned}$$

DENN: Dann gilt sofort die Linkskürzungsregel und damit $w^{-1}w = e^{-1}e =: 1$ und $g^{-1} = h^{-1} \Longrightarrow g = h$. Wegen $g_2 \cdot 1 = 1$ haben wir weiter $(a1)^{-1} \cdot (1a) = 1$, also $a1 = 1a$. Fortsetzung des Verfahrens liefert dann $a(bc) = (ab)c$. Damit sind wir am Ziel wegen $1 = ww^{-1} = w^{-1}w$, da 1 jedes Element von rechts und damit auch von links teilt.
Die hier vorgestellte Gleichung (G) eignet sich vorzüglich für Übungen, doch sei betont, dass die Gleichungen von Tarski bzw. von Higman & Neumann die kürzest möglichen sind.
Und schließlich noch ein letzter wichtiger Hinweis: Wollen wir etwa die Quasigruppe erfassen, so gelingt mit McKenzie’s Methode eine Charakterisierung, wie sie eleganter nicht sein kann und glänzend geeignet ist als Übungsaufgabe – dank McKenzie. Denn hier ist ja bereits die Struktur mittels Absorptionsgleichungen beschrieben, man erinnere sich: Eine Quasigruppe ist definiert über drei Operationen $\circ, \backslash, /$ mittels der Gleichungen:

$$\text{(Q)} \qquad a \circ a\backslash b = b \ \ \& \ \ b/a \circ a = b$$

Insgesamt böte sich demnach eine vertiefte Studie des Zusammenhangs zwischen den Beiträgen von Tarski [151], Higman & Neumann [93], McKenzie [122], Padmanabhan & Quackenbush [130] sowie den hier vorgestellten Resultaten an.

Kapitel 5

Residuationsgruppoide

5.1 Redukte

Unter dem *Residuationsredukt,* auch kurz unter dem *Redukt* einer komplementären Halbgruppe $\mathfrak{S}$ verstehen wir die Menge S, betrachtet bezüglich der Residuation. Weiter verstehen wir unter einem *Clan* ein Residuationsgruppoid, das sich einbetten lässt in ein Redukt. Genauer: Unter einem *Kegel-Clan* werden wir ein Residuationsgruppoid $(C, *, :)$ verstehen, das sich ausdehnen lässt zu dem Redukt eines ℓ-Gruppenkegels und damit, wie wir sehen werden, eines *Bricks*, unter einem *brouwerschen Clan* ein Residuationsgruppoid $(B, *)$, das sich ausdehnen lässt zu dem Redukt eines brouwerschen Halbverbandes, und etwa unter einem *booleschen Clan* ein Residuationsgruppoid, das sich ausdehnen lässt zu dem Redukt eines booleschen Ringes und damit, wie wir sehen werden, eines booleschen Verbandes.
Ziel dieses Kapitels ist eine Klärung dieser Strukturen. Hierzu beginnen wir mit der Analyse des Clans der rechtskomplementären Halbgruppe. Dabei stoßen wir auf das verblüffende Ergebnis, dass diese Clans identisch sind mit den Clans der *links-kürzbaren rechts-komplementären* Halbgruppe. Genauer wird sich zeigen, dass $\mathfrak{R}$ genau dann ein solcher Clan ist, wenn gilt:

$$\text{(R0)} \qquad (a*a)*b = b$$

$$\text{(R1)} \qquad (a*b)*(a*c) = (b*a)*(b*c)$$

$$\text{(R2)} \qquad a*(b*b) = c*c$$

$$\text{(R3)} \qquad a*b = c*c = b*a \Longrightarrow a = b\,.$$

Da (R0), …,(R3) eine Ausdehnung zu einem Residuationsgruppoid einer rechts-komplementären Halbgruppe gewährleisten, nennen wir Gruppoide, die diesen Axiomen genügen, *Rechts-Residuations-Gruppoide,* kurz *RR-Gruppoide.*
Unter den links-kürzbaren rechts-komplementären Halbgruppen sind vor allem die kommutativen von Interesse. Denn sie lassen sich ja, wie wir sahen, auffassen als Kegel einer abelschen Verbandsgruppe. Somit stellt sich die natürliche Frage nach dem Clan eines abelschen Verbandsgruppenkegels. Hier wird sich das Zusatzsystem

(R2') $$a * (b * a) \;=\; a * a$$

(AB) $$(a * b) * b \;=\; (b * a) * a$$

als charakteristisch erweisen. RR-Gruppoide diesen Typs bezeichnen wir als *symmetrisch* und deshalb kurz als *SR-Gruppoide.*
In einem besonderen Abschnitt werden wir die Abhängigkeiten zwischen *Ausgangs*-und *Ausdehnungs*-struktur untersuchen. Die dabei zu Tage geförderten Ergebnisse werden sich vor allem als interessant im Blick auf das spätere Kapitel über Bricks erweisen.
Die Frage stellt sich, ob Axiom (R3) durch Gleichungen ersetzt werden könnte. Dies ist (im allgemeinen Fall) nicht möglich, da es ein Modell von 4 Elementen gibt mit einem homomorphen Bild, das nicht Axiom (R3) erfüllt. Man definiere etwa auf $\{1, a, b, c\} : x * x := 1 =: a * c =: b * c, a * b := c =: b * a, c * a := a, c * b := b$.
In Sonderfällen hingegen lässt sich (R3) sehr wohl durch Gleichungen ersetzen, etwa im Falle der *Hilbert-Algebra* – wie wir noch sehen werden – oder aber im Fall des abelschen Verbandsgruppenkegels.

5.2 Allgemeine Clans

5. 2. 1 Proposition. *Sei $\mathfrak{R}$ ein RR-Gruppoid. Dann liefert*

$$a \geq b \;:\Longleftrightarrow\; a * b = c * c$$

eine Partialordnung auf R mit $a * a = b * b =: 1$ als Minimum.
Ist $\mathfrak{R}$ sogar ein SR-Gruppoid, so ist diese Partialordnung zudem $\wedge$-abgeschlossen via $a \wedge b := (a * b) * b$.

BEWEIS. $a*a = b*b$ folgt aus (R2), Reflexivität und Antisymmetrie sind evident und die Transitivität folgt aus

$$\begin{array}{rcl} a \leq b & \& & b \leq c \\ & \Longrightarrow & \\ c*a & = & (c*b)*(c*a) \\ & = & (b*c)*(b*a) \\ & = & d*d\,. \end{array}$$

Schließlich haben wir in SR-Gruppoiden zunächst

$$\begin{array}{rrcl} & ((a*b)*b)*b & = & ((b*(a*b))*(a*b) = a*b \\ \rightsquigarrow & a \geq (a*b)*b & \& & b \geq (a*b)*b \\ & & \text{und} & \\ & x & \leq & a, b \\ & & \Longrightarrow & \\ & ((a*b)*b)*x & = & ((a*b)*b)*((x*b)*b) \\ & & = & (x*b)*(a*b) \\ & & = & a*((x*b)*b) \\ & & = & 1\,. \end{array}$$

□

Wir werden nun – ausgehend von einem beliebigen RR-Gruppoid – eine *Erweiterung* konstruieren, die ihrerseits Residuationsgruppoid einer links-kürzbaren rechts-komplementären Halbgruppe ist.
Zu diesem Zweck werden wir vorweg eine Charakterisierung dieser Halbgruppen in der Sprache der Residuation geben.

5. 2. 2 Proposition. *Ein Gruppoid $(R, *)$ ist das Residuationsguppoid einer links-kürzbaren rechts-komplementären Halbgruppe gdw. es der Bedingung genügt:*

(AC) $$\forall\ a, b\ \exists x : \ \ a*x = b\ \&\ x*a = 1\,.$$

BEWEIS. Sei $(R, \cdot, *)$ eine links-kürzbare rechts-komplementäre Halbgruppe. Dann gilt $a*ab = b$ und $ab*a = b*(a*a) = 1$. Folglich lässt sich (AC) erfüllen mittels ab.

Sind nun umgekehrt in $(R, *)$ die Bedingungen (R0), ..., (R3) erfüllt, so resultiert:

$$\begin{matrix} a * x = b & & x * a = 1 & & \\ & \& & & \Longrightarrow & x = y\,. \\ a * y = b & & y * a = 1 & & \end{matrix}$$

Denn die linke Seite liefert:

$$\begin{array}{rcl} x * y = (x * a) * (x * y) & = & (a * x) * (a * y) = b * b = 1 \\ & \Longrightarrow & \\ y & \leq & x\,, \end{array}$$

also aus Gründen der Dualität $x \leq y \;\&\; y \leq x \rightsquigarrow x = y$. Somit ist x eindeutig bestimmt.
Erfülle schließlich $(R, *)$ zusätzlich bezüglich der Komponenten a, b die Bedingung (AC). Dann folgt sukzessive mit $x := ab$

$$\begin{array}{llcll} (i) & a * ab & = & b \quad (\textit{per definitionem}) & \\ (ii) & ab * c & = & (ab * a) * (ab * c) & \text{(AC)} \\ & & = & (a * ab) * (a * c) & \text{(R1)} \\ & & = & b * (a * c) & \text{(R1)} \\ (iii) & a(a * b) * b(b * a) & = & (a * b) * (a * b(b * a)) & \\ & & = & (b * a) * (b * b(b * a)) & \\ & & = & b(b * a) * b(b * a) & \\ & & = & 1 & \\ & & \Longrightarrow & & \\ & a(a * b) & = & b(b * a)\,. & \end{array}$$

Somit erfüllt ein RR-Gruppoid unter der Voraussetzung von (AC) die Bedingungen der links-kürzbaren rechts-komplementären Halbgruppe. □

(A) Wir definieren nun eine Operation $*_1$ auf $R \times R$ vermöge

$$[a \,|\, b] *_1 [c \,|\, d] \;:=\; [b * (a * c) \,|\, ((a * c) * b) * ((c * a) * d)]$$

und beweisen als

5. 2. 3 Ein erstes Zwischenergebnis. $(R \times R)$ *erfüllt bezüglich* $*$ *die Bedingungen* (R0), (R1), (R2), *nicht hingegen notwendig auch Bedingung* (R3).

(B) Wir definieren eine Relation θ auf $(R \times R, *_1)$ vermöge

$$\begin{aligned}[a \mid b] \equiv [c \mid d](\theta) \ :\Longleftrightarrow \ & [a \mid b] *_1 [c \mid d] = [1 \mid 1] \\ \& \quad & [c \mid d] *_1 [a \mid b] = [1 \mid 1]\end{aligned}$$

und beweisen als

5. 2. 4 Ein zweites Zwischenergebnis.

(1) *θ ist eine Kongruenzrelation*

(2) *$(R \times R, *_1)/\,\theta$ ist ein RR-Gruppoid*

(3) $a \neq b \Longrightarrow [a \mid 1]\,\theta \neq [b \mid 1]\,\theta$

(4) $[a \mid 1]\,\theta \ *_{1\theta} \ [b \mid 1]\,\theta = [a * b \mid 1]\,\theta$

(5) $[a \mid 1]\,\theta \ *_{1\theta} \ X \doteq [b \mid 1]\,\theta \ \& \ X \ *_{1\theta} \ [a \mid 1]\,\theta \doteq [1 \mid 1]\,\theta$
ist für alle $a, b \in R$ lösbar.

(C) Wir wenden 5.2.4 an und erhalten als

5. 2. 5 Ein drittes Zwischenergebnis. *Es existiert eine Kette*

$$(R, *) \subseteq (R_1, *_1) \cdots (R_n, *_n) \subseteq \cdots ,$$

derart dass jedes Gleichungssystem (AC) *mit Koeffizienten a, b aus R_i lösbar ist in $(R_{i+1}, *_{i+1})$.*

Dies führt dann schließlich zu dem

5. 2. 6 Hauptsatz. *Jede zugleich links-kürzbare und rechts-komplementäre Ausdehnung $\mathfrak{S} := (S, *, \cdot)$ von $\mathfrak{R} := (R, *)$ enthält eine Produkterweiterung $\mathfrak{P} := (P_S(R), *_S)$ als Unterstruktur, die aus genau allen Produkten $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ $(a_i \in R)$ besteht, und es sind je zwei Produkterweiterungen $(P_S(R)\,, *_S)$, $(P_T(R)\,, *_T)$ isomorph.*

Hiernach kommen wir zu den Beweisschritten des Hauptsatzes. Dabei werden wir wie üblich auf die Operationsindizes $_1$, $_S$, $_\theta$ ... verzichten. Vorweg:

$$[a \mid b] * [c \mid d] \ = \ [b \mid 1] * ([a \mid 1] * [c \mid d])\,. \tag{5.8}$$

5. 2. 7 Proposition. *Erfülle $(R\,, *)$ die Bedingungen* (R0), ..., (R2). *Dann erfüllt auch $(R \times R\,, *)$ die Bedingungen* (R0), ..., (R2).

BEWEIS. Wir haben unmittelbar $[a \mid b] * [a \mid b] = [1 \mid 1]$ und damit sofort:

$$\text{(R0)} \qquad ([a \mid b] * [a \mid b]) * [c \mid d] \;=\; [1 \mid 1] * [c \mid d] = [c \mid d]$$

$$\text{(R2)} \qquad [a \mid b] * ([c \mid d] * [c \mid d]) \;=\; [a \mid b] * [1 \mid 1] = [1 \mid 1]$$

Die Verifikation von (R1) erfolgt in drei Schritten:

$$\begin{array}{rl}
(i) & ([a \mid 1] * [c \mid 1]) * ([a \mid 1] * [u \mid v]) \\
= & [a * c \mid 1] * [a * u \mid (u * a) * v] \\
= & [(a * c) * (a * u) \mid ((a * u) * (a * c)) * ((u * a) * v)] \\
= & [(a * c) * (a * u) \mid ((u * a) * (u * c)) * ((u * a) * v)] \\
= & [(c * a) * (c * u) \mid ((u * c) * (u * a)) * ((u * c) * v)] \\
= & [(c * a) * (c * u) \mid ((c * u) * (c * a)) * ((u * c) * v)] \\
= & [c * a \mid 1] * [c * u \mid (u * c) * v] \\
= & ([c \mid 1] * [a \mid 1]) * ([c \mid 1] * [u \mid v])
\end{array}$$

$$\begin{array}{rl}
(ii) & ([a \mid b] * [c \mid 1]) * ([a \mid b] * [u \mid v]) \\
= & [b * (a * c) \mid 1] * ([b \mid 1] * ([a \mid 1] * [u \mid v])) \\
= & ([b \mid 1] * [a * c \mid 1]) * ([b \mid 1] * ([a \mid 1] * [u \mid v])) \\
= & ([a * c \mid 1] * [b \mid 1]) * ([a * c \mid 1] * ([a \mid 1] * [u \mid v])) \\
= & [(a * c) * b \mid 1] * (([a \mid 1] * [c \mid 1]) * ([a \mid 1] * [u \mid v])) \\
= & [(a * c) * b \mid 1] * (([c \mid 1] * [a \mid 1]) * ([c \mid 1] * [u \mid v])) \\
= & [(a * c) * b \mid 1] * ([c * a \mid 1] * ([c \mid 1] * [u \mid v])) \\
= & [c * a \mid (a * c) * b] * ([c \mid 1] * [u \mid v]) \\
= & ([c \mid 1] * [a \mid b]) * ([c \mid 1] * [u \mid v])
\end{array}$$

$$\begin{array}{rl}
(iii) & ([a \mid b] * [c \mid d]) * ([a \mid b] * [u \mid v]) \\
= & ([b \mid 1] * ([a \mid 1] * [c \mid d])) * ([b \mid 1] * ([a \mid 1] * [u \mid v])) \\
= & (([a \mid 1] * [c \mid d]) * [b \mid 1]) * (([a \mid 1] * [c \mid d]) * ([a \mid 1] * [u \mid v])) \quad (ii) \\
= & ([a * c \mid (a * a) * d] * [b \mid 1]) * (([c \mid d] * [a \mid 1]) * ([c \mid d] * [u \mid v])) \\
= & ([a * c \mid (c * a) * d] * [b \mid 1]) * ([d * (c * a) \mid 1] * ([c \mid d] * [u \mid v])) \\
= & [((c * a) * d) * ((a * c) * b) \mid 1] * ([d * (c * a) \mid 1] * ([c \mid d] * [u \mid v])) \\
= & [d * (c * a) \mid ((c * a) * d) * ((a * c) * b)] * ([c \mid d] * [u \mid v])) \\
= & ([c \mid d] * [a \mid b]) * ([c \mid d] * [u \mid v]) \,. \qquad \square
\end{array}$$

Aufgrund von 5.2.3 ist $(R \times R\,, *)$ ein schon fast RR-Gruppoid, es fehlt noch Axiom (R3). Wir gehen deshalb mittels der unter (B) definierten Relation über zu $\mathfrak{R}/\theta$.

5. 2. 8 Lemma. *θ ist eine Kongruenz-Relation.*

BEWEIS. (a) θ ist ein Äquivalenz-Relation, denn:

$$\begin{array}{rrcl}
(i) & [a \mid b] * [a \mid b] & = & [1 \mid 1] \\
(ii) & [a \mid b] \equiv [c \mid d] & \Rightarrow & [c \mid d] \equiv [a \mid b] \quad \textit{(per definitionem)} \\
(iii) & [a \mid b] \equiv [c \mid d] & \& & [c \mid d] \equiv [u \mid v] \\
& & \Longrightarrow & \\
& [a \mid b] * [u \mid v] & = & ([a \mid b] * [c \mid d]) * ([a \mid b] * [u \mid v]) \\
& & = & ([c \mid d] * [a \mid b]) * ([c \mid d] * [u \mid v]) \\
& & = & [1 \mid 1] * [1 \mid 1] = [1 \mid 1] \\
& & \Longrightarrow & \\
& [a \mid b] & \equiv & [u \mid v] \qquad \text{(beachte die Dualität.)}
\end{array}$$

(b) θ ist verträglich mit $*$, denn:

$$\begin{array}{rcl}
[x \mid y] \equiv [u \mid v] & \Rightarrow & [x \mid y] * [u \mid v] = [1 \mid 1] \\
& \& & [u \mid v] * [x \mid y] = [1 \mid 1] \\
& \Longrightarrow & \\
& & [x \mid y] * [a \mid b] \\
& = & ([x \mid y] * [u \mid v]) * ([x \mid y] * [a \mid b]) \\
& = & ([u \mid v] * [x \mid y]) * ([u \mid v] * [a \mid b]) \\
& = & [u \mid v] * [a \mid b] . \\
& \& & ([a \mid b] * [x \mid y]) * ([a \mid b] * [u \mid v]) \\
& = & ([x \mid y] * [a \mid b]) * ([x \mid y] * [u \mid v]) \\
& = & ([x \mid y] * [a \mid b]) * [1 \mid 1] = [1 \mid 1] .
\end{array}$$

Damit haben wir zusammenfassend:

$$\begin{array}{rrcl}
& [x \mid y] * [a \mid b] & \equiv & [u \mid v] * [a \mid b] \ \ (\theta) . \\
\& & [a \mid b] * [x \mid y] & \equiv & [a \mid b] * [u \mid v] \ \ (\theta) .
\end{array}$$

□

5. 2. 9 Lemma. $(R \times R, *)/\,\theta$ *Ist ein RR-Gruppoid.*

BEWEIS. Wir haben:

$$[a \mid b] \equiv [1 \mid 1] \implies [a \mid b] = [1 \mid 1]$$

und

$$
\begin{array}{rrcccc}
 & [a \mid b]\,\theta * [c \mid d]\,\theta & = & [1 \mid 1]\,\theta & = & [c \mid d]\,\theta * [a \mid b]\,\theta \\
\Longrightarrow & ([a \mid b] * [c \mid d])\,\theta & = & [1 \mid 1]\,\theta & = & ([c \mid d] * [a \mid b])\,\theta \\
\Longrightarrow & [a \mid b] * [c \mid d] & = & [1 \mid 1] & = & [c \mid d] * [a \mid b]
\end{array}
$$

ALSO

$$[a \mid b] \equiv [c \mid d] \quad \Longrightarrow \quad [a \mid b]\,\theta = [c \mid d]\,\theta\,. \qquad \square$$

(5.11)
$$
\begin{array}{rcl}
a \neq b & \Longrightarrow & [a \mid 1] * [b \mid 1] = [a * b \mid 1] \neq [1 \mid 1] \\
 & \vee & [b \mid 1] * [a \mid 1] = [b * a \mid 1] \neq [1 \mid 1]\,. \\
 & \Longrightarrow & \\
a \neq b & \Longrightarrow & [a \mid 1]\,\theta \neq [b \mid 1]\,\theta
\end{array}
$$

(5.12)
$$[a \mid 1]\,\theta * [b \mid 1]\,\theta \;=\; [a * b \mid 1]\,\theta$$

DENN: Dies folgt fast *per definitionem* $\square$

5. 2. 10 Lemma. *In $(R \times R, *)/\,\theta$ existieren Lösungen zu jedem Forderungssystem*

$$
\begin{array}{rcl}
[a \mid 1]\,\theta * X & \doteq & [b \mid 1]\,\theta \\
 & \& & \\
X * [a \mid 1] & \doteq & [1 \mid 1]\,\theta
\end{array}
$$

DENN:
$$
\begin{array}{rrcl}
 & [a \mid 1] * [a \mid b] & = & [1 \mid b] \equiv [b \mid 1] \\
\& & [a \mid b] * [a \mid 1] & = & [1 \mid 1] \equiv [1 \mid 1]\,.
\end{array}
\qquad \square
$$

Hiernach können wir zeigen:

5. 2. 11 Proposition. *Es existiert eine Kette*

$$(R, *) \subseteq (R_1, *_1) \;\subseteq\; \cdots \subseteq (R_n, *_n) \cdots$$

derart, dass jedes Gleichungssystem (AC) *mit $a, b \in R_i$ lösbar ist in R_{i+1}.*

BEWEIS. Wir bezeichnen mit $\overline{\mathfrak{R}} := (\overline{R}, *)$ die Algebra $(R \times R, *)/\,\theta$. Dann erhalten wir vermöge (5.12) eine Algebra $(R_1, *_1)$, die isomorph ist zu $(\overline{R}\,,\overline{*})$, indem wir alle Klassen von $(R \times R,*)/\,\theta$ zu dem Gruppoid $(R,*)$ adjungieren, die sich nicht durch ein Paar der Form $[a\,\big|\,1]$ repräsentieren lassen. Auf diese Weise entsteht eine Kette $(R,*) \subseteq (R_1,*)$, und wir können entlang der Reihe der natürlichen Zahlen fortfahren. □

Damit gilt bei Kombination der soeben bewiesenen Sätze

5. 2. 12 Das allgemeine Clan-Theorem. *Sei $(R,*)$ ein beliebiges RR-Gruppoid. Dann kann $(R,*)$ ausgedehnt werden zu einem Residuationsgruppoid einer links-kürzbaren rechts-komplementären Halbgruppe.*

BEWEIS. Wir betrachten die Kette aus 5.2.11 und $S := \bigcup R_n$ $(n \in \mathbf{N})$. Dann gibt es ein kleinstes m mit $a,b \in R_m$ und $c = a*b$ in R_m. Hiernach definieren wir $a*b := c$. Dann ist $(S,*)$ Residuationsgruppoid einer links-kürzbaren rechts-komplementären Halbgruppe, und es ist $(R,*)$ eingebettet in $(S,*)$, . □

Wir beenden diesen Abschnitt mit

5. 2. 13 Proposition. *Sei $(S,*,\cdot)$ eine links-kürzbare rechts-komplementäre Halbgruppe und sei $(R\,,*)$ eingebettet in $(S\,,*)$. Dann ist die Menge S_1 aller ab in $(S,*,\cdot)$ mit $a,b \in R$ abgeschlossen unter $*$, und es ist $(S_1,*)$ isomorph zu dem Gruppoid $(R\times R,*)/\,\theta$. Somit erhalten wir auf dem Wege der Induktion, dass die Menge aller Produkte mit Faktoren aus R abgeschlossen ist unter $*$ und isomorph ist zu der oben konstruierten Ausdehnung.*

BEWEIS. (i) R_1 ist abgeschlossen unter $*$ aufgrund der Definition von $ab*cd$.
(ii) $\Phi\ :\ [a\,\big|\,b]\,\theta \longrightarrow ab$ ist eine bijektive Funktion, denn:

$$\begin{aligned}
& [a\,\big|\,b]\,\theta \geq [c\,\big|\,d]\,\theta \\
\Longleftrightarrow\ & [a\,\big|\,b] * [c\,\big|\,d] = [1\,\big|\,1] \\
\Longleftrightarrow\ & [b*(a*c)\,\big|\,((a*c)*b)*((c*a)*d) = (1\,\big|\,1] \\
\Longleftrightarrow\ & b*(a*c) = 1 = ((a*c)*b)*((c*a)*d) \\
\Longleftrightarrow\ & (b*(a*c))((a*c)*b)((c*a)*d) = 1 \\
\Longleftrightarrow\ & ab*cd = 1 \\
\Longleftrightarrow\ & ab \geq cd
\end{aligned}$$

(*iii*) Schließlich ist Φ verträglich wegen

$$\begin{aligned}
& \Phi\,([a\,|\,b]\,\theta * [c\,|\,d]\,\theta) \\
= \ & [b * (a * c)\,|\,((a * c) * b) * ((c * a) * d]\,\theta \\
= \ & (b * (a * c))(((a * c) * b) * ((c * a) * d)) \\
= \ & ab * cd \\
= \ & \Phi([a\,|\,b]\,\theta) * \Phi([c\,|\,d]\,\theta)\,.
\end{aligned}$$

Wiederholung der Methode führt dann auf dem Wege der Induktion zum Ziel. □

Ein Hinweis: Mit dem Hauptsatz ist u. a. gewährleistet, dass das Wortproblem für RR-Gruppoide gleichwertig ist mit dem Wortproblem für linkskürzbare rechtskomplementäre Halbgruppen. Eine Lösung dieses Problems gab G. Heinemann in [92].

5.3 Symmetrische ℓ-Gruppenclans

Grundlage des nachfolgenden Abschnitts ist

5. 3. 1 Das abelsche Kegel-Clan-Theorem. *Ein RR-Gruppoid* $\mathfrak{R} := (R, *)$ *lässt eine abelsche* ℓ-Gruppenkegel-Erweiterung zu gdw. es die Axiome erfüllt:

$$\text{(R2')} \qquad a * (b * a) = a * a$$

$$\text{(AB)} \qquad (a * b) * b = (b * a) * a\,.$$

BEWEIS. Offenbar sind die geforderten Bedingungen notwendig.
Seien in $\mathfrak{R}$ die Bedingungen (R2') and (AB) erfüllt. Dann gilt in $\mathfrak{R}$ auch:

$$\text{(RS)} \qquad \begin{aligned}
a * (b * c) &= (a * (b * a)) * (a * (b * c)) \\
&= ((b * a) * a) * ((b * a) * (b * c)) \\
&= ((a * b) * b) * ((a * b) * (a * c)) \\
&= b * (a * c)\,,
\end{aligned}$$

und es resultiert problemlos

$$\text{(ES)} \qquad \begin{gathered}
[a\,|\,b] \equiv [c\,|\,d] \\
\Longleftrightarrow \\
a * c = d * b \quad \& \quad c * a = b * d
\end{gathered}$$

Unmittelbar klar ist hiernach

$$[a \,|\, b] \;\equiv\; [b \,|\, a]\,. \tag{5.17}$$

Wir haben zu zeigen, dass (R2') und (AB) übertragen werden auf die Erweiterung $\mathfrak{R}_1 := (R \times R, *)/\equiv$.
Dies ergibt sich fast unmittelbar für (R2'), man nutze (RS).
Auch haben wir unmittelbar Erfolg im Falle der speziellen Formel:

$$([a \,|\, b] * [c \,|\, 1]) * [c \,|\, 1] \;\equiv\; ([c \,|\, 1] * [a \,|\, b]) * [a \,|\, b]$$

Komplizierter hingegen ist der allgemeine Fall. Hier erhalten wir zunächst:

$$\begin{array}{lll}
(i) & & ([a \,|\, b] * [c \,|\, d]) * [c \,|\, d] \\
& = & [b * (a * c) \,|\, ((a * c) * b) * ((c * a) * d)] * [c \,|\, d] \\
& = & [((a * c) * b) * ((c * a) * d) \,|\, 1] * ([b * (a * c) \,|\, 1] * [c \,|\, d]) \\
& = & [((a * c) * b) * ((c * a) * d) \,|\, 1] * [(b * (a * c)) * c \,|\, d] \\
& = & [((a * c) * b) * ((c * a) * d) \,|\, 1] * [d \,|\, (b * (a * c)) * c] \\
& \equiv & [(((a * c) * b) * ((c * a) * d)) * d \,|\, (b * (a * c)) * c] \\
& =: & [P \,|\, Q] \\
\rightsquigarrow & & [R \,|\, S] \\
& := & [(((c * a) * d) * ((a * c) * b)) * b \,|\, (d * (c * a)) * a] \\
& \equiv & ([c \,|\, d] * [a \,|\, b]) * [a \,|\, b]
\end{array}$$

Demzufolge sind wir am Ziel, sobald wir bewiesen haben:

$$P * R = S * Q \quad \& \quad R * P = Q * S\,.$$

Aufgrund der Dualität genügt es aber, die erste dieser Gleichungen zu beweisen. Und hierzu genügt der Nachweis von

$$[P * R \,|\, 1] \;\equiv\; [S * Q \,|\, 1]\,,$$

der sich wie folgt ergibt:

$$
\begin{aligned}
& [P * R \,|\, 1] \\
= \;& [((((a*c)*b)*((c*a)*d))*d)*((((c*a)*d)*((a*c)*b)))*b \,|\, 1] \\
= \;& (([c*a \,|\, (a*c)*b]*[d \,|\, 1])*[d \,|\, 1])*[(((c*a)*d)*((a*c)*b))*b \,|\, 1] \\
\equiv \;& (([d \,|\, 1]*[c*a \,|\, (a*c)*b])*([c*a \,|\, (a*c)*b]) \\
* \;& [(((c*a)*d)*((a*c)*b))*b \,|\, 1] && (i) \\
\equiv \;& [(((c*a)*d)*((a*c)*b))*((a*c)*b) \,|\, (d*(c*a))*(c*a)] \\
* \;& [(((c*a)*d)*((a*c)*b))*b \,|\, 1] \\
\equiv \;& [(d*(c*a))*(c*a) \,|\, 1]*[((a*c)*b)*b \,|\, 1] && \text{(R1, R2')} \\
\equiv \;& [((d*(c*a))*(c*a))*((b*(a*c))*(((a*c)*c)*c)) \,|\, 1] && \text{(AB, R2)} \\
\equiv \;& [((d*(c*a))*(c*a))*((b*(a*c))*(((c*a)*a)*c)) \,|\, 1] \\
\equiv \;& [((c*a)*a)*(((d*(c*a))*(c*a))*((b*(a*c))*c)) \,|\, 1] && \text{(RS)} \\
\equiv \;& ([d*(c*a) \,|\, 1]*[c*a \,|\, (c*a)*a])*[(b*(a*c))*c \,|\, 1] \\
\equiv \;& ([d*(c*a) \,|\, 1]*[a \,|\, 1])*[(b*(a*c))*c \,|\, 1] && \text{(ES)} \\
\equiv \;& [(d*(c*a))*a \,|\, 1]*[(b*(a*c))*c \,|\, 1] && \text{(ES)} \\
\equiv \;& [((d*(c*a))*a)*((b*(a*c))*c) \,|\, 1] \\
= \;& [S*Q \,|\, 1]\,.
\end{aligned}
$$

Damit sind wir am Ziel □

5.4 Zur Struktur der Produkterweiterungen

Gemäß dem Einbettungssatz besitzen RR-Gruppoide eine links-kürzbare *rechts-komplementäre Halbgruppenerweiterung,* die im symmetrischen Fall eine abelsche ℓ-Gruppenkegelerweiterung darstellt. Nichts aber kann bislang über die Qualität dieser Erweiterunge(en) gesagt werden.
So wissen wir beispielsweise nicht, ob – endliche – Suprema mitgehen, ob Vollständigkeit erhalten bleibt, ob Maße mitgehen usw. Dergleichen zu klären ist unser nächstes Ziel.
Allerdings wissen wir nach dem vorhergehenden Paragraphen schon, dass die von uns betrachtete Erweiterung als Produkterweiterung i. w. eindeutig bestimmt ist. Deshalb können wir von *dem* Produktkegel $\mathfrak{P}$ des RR-Gruppoids $(R,*) =: \mathfrak{R}$ sprechen. Seine Elemente lassen sich als Produkte der Form $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ $(a_i \in R)$ darstellen.

Im folgenden werden wir weitere Abhängigkeiten herleiten.

5. 4. 1 Proposition. *Sei $\mathfrak{R}$ ein RR-Gruppoid und erfülle c das Bedingungssystem:*

$$a * c = a * b \quad \& \quad c * a = 1\,.$$

Dann ist c Supremum zu a und b in $\mathfrak{R}$.

BEWEIS. Wir haben

$$\begin{aligned} c * b &= (c * a) * (c * b) \\ &= (a * c) * (a * b) \\ &= (a * b) * (a * b) \\ &= 1 \\ &= c * a\,. \end{aligned}$$

Also gilt $a, b \leq c$. Sei nun $a, b \leq v$ für $v \in P$. Dann folgt:

$$\begin{aligned} v * c &= (v * a) * (v * c) \\ &= (a * v) * (a * c) \\ &= (a * v) * (a * b) \\ &= (v * a) * (v * b) = 1\,. \end{aligned}$$ □

Weiter erhalten wir mittels 5.4.1

5. 4. 2 Proposition. *Sei $\mathfrak{R}$ ein SR-Gruppoid und c die obere Grenze zu a und b. Dann ist c auch obere Grenze zu a und b in $\mathfrak{P}$.*

BEWEIS. Es gilt $\quad c = ((a * b) * (a * c)) * c =: s$

wegen

$$\begin{aligned} s * a &= (((a * b) * (a * c)) * c) * a \\ &= (((a * b) * (a * c)) * c) * ((a * c) * c) \\ &= (a * c) * ((a * b) * (a * c)) \\ &= 1 = s * b\,. \end{aligned}$$

Und dies liefert

$$\begin{aligned} a * c &= a * (((a * b) * (a * c)) * c) \\ &= ((a * b) * (a * c)) * (a * c) \\ &= ((a * c) * (a * b)) * (a * b) \\ &= ((c * a) * (c * b)) * (a * b) \\ &= a * b\,. \end{aligned}$$

Damit sind wir am Ziel, aufgrund von 5.4.1 □

Hiernach beweisen wir als ein erstes Hauptergebnis dieses Paragraphen:

5. 4. 3 Proposition. *Nenne R-Kongruenz jede Kongruenz von* $\mathfrak{R}$ *mit der Eigenschaft* $a * b \equiv c * c \equiv b * a \Longrightarrow a \equiv b$. *Dann sind die Kongruenzen von* $\mathfrak{P}$ *eindeutige Fortsetzungen der R-Kongruenzen von* $\mathfrak{R}$ *und jede R-Kongruenz von* $\mathfrak{R}$ *kann auf* $\mathfrak{P}$ *ausgedehnt werden.*

BEWEIS. Sei $\equiv$ eine Kongruenz auf $\mathfrak{P}$. Dann erhalten wir für $a, b, c, d \in R_1$ die Äquivalenz:

$$\begin{aligned} ab \equiv cd &\iff ab * cd \equiv 1 \equiv cd * ab \\ &\iff b * (a * c) \equiv 1 \equiv d * (c * a) \\ &\quad\& \quad (a * c) * b \equiv (c * a) * d \end{aligned}$$

Folglich gibt es zu jeder R-Kongruenz von $\mathfrak{R}$ höchstens eine Ausdehnung. Sei nun $\equiv$ eine R-Kongruenz von $\mathfrak{R}$ und $(\overline{R}_1, \overline{*}_1)$ die Ausdehnung von $(R, *)/\equiv$ im obigen Sinne. Dann definiert

$$\Phi : ab \longmapsto \overline{ab}$$

einen Homomorphismus von $(R_1 \ , *_1)$ auf $(\overline{R}_1 \ , \overline{*}_1)$, wie der Leser leicht bestätigt. Weiter haben wir die Äquivalenz

$$\begin{array}{cccc} & \Phi\,(ab) & = & \Phi\,(cd) \\ & & \iff & \\ & b * (a * c) \equiv & 1 & \equiv d * (c * a) \\ \& & (a * c) * b & \equiv & (c * a) * d\,. \end{array}$$

Damit ist alles gezeigt. □

Als nächstes geben wir ein Ergebnis über Maße auf $\mathfrak{R}$.

5. 4. 4 Definition. $\mu : a \longrightarrow |\,a\,| \in \mathbf{R}$ heiße ein Maß auf $\mathfrak{R}$, wenn gilt:

(M1) $$|\,a\,| + |\,a * b\,| \;=\; |\,b\,| + |\,b * a\,|$$

(M2) $$|\,1\,| \;=\; 0\,.$$

Wie üblich nennen wir ein Maß auch eine Maßfunktion. Offenbar stimmt diese Definition im booleschen Fall überein mit der üblichen Definition, denn der Leser beachte:

$$\begin{aligned} |\,a\,| &= |\,a\,| + |\,a * (a \wedge b)\,| \\ &= |\,a \wedge b\,| + |\,b * a\,| \\ &\Longrightarrow \\ |\,a \wedge b\,| + |\,a \vee b\,| &= |\,a \wedge b\,| + |\,b * a\,| + |\,b\,| \\ &= |\,a\,| + |\,b\,|\,. \end{aligned}$$

5. 4. 5 Proposition. *Sei μ eine Maßfunktion auf $\mathfrak{R}$. Dann ist*

$$\mu_1 : |\,ab\,| \;\longrightarrow\; |\,a\,| + |\,b\,|$$

eine Maßfunktion auf $\mathfrak{R}_1$. Folglich kann jede Maßfunktion auf $\mathfrak{R}$ ausgedehnt werden zu einer Maßfunktion auf $\mathfrak{P}$, die zusätzlich $|\,ab\,| = |\,a\,| + |\,b\,|$ erfüllt.

BEWEIS. μ_1 ist eine Funktion, denn

$$\begin{array}{rcl} ab & = & cd \\ & \Longleftrightarrow & \\ b * (a * c) = & 1 & = d * (c * a) \\ & \& & \\ (a * c) * b & = & (c * a) * d \end{array}$$

Weiter gilt:

$$\begin{aligned} |\,a\,| + |\,b\,| &= |\,a\,| + |\,b\,| + 0 \\ &= |\,a\,| + |\,b\,| + |\,b * (a * c)\,| \\ &= |\,a\,| + |\,a * c\,| + |\,(a * c) * b\,| \\ &= |\,c\,| + |\,c * a\,| + |\,(c * a) * d\,| \\ &= |\,c\,| + |\,d\,| + |\,d * (c * a)\,| \\ &= |\,c\,| + |\,d\,| + 0 \\ &= |\,c\,| + |\,d\,|\,. \end{aligned}$$

Es ist μ_1 aber nicht nur eine Funktion, sondern (sogar) eine Maßfunktion. Denn $\mu_1(1) = 0$ ist evident, und es gilt:

$$\begin{aligned} & |\ ab\ | + |\ ab * cd\,| \\ = \;& |\,a\,| + |\,b\,| + |\,b * (a * c)\,| + |\,((a * c) * b) * ((c * a) * d)\,| \\ = \;& |\,a\,| + |\,a * c\,| + |\,(a * c) * b\,| + |\,((a * c) * b) * ((c * a) * d)\,| \\ = \;& |\,c\,| + |\,c * a\,| + |\,(c * a) * d\,| + |\,((c * a) * d) * ((a * c) * b)\,| \\ = \;& |\,c\,| + |\,d\,| + |\,d * (c * a)\,| + |\,((c * a) * d) * ((a * c) * b)\,| \\ = \;& |\,cd\,| + |\,cd * ab\,|. \end{aligned}$$

□

Als nächstes halten wir fest:

5. 4. 6 Proposition. *Ist $\mathfrak{R}$ linear geordnet vermöge $a \geq b :\Longleftrightarrow b * a = 1$, so ist $\mathfrak{P}$ linear geordnet vermöge $[\,a\,|\,b\,] \geq [\,c\,|\,d\,] \Longleftrightarrow [\,a\,|\,b\,] * [\,c\,|\,d\,] = [\,1\,|\,1\,]$.*

BEWEIS. Da $\mathfrak{P}$ vermöge $\leq$ partialgeordnet ist, genügt es zu zeigen, dass je zwei Elemente vergleichbar sind. Hier dürfen wir uns aber aus methodischen

Gründen beschränken auf $\mathfrak{R}_1$. Zu diesem Zweck seien a, b, c, d aus R und es gelte $a * c = 1$. Dann folgt:

$$\begin{aligned} ab * cd &= b * (a * c)((c * a) * d) \\ &= b * ((c * a) * d)\,. \end{aligned}$$

Ist nun $b*((c*a)*d) = 1$, so erhalten wir $ab \geq cd$. Andernfalls muss $(c*a)*d$ verschieden sein von 1, was bedeutet, dass $d * (c * a) = 1 = ((c * a) * d) * b$ erfüllt ist, also :

$$\begin{aligned} cd * ab &= d * (c * a)((a * c) * b) \\ &= d * (c * a)b \\ &= (d * (c * a))(((c * a) * d) * b) \\ &= 1 \cdot 1 = 1 \\ cd &\geq ab\,. \end{aligned}$$

□

Im Rest dieses Abschnitts befassen wir uns mit dem symmetrischen Fall. Wir ergänzen als erstes 5.4.5 durch

5. 4. 7 Proposition. *Sei $\mathfrak{R}$ symmetrisch. Dann erfüllt $\mathfrak{P}$ Axiom* (R2′) *und gibt es kürzbare Elemente, so existiert eine Quotientenhülle $\mathfrak{Q}$, die ihrerseits genau dann $a/b = c/d$ erfüllt, wenn es in P kürzbare Elemente x, y gibt, derart dass $ax = cy$ und $bx = dy$ erfüllt ist, und es lässt sich jede Maßfunktion μ auf $\mathfrak{R}$ fortsetzen zu einer additiven Funktion μ_1 auf $\mathfrak{Q}$ vermöge:*

$$\mu_1 : a/b \ \longrightarrow\ |\,a\,| - |\,b\,|\,.$$

BEWEIS. Nach 5.3.1 können wir zu einem Verbandsgruppenkegel übergehen und hier definieren

$$a/b \ \theta\ c/d \iff \exists\, x, y\, : ax = cy \ \&\ bx = dy\,.$$

Dann erhalten wir eine Erweiterung des gesuchten Typs.
Als nächstes erkennen wir unmittelbar, dass μ_1 eine Funktion ist, wegen:

$$\begin{aligned} a/b = c/d &\Longrightarrow ax = cy \ \&\ bx = dy \\ &\Longrightarrow |\,a\,| + |\,x\,| = |\,c\,| + |\,y\,| \\ &\quad\ \&\ \ |\,b\,| + |\,x\,| = |\,d\,| + |\,y\,| \\ &\Longrightarrow |\,a\,| - |\,b\,| = |\,c\,| - |\,d\,|\,. \end{aligned}$$

Schließlich gelten

$$
\begin{aligned}
|\, a/a \,| &= |\, a \,| - |\, a \,| = 0 \\
&\& \\
|\, (a/b) \cdot (c/d) \,| &= |\, a(b * c)/d(c * b) \,| \\
&= |\, a \,| + |\, b * c \,| - |\, d \,| - |\, c * b \,| \\
&= |\, a \,| - |\, b \,| + |\, c \,| - |\, d \,| \\
&= |\, a/b \,| + |\, c/d \,| \,.
\end{aligned}
$$

Damit sind wir am Ziel □

Kapitel 6

ℓ-Gruppen-Redukte

6.1 Vorbemerkungen

Schon oben wurde erklärt, was wir unter einem Kegel-Clan verstehen wollen. Ihn zu charakterisieren, ist das Ziel dieses Kapitels.
Sei $(C, \cdot, \wedge)$ ein Verbandsgruppenkegel. Dann wird C *via* $a * b := 1 \vee a^{-1}b$ und $a : b := 1 \vee ab^{-1}$ C bezüglich $*$ und $:$ zu einer Algebra mit

$$
\begin{array}{llcl}
(\mathrm{R1}^{*}) & (a * b) * (a * c) & = & (b * a) * (b * c) \\
(\mathrm{R1}^{:}) & (c : b) : (a : b) & = & (c : a) : (c : b) \\
(\mathrm{R2}^{*}) & (a * a) * b & = & b \\
(\mathrm{R2}^{:}) & b & = & b : (a : a) \\
(\mathrm{R3}) & a * (b : c) & = & (a * b) : c \\
(\mathrm{R4}) & a : (b * a) & = & (b : a) * b\,.
\end{array}
$$

Tatsächlich wird sich diese Algebra als *Kegel-Clan* erweisen, doch solange dies nicht verifiziert ist, haben wir natürlich eine neutrale Benennung zu wählen. Aus diesem Grunde sei vorab die oben definierte Algebra als Kegel-Algebra bezeichnet.
Offenbar werden die Axiome der Kegel-Algebra auch vom RR-Redukt der booleschen Algebra erfüllt, das in [1] intensiv von J. C. Abbot studiert wurde.
Ein erstes Hauptergebnis dieses Kapitels wird sein, dass die oben gesammelte „Liste‘“ von Bedingungen charakteristisch ist für den Kegel-Clan.

Als ein zweites Hauptergebnis werden wir einen kanonischen Nullabschluss für y *Kegelredukte* vorstellen.

Grob gesprochen wird damit gezeigt, dass es eine zweite Erweiterungstheorie für Verbandsgruppenkegel gibt:

Indem wir *Inverse* adjungieren, werden wir zur *Quotientenhülle* und damit zur Struktur der Verbandsgruppe geführt.

Indem wir *Komplemente* adjungieren, werden wir zur *Komplementenhülle* und damit zur Struktur des *Brick* geführt.

Aus diesem Grunde können wir konstatieren, dass Theoreme der ℓ-Gruppen-Theorie auch Theoreme der Brick-Theorie sind, also auch eine Brick-Version haben, und *vice versa*, dass Theoreme der Brick-Therorie auch Theoreme der ℓ-Gruppen-Theorie sind, also auch eine ℓ-Gruppen-Version haben.

Wie stark die Struktur der *assoziierten* Verbandsgruppe eines Kegel-Clans $(R\,*, :)$ von diesem Kegel-Clan bestimmt wird, dürfte sich an dieser Stelle am deutlichsten dadurch beschreiben lassen, dass alle Propositionen, die im letzten Kapitel für RR-Gruppoide und SR-Gruppoide formuliert wurden, auch für Kegel-Clans gültig bleiben.

Schließlich untersuchen wir ℓ-Gruppen-Clans, das sind partielle Verbandshalbgruppen mit Kürzungsregel. Sie lassen sich einbetten in Verbandsgruppen.

Gezielte Beiträge zur Theorie der *Bricks* werden wir in einem späteren Kapitel vorstellen.

6.2 Arithmetik

Grundgegebenheit sei im folgenden stets eine Kegel-Algebra. Wir stellen zunächst die Regeln der Arithmetik zusammen, soweit sie in diesem Kapitel eine Rolle spielen werden. Dabei ist zu beachten, dass die Kegel-Algebra *rechts-links-dual* erklärt ist, weshalb stets auch die dualen Aussagen mit bewiesen sind. Dennoch werden wir gelegentlich aus Gründen der Betonung „doppeln“.

(6.7) $$a * a = \ 1 \ = b : b\,.$$

DENN:
$$\begin{aligned} a * a &= ((a * a) : (b : b)) * (a * a) \\ &= (b : b) : ((a * a) * (b : b)) \\ &= b : b\,, \end{aligned}$$

fertig! □

Natürlich ist aufgrund von (6.7) auch $a * a = b * b$ und $a : a = b : b$ erfüllt. Deshalb können wir $a*a := 1 =: b : b$ setzen. Damit folgt dann unmittelbar aus (R2*), (R2$^:$)

(6.8) $$1 * a = \ a \ = a : 1\,,$$

(6.9) $$a * 1 = \ 1 \ = 1 : a\,.$$

DENN:

$$a * 1 = a * ((a : 1) * a) = a * (1 : (a * 1)) = (a * 1) : (a * 1) = 1.$$

□

(6.10) $$c * (b * a) = 1 \iff (a : c) : b = 1\,.$$

BEWEIS. Es genügt zu zeigen, dass $a * b = 1 \Longrightarrow b : a = 1$ erfüllt ist, da sich hieraus $c*(b*a) = 1 \Longrightarrow (b*a) : c = b*(a : c) = (a : c) : b = 1$ ergibt. Es gilt aber

$$\begin{aligned} a * b &= 1 \\ &\Longrightarrow \\ b : a &= (b : (a * b)) : a \\ &= ((a : b) * a) : a \\ &= (a : b) * (a : a) = 1 \end{aligned}$$

□

(6.11) $$a * (b * a) = \ 1 \ = (a : b) : a\,.$$

DENN: $$(b * a) : a = b * (a : a) = 1\,.$$ □

Das nächste Lemma sichert, dass $(C, *)$ ein RR-Gruppoid ist.

(6.12) $$\begin{aligned} a * b = \ 1 \ &= b * a \\ &\Longrightarrow \\ a = a : (b * a) \ &= \ (b : a) * b = b\,. \end{aligned}$$

6. 2. 1 Proposition. *$a * b = 1 \Longleftrightarrow: a \geq b$ erzeugt eine Partialordnung auf R, die zudem den Implikationen genügt:*

$$a \geq b \implies a * c \leq b * c\,. \tag{6.13}$$

$$b \geq c \implies a * b \geq a * c\,. \tag{6.14}$$

DENN: Der erste Teil der Behauptung folgt aus 5.2.1, und es gilt:

$$\begin{array}{rcl} a * b = 1 & \implies & a * (b : (c * b)) = 1 \\ & \implies & (a * b) : (c * b) = 1 \\ & \& & \\ (a * b) * (a * c) & = & (b * a) * (b * c)\,. \end{array}$$

□

$$a : (b * a) \;=\; \inf\,(a, b) =: a \wedge b\,. \tag{6.15}$$

DENN:

$$\begin{array}{rrcl} & a * (a : (b * a)) & = & (a * a) : (b * a) = 1 \\ \& & b * (a : (b * a)) & = & (b * a) : (b * a) = 1 \\ & & \text{und} & \\ & x & \leq & a, b \\ & & \implies & \\ & (a : (b * a)) * x & = & (a : (b * a)) * (a : (x * a)) \\ & & = & 1 \qquad\qquad (6.13, 6.14) \end{array}$$

□

$$a : (b * a) = (b : a) * b = a \wedge b = (a : b) * a = b : (a * b)\,. \tag{6.16}$$

$$(a \wedge b) * b \;=\; a * b\,. \tag{6.17}$$

DENN: $b * (a * b) = 1 \rightsquigarrow a * b \leq b \rightsquigarrow (a \wedge b) * b = (b : (a * b) * b = a * b\,.$ □

$$a \wedge b = 1 \implies a * b = b \;\&\; b : a = b\,. \tag{6.18}$$

$$a * b \wedge b * a = \quad 1 \quad = b : a \wedge a : b\,. \tag{6.19}$$

DENN:

$$\begin{array}{rcl} (a * b) \wedge (b * a) & = & ((a * b) : (b * a)) * (a * b) \\ & = & (a * (b : (b * a))) * (a * b) \\ & = & ((b : (b * a)) * a) * ((b : (b * a)) * b) \\ & = & 1\,. \qquad\qquad\qquad (6.13, 6.14) \end{array}$$

Damit ist aus Gründen der Dualität alles gezeigt. □

(6.20)
$$a * (b \wedge c) \;=\; (a * b) \wedge (a * c)\,.$$

DENN: Sei zunächst $a \le b \wedge c$ erfüllt. Dann folgt

$$\begin{aligned}
a * (b \wedge c) &= a * (b : (c * b) \\
&= (a * b) : (c * b) \\
&= (a * b) : ((c * a) * (c * b)) \\
&= (a * b) : ((a * c) * (a * b)) \\
&= a * b \wedge a * c\,.
\end{aligned}$$

Das liefert weiter
$$\begin{aligned}
&\big(a * (b \wedge c)\big) * \big(a * b \wedge a * c) \\
= \;&\big((a * (b \wedge c)) * (a * b)\big) \\
\wedge \;&\big((a * (b \wedge c)) * (a * c)\big) \\
= \;&\big((b \wedge c) * a) * ((b \wedge c) * b)\big) \\
\wedge \;&\big((b \wedge c) * a) * ((b \wedge c) * c)\big) \\
\le \;&(b \wedge c) * b \wedge (b \wedge c) * c \\
= \;&c * b \wedge b * c = 1\,.
\end{aligned}$$
□

(6.21)
$$\begin{aligned}
a \wedge b = 1 \implies\; & c * b = (a * c) * b = (c : a) * b \\
\& \;\; & b : c = b : (c : a) = b : (a * c)\,.
\end{aligned}$$

DENN:
$$\begin{aligned}
a \wedge b &= 1 \\
&\Longrightarrow \\
(a * c) * b &= ((c : (a * c)) * c) \\
&\ast\;\; ((c : (a * c)) * b) && (6.16, 6.18) \\
&= c * b && (\mathrm{R}1^*, 6.11) \\
&= ((c : a) * c) * ((c : a) * b) && (\mathrm{R}1^*, \quad 6.11) \\
&= (c : a) * b && (6.16, 6.18)
\end{aligned}$$

Hieraus folgt der Rest aus Gründen der Dualität. □

(6.22)
$$\begin{aligned}
a \wedge b = 1 \implies\; & (c * d) * b = ((c : a) * d) * b \\
\& \;\; & b : (d : c) = b : (d : (a * c))\,.
\end{aligned}$$

DENN:
$$\begin{aligned}
a \wedge b &= 1 \\
&\Longrightarrow \\
((c : a) * d) * b &= (((c : a) * c) * ((c : a) * d)) * b && (6.21) \\
&= (c * d) * b
\end{aligned}$$
□

(6.23)
$$\begin{aligned}(a*b)*(a*c) &= (b*a)*(b*c)\\ &= (((a:(b*a))*a)\\ &* (((b:a)*b)*((b:a)*c)))\\ &= a*((b:a)*c)\end{aligned}$$

(6.24)
$$\begin{aligned} x\wedge z = {}& 1 = y\wedge z\\ &\Longrightarrow\\ (((b:x):y)*b):z &= ((b:x):y)*b\,.\end{aligned}$$

BEWEIS. Zweimalige Anwendung von (6.23) liefert zunächst die Gleichheit $x*(y*(((b:x):y)*b))=1$. Wir definieren $(((b:x):y)*b)\wedge z =: d$. Dann erhalten wir $x*(y*d)=1$, und hieraus folgt $y*d \le x\wedge z$. Somit führt $x\wedge z = 1 = y\wedge z$ zu $d=1$. □

(6.25)
$$\begin{aligned}(a:b)*c &= (c:((a:b)*c))*c && (6.16)\\ &= ((a:b):(c*(a:b)))*c && (6.16)\\ &= ((a:b):((c*a):b))*c && (\mathrm{R}3)\\ &= ((a:(c*a)):(b:(c*a)))*c && (\mathrm{R}1^{:})\end{aligned}$$

(6.26)
$$\begin{aligned}&(u:x):(v:y)\\ =\ &\big((u:(y*x)):(x:(y*x))\big):\big((v:(x*y)):(y:(x*y))\big)\\ =\ &\big((u:(y*x)):((v:(x*y))\big):\big((y:(x*y)):(v:(x*y))\big)\\ =\ &\big((u:(y*x)):((v:(x*y))\big):\big((y:v):((x*y):v)\big)\,.\end{aligned}$$

6. 2. 2 Proposition. *Sei* $\mathfrak{R}$ *eine Algebra, die den Axiomen* (R1*) *bis* (R3) *genügt. Dann ist* $\mathfrak{R}$ *genau dann eine Kegel-Algebra, wenn* $\mathfrak{R}$ *zusätzlich erfüllt:*
$$a*a = b:b := 1 \ \ \&\ \ a*b=1 \Longleftrightarrow b:a=1$$
$$(a:b)*a = (b:a)*b \ \ \&\ \ a:(b*a) = b:(a*b)\,.$$

DENN: Man beachte, dass der Beweis zu (6.15) lediglich auf (R4$^{:}$) zurück greift. □

Schließlich gilt:

$$a : (b * (c * a)) \;=\; ((a : b) : c) * a\,. \tag{6.27}$$

DENN: Wir erhalten die Implikationskette:

$$\begin{aligned}
&(a : (b * (c * a))) * (((a : b) : c) * a)\\
= \;&(a : (b * (c * a))) * ((a : (((a : b) : c) * a)) * a)\\
= \;&(a : (b * (c * a))) * (a : ((((a : b) : c) * a) * a))\\
= \;&((a : (b * (c * a))) * a) : ((((a : b) : c) * a) * a)\\
= \;&(b * (c * a)) : ((((a : b) : c) * a) * a))\\
= \;&b * ((c * a) : (((a : b) : c) * a) * a)\\
= \;&b * (c * (a : (((a : b) : c) * a) * a))\\
= \;&b * (c * (((a : b) : c) * a))\ ,
\end{aligned}$$

beachte (6.10) und

$$\begin{aligned}
(((a : b) : c) * a) : b) : c \;&=\; ((a : b) : c) * (a : b)) : c\\
&=\; ((a : b) : c) * ((a : b) : c) = 1\,. \qquad \Box
\end{aligned}$$

6.3 Vom Kegel-Clan zum Kegel

Haben wir in einer Kegel-Algebra

$$\forall\, a, b\ \exists\, x :\ \ a * x = b \ \&\ x * a = 1\,, \tag{AC*}$$

so gilt auch $x : b = x : (a * x) = (a : x) * a = a$ und $b : x = (a * x) : x = a * (x : x) = 1$, also mit (AC*) auch

$$\forall\, a, b\ \exists\, x :\ \ x : b = a \ \&\ b : x = 1\,. \tag{AC$^:$}$$

Hieraus resultiert

6. 3. 1 Proposition. *Eine Kegel-Algebra ist ein Kegelredukt genau dann, wenn sie der Bedingung genügt:*

$$\forall\, a, b\ \exists\, x :\ \ a * x = b \ \&\ x * a = 1\,. \tag{AC*}$$

Nach den Axiomen der Kegel-Algebra und aufgrund von (6.9), 6.2.1 ist jede Kegel-Algebra ein RR-Gruppoid bezüglich $*$ und ebenso bezüglich $:$. Somit gelten die Theoreme des letzten Kapitels sowohl für $(R\,, *)$ als auch für $(R\,,:)$. Aber die Frage bleibt offen, ob diese beiden Erweiterungen übereinstimmen. Klar ist in dieser Hinsicht unmittelbar, dass $(R\times R\,,\,*\,,\,:)$ die Axiome (R1*, R1$^:$, R2*, R2$^:$) erfüllt bezüglich

$$\begin{aligned}[a\,|\,b]*[c\,|\,d] &:= [b*(a*c)\,|\,((a*c)*b)*((c*a)*d)]\\ [d\,|\,c]:[b\,|\,a] &:= [(d:(a:c)):(b:(c:a)\,|\,(c:a):b]\end{aligned} \tag{6.31}$$

6. 3. 2 Proposition. *Sei $\mathfrak{R}$ eine Kegel-Algebra. Dann erfüllt $R\times R$ im Blick auf* (*6.31*) *Axiom* (R3).

BEWEIS.
$$\begin{aligned}&([\,a\,|\,1\,]*[\,u\,|\,v\,]):[\,c\,|\,1\,]\\ =\;&[\,a*u\,|\,(u*a)*v\,]:[\,c\,|\,1\,]\\ =\;&[\,(a*u):(c:((u*a)*v))\,|\,((u*a)*v):c\,]\\ =\;&[\,(a*u):(c:v)\,|\,(u*a)*(v:c)\,] && (6.22)\\ =\;&[\,a*(u:(c:v))\,|\,((u:(c:v))*a)*(v:c)\,] && (6.22)\\ =\;&[\,a\,|\,1\,]*[\,u:(c:v)\,|\,v:c\,]\\ =\;&[\,a\,|\,1\,]*([\,u\,|\,v\,]:[\,c\,|\,1\,])\end{aligned}$$

führt zu
$$\begin{aligned}&([\,a\,|\,b\,]*[\,u\,|\,v\,]):[\,c\,|\,d\,]\\ =\;&(([\,b\,|\,1\,]*([\,a\,|\,1\,]*[\,u\,|\,v\,])):[\,d\,|\,1\,]):[\,c\,|\,1\,]\\ =\;&([\,b\,|\,1\,]*(([\,a\,|\,1\,]*[\,u\,|\,v\,]):[\,d\,|\,1\,])):[\,c\,|\,1\,]\\ =\;&([\,b\,|\,1\,]*([\,a\,|\,1\,]*([\,u\,|\,v\,]:[\,d\,|\,1\,]))):[\,c\,|\,1\,]\\ =\;&[\,b\,|\,1\,]*(([\,a\,|\,1\,]*([\,u\,|\,v\,]:[\,d\,|\,1\,])):[\,c\,|\,1\,])\\ =\;&[\,b\,|\,1\,]*([\,a\,|\,1\,]*(([\,u\,|\,v\,]:[\,d\,|\,1\,]):[\,c\,|\,1\,]))\\ =\;&[\,b\,|\,1\,]*([\,a\,|\,1\,]*([\,u\,|\,v\,]:[\,c\,|\,d\,]))\\ =\;&([\,a\,|\,b\,]*([\,u\,|\,v\,]:[\,c\,|\,d\,]))\end{aligned}$$
□

Als nächstes erhalten wir

$$[\,a\,|\,b\,]*[\,c\,|\,d\,]=[\,1\,|\,1\,]\implies[\,c\,|\,d\,]:[\,a\,|\,b\,]=[\,1\,|\,1\,] \tag{6.32}$$

BEWEIS. Wir zeigen, dass $[\,a\,|\,b\,]*[\,c\,|\,d\,]=[\,1\,|\,1\,]$ äquivalent ist zu

$$a*c\le b:d \quad \& \quad c*a\ge d:b\,. \tag{KV}$$

Zunächst gilt die Äquivalenz von $[\,a\,|\,b\,] * [\,c\,|\,d\,] = [\,1\,|\,1\,]$ mit:

(E) $$b * (a * c) = 1 \quad \& \quad (a * c) * b \geq (c * a) * d\,.$$

Diese ist evident in einer Richtung und ergibt sich auch in der anderen Richtung problemlos. Also ist $[\,a\,|\,b\,] * [\,c\,|\,d\,] = [\,1\,|\,1\,]$ äquivalent zu (E), und wir sind am Ziel, sobald wir (KV)$\Longleftrightarrow$(E) bewiesen haben.
Sei also (E) erfüllt. Dann erhalten wir nach (6.16, 6.18) und (6.19):

$$\begin{array}{rcll}
a * c & = & (a * c) : ((d : b) * (d : ((c * a) * d))) & \\
& = & (a * c) : (((d : b) * d) : ((c * a) * d)) & \text{(R3)} \\
& \leq & (a * c) : (((b : d) * b) : ((a * c) * b)) & \text{(E)} \\
& = & (a * c) : ((b : d) * (b : ((a * c) * b))) & \text{(R3)} \\
& = & (a * c) : ((b : d) * (a * c)) & \text{(E)} \\
& \leq & b : d &
\end{array}$$

also mittels (E) $$\begin{array}{rcl}
(c * a) * (d : b) & = & ((c * a) * d) : b = 1 \\
& \rightsquigarrow & \\
c * a & \geq & d : b\,.
\end{array}$$

Sei hiernach (KV) erfüllt. Dann ergibt sich (E) vermöge:

$$\begin{array}{rcl}
b * (a * c) & \leq & b * (b : d) = 1 \\
& \& & \\
(a * c) * b \geq (b : d) * b & = & (d : b) * d \geq (c * a) * d\,.
\end{array} \qquad \square$$

(6.35)
Insbesondere erhalten wir nach (6.32) :

$$\begin{array}{rcl}
[\,a\,|\,b\,] & \equiv & [\,c\,|\,d\,]\ (\theta) \\
& :\Longleftrightarrow & \\
{[\,a\,|\,b\,] * [\,c\,|\,d\,]} = & [\,1\,|\,1\,] & = [\,c\,|\,d\,] * [\,a\,|\,b\,]\,.
\end{array}$$

Das liefert eine Kongruenzrelation vermöge

(6.36) $$[\,a\,|\,b\,]\,\theta\,[\,c\,|\,d\,] \iff a * c = b : d \;\&\; c * a = d : b\,.$$

Im Rest dieses Paragraphen wenden wir uns dem Residuationsgruppoid $\mathfrak{R}_1 := (R \times R\,, *\,, :)/\theta$ zu. Offenbar ist der erste Einbettungssatz wegen (6.25), 6.2.2 bewiesen, sobald wir gezeigt haben, dass $[\,a\,|\,b\,] : ([\,c\,|\,d\,] *$

$[\,a\,|\,b\,])$ modulo θ kongruent ist zu $[\,c\,|\,d\,] : ([\,a\,|\,b\,] * [\,c\,|\,d\,])$. Hierzu zeigen wir zunächst:

(6.37)
$$\begin{aligned}&[a\,|\,b] : \Big([c\,|\,d] * [a\,|\,b]\Big) =: [A\,|\,B]\\ = \;& [a : (d * (c * a))\,\big|\, b : (((c * a) * d) * ((a * c) * b))]\,.\end{aligned}$$

BEWEIS. Anwendung von (6.31) liefert unter Berücksichtigung von (6.11)

$$\begin{aligned} A &= a : \Big(\big(d * (c * a)\big) : \big(b : (((c * a) * d) * ((a * c) * b))\big)\Big)\\ &\;\&\\ B &= \big(b : (((c * a) * d) * ((a * c) * b))\big) : \big(d * (c * a)\big)\,. \end{aligned}$$

Und das impliziert:

$$\begin{aligned} A &= a : ((d * (c * a)) : (b : ((a * c) * b))) && (6.22)\\ &= a : (d * (c * a)) && (6.19, 6.18)\\ &\;\&\\ B &= b : (((c * a) * d) * ((a * c) * b)) && (6.24), \end{aligned}$$

was zu beweisen war. □

Weiter haben wir:

(6.38)
$$[\,a\,|\,b\,] : ([\,c\,|\,d\,] * [\,a\,|\,b\,]) \;\; \theta \;\; [\,c\,|\,d\,] : ([\,a\,|\,b\,] * [\,c\,|\,d\,])\,.$$

BEWEIS. Durch Reduktion gemäß (6.37), aus Gründen der Dualität und aufgrund von (6.32) genügt es zu zeigen:

$$\begin{aligned} & (a : (d * (c * a))) * (c : (b * (a * c)))\\ = \;& (((c : (a * c)) * c) : (b * (a * c))) && (R3), (6.25)\\ = \;& (a * c) : (b * (a * c)) && (6.16, 6.19, 6.18)\\ = \;& b : ((a * c) * b)\\ = \;& (b : ((a * c) * b)) : (d : ((c * a) * d))\\ = \;& (b : (((c * a) * d) * ((a * c) * b))) : (d : (((a * c) * b) * ((c * a) * d)))\,, \end{aligned}$$

worin die letzte Zeile aus (6.25) resultiert, wenn wir b für u, $(a * c) * b$ für x, d für v und $(c * a) * d$ für y setzen, da in diesem Falle $y : v$ gleich 1 erfüllt ist. □

Damit gilt aufgrund des allgemeinen Clan-Theorems

6. 3. 3 Das Kegel-Clan-Theorem. *Ein Residuationsgruppoid* $(R, *\,, :)$ *ist genau dann ein Kegel-Clan, wenn es eine Kegel-Algebra ist.*

6.4 Weiteres zur Produktalgebra

In diesem Abschnitt setzen wir die Untersuchungen über die korrespondierende Produktakgebra, wie wir sie oben für RR-Gruppoide schon eingeleitet hatten, für den Sonderfall des Clans fort.
Wir ergänzen als erstes 5.4.5 durch

6. 4. 1 Proposition. *Sei $\mathfrak{R}$ ein Clan. Dann erfüllt $\mathfrak{P}$ Axiom* (R2′) *und gibt es kürzbare Elemente, so existiert eine Quotientenhülle $\mathfrak{Q}$, die ihrerseits genau dann $a/b = c/d$ erfüllt, wenn es in P kürzbare Elemente x, y gibt, derart dass $ax = cy$ und $bx = dy$ erfüllt ist, und es lässt sich jede Maßfunktion μ auf $\mathfrak{R}$ fortsetzen zu einer additiven Funktion μ_1 auf $\mathfrak{Q}$ vermöge:*

$$\mu_1 : a/b \ \longrightarrow \ |\,a\,| - |\,b\,|\,.$$

BEWEIS. Existiert ein Maß, so gilt in dem korrespondierenden Verbandsgruppenkegel zunächst

$$\begin{aligned} a \leq b \ &\Longrightarrow \ \exists n \in \mathbf{N} : a^n \not\leq b \\ \text{also} \quad a^n \leq b \ \ (\forall n \in \mathbf{N}) \ &\Longrightarrow \ a = 1\,. \end{aligned}$$

Somit ist $\mathfrak{P}$ in diesem Falle kommutativ, weshalb wir ausgehen können von einem SR-Gruppoid.
Nach 5.3.1 können wir zu einem Verbandsgruppenkegel übergehen und hier definieren

$$a/b \ \theta \ c/d \iff \exists\, x, y \ : ax = cy \ \&\ bx = dy\,.$$

Dann erhalten wir eine Erweiterung des gesuchten Typs.
Als nächstes erkennen wir unmittelbar, dass μ_1 eine Funktion ist, wegen:

$$\begin{aligned} a/b = c/d \ &\Longrightarrow \ ax = cy \ \&\ bx = dy \\ &\Longrightarrow \ |a| + |x| = |c| + |y| \\ &\quad \& \quad |b| + |x| = |d| + |y| \\ &\Longrightarrow \ |a| - |b| = |c| - |d|\,. \end{aligned}$$

Schließlich gilt

$$
\begin{array}{rcl}
|a/a| & = & |a| - |a| = 0 \\
 & \& & \\
|(a/b)\cdot(c/d)| & = & |a(b*c)/d(c*b)| \\
 & = & |a| + |b*c| - |d| - |c*b| \\
 & = & |a| + |b\wedge c| + |b*c| \\
 & & -|d| - |b\wedge c| - |c*b| \\
 & = & |a| - |b| + |c| - |d| \\
 & = & |a/b| + |c/d|\,.
\end{array}
$$

Damit sind wir am Ziel □

6. 4. 2 Proposition. *Sei $\mathfrak{R}$ ein $\bigwedge$-abgeschlossener Clan. Dann ist $\mathfrak{P}$ ebenfalls $\bigwedge$-abgeschlossen.*

BEWEIS. Zunächst gilt $ab \leq c \in R \Longrightarrow ab \wedge c = (b*(a*c))*c$. Folglich kommen zu den Teilern von $c \in R$ aus $\mathfrak{R}$ in $\mathfrak{P}$ keine weiteren Teiler hinzu. Wir betrachten nun ein $S := \{s_i \,\big|\, s_i = a_i b_i \ \ (i \in I,\ \ a_i, b_i \in R)\}$ und gehen zunächst aus von $a_1 \cdot b_1 \in S \cap R_1$ und setzen:

$$a_0 := \bigwedge (a_1 \wedge a_i \cdot b_i) \quad \& \quad b_0 := \bigwedge (b_1 \wedge (a_1 * a_i \cdot b_i))\,.$$

Dann folgt *per definitionem* $a_0 \cdot b_0 \leq a_i\, b_i \ \ (i \in I)$, und es lässt sich beweisen:

$$a_0 \cdot b_0 \ = \ \bigwedge a_i \cdot b_i\,.$$

Hierzu haben wir zu zeigen, dass die Elemente $xy \in R_1$, die einerseits alle Elemente s_i teilen, andererseits auch $a_0 \cdot b_0$ teilen. Gelte also $R_1 \ni xy \leq s_i \ \ (i \in I)$. Es folgt unmittelbar $a_1 \wedge xy \leq a_0$ und $a_1 * xy \leq a_1 * a_i b_i \ \ (i \in I)$ sowie $b_1 * (a_1 * xy) = a_1 b_1 * xy = 1$, also $xy \in R_1$. Somit gilt $\alpha \,\big|\, s_i \ \ (i \in I) \Longrightarrow \alpha \in R_1$ und folglich $\alpha \,\big|\, s_i \ \ (i \in I) \Longrightarrow \alpha \,\big|\, a_0 \cdot b_0$, woraus dann die Behauptung $a_0 \cdot b_0 = \bigwedge_{i \in I} s_i$ resultiert.
Damit erhalten wir induktiv, dass $\mathfrak{P}$ $\bigwedge$-vollständig ist. □

Später werden wir uns ausführlich mit ganz-abgeschlossenen SR-Gruppoiden befassen, die ihrerseits aufs engste mit klassischen Unterstrukturen des Würfels R^ω zusammenhängen.

6. 4. 3 Definition. Ein Clan heiße vollständig ganz abgeschlossen, wenn er der Bedingung genügt:

(VGA) $\qquad \forall\, t \neq 1, a \in S^+ \ \exists\, n \in \mathbf{N} \ : \ t^n * a \not\geq t \not\leq a : t^n\,.$

6. 4. 4 Proposition. *Sei $\mathfrak{R}$ ein ganz-abgeschlossener Clan. Dann ist $\mathfrak{P}$ ebenfalls ganz-abgeschlossen.*

BEWEIS. Erneut genügt es zu zeigen, dass die betrachtete Eigenschaft sich überträgt von $\mathfrak{R}$ auf $\mathfrak{R}_1$. Seien deshalb a, b, c, d Elemente aus R und gelte in der Produktalgebra $\mathfrak{P}$ die Relation $(ab)^n \leq cd$ $(\forall n \in \mathbf{N})$. Dann folgt in $\mathfrak{P}$ weiter $a^n \leq cd$ $(\forall\ n \in \mathbf{N})$ und somit $(a^n)^n \leq cd$ $(\forall\ n \in \mathbf{N})$. Das bedeutet aber jeweils für alle $n \in \mathbf{N}$

$$\begin{array}{rcl} (c \wedge a^n)(c * a^n)a^{n-1} & \leq & (c \wedge a^n)(a^n * c)d \\ & \Rightarrow & \\ (c * a^n)a^{n-1} & \leq & (a^n * c)d \\ & \Rightarrow & \\ (c * a)^n & \leq & d \\ & \Rightarrow & \\ c & \geq & a \\ & \Rightarrow & \\ c & \geq & a^n \,. \end{array}$$

Folglich erhalten wir aus Gründen der Dualität $a = 1 = b$, also $ab = 1$. □

Als eine unmittelbare Folgerung aus 6.4.4 stellen wir noch ausdrücklich heraus:

6. 4. 5 Proposition. *Sei $\mathfrak{R}$ ganz-abgeschlossen, so ist die assoziierte Verbandsgruppe archimedisch.*

Nach 6.4.2 wissen wir, dass $\mathfrak{P}$ $\bigwedge$-abgeschlossen ist, wenn $\mathfrak{R}$ die absteigende Kettenbedingung erfüllt. Unter Anwendung von $ab \leq cd \Longrightarrow ab = uv$ mit $u \leq c$ und $v \leq d$, erhalten wir hierüber hinaus sogar:

6. 4. 6 Proposition. *Sei $\mathfrak{R}$ ein Clan, der die absteigende Kettenbedingung erfüllt. Dann erfüllt auch $\mathfrak{P}$ die absteigende Kettenbedingung.*

Als einen weiteren Satz beweisen wir:

6. 4. 7 Proposition. *Sei $\mathfrak{R}$ ein vollständig verbandsdistributiver Clan, vergleiche 2.3.2 Dann ist $\mathfrak{P}$ ebenfalls vollständig verbandsdistributiv.*

BEWEIS. Ähnlich wie in [79] kann man zeigen, dass WEINBERGs Kriterium auch in SR-Gruppoiden greift. Deshalb beschränken wir uns darauf zu zeigen, dass sich diese Bedingung fortpflanzt, d. h. darauf, zu verifizieren:

(W) $$\forall\, a\ \exists\, a^\star : a = \bigvee a_i \implies a^\star \leq a_i\ (\exists\, a_i)\,.$$

Wir zeigen, dass (W) sich fort pflanzt von $\mathfrak{R}$ auf $\mathfrak{R}_1$. Nehmen wir also an, es sei $ab = \bigvee x_i \cdot y_i\ \ (x_i, y_i \in R)$. Dann folgt

$$\begin{array}{lcl} a \wedge x_i y_i \leq a & & a \wedge x_i \cdot y_i =: u_i \in R \\ & \Longrightarrow & \\ a * x_i y_i \leq b & & a * x_i \cdot y_i =: v_i \in R\,, \end{array}$$

und wir erhalten nach den Regeln der Verbandsgruppenarithmetik

$$\begin{array}{rcl} a = a \wedge ab & = & \bigvee_{i\in I} x_i \cdot y_i \\ b = a * ab & = & \bigvee_{i\in I} x_i \cdot y_i\,, \end{array}$$

man vergleiche etwa das Kapitel über Bricks.
Somit ist jedes mit a assoziierte $a^\star \neq 1$ auch assoziiert mit ab. □

Schließlich ist es eine Sache der Routine durch Anwendung der $\bigwedge$- und $\bigvee$-Formeln, wie sie unter 6.4.2 und 6.4.7 gegeben wurden, zu zeigen, dass Obergrenzen bei Maßen mitgehen, vgl. etwa [109], kurz zu zeigen:

6. 4. 8 Proposition. *Stetige Maße auf einem Clan haben stetige Fortsetzungen auf* $\mathfrak{Q}$.

6.5 Vom Kegel zum Brick

Sei $\mathfrak{R}$ eine Kegel-Algebra, also wie wir sahen, sogar ein Kegel-Clan. Dann bildet jedes Intervall $[\,1, s\,]$ bezüglich $*$ und $:$ eine beschränkte (Unter-) Kegel-Algebra. Auf der anderen Seite werden wir sehen, dass sich jede beliebige Kegel-Algebra ausdehnen lässt zu einer 0-beschränkten Kegelagebra. Somit sind Kegelalgebren mit 0 „nicht weniger allgemein" als beliebige Kegelalgebren. Kegelalgebren mit 0 sollen im weiteren als *Brick* bezeichnet werden, da sie im Sonderfall des $\mathbf{R}^n$ einen *Quader* (im Englischen *brick)* bilden. Als eine erste Beschreibung , der wir später weitere Beschreibungen an die Seite stellen werden, geben wir:

6. 5. 1 Proposition. *Eine Algebra* $\mathfrak{B} := (B\,, *, :, 0)$ *ist ein Brick, wenn sie die Gleichungen erfüllt:*

(BR1) $$(a * a) * b \ = \ b$$

$$\text{(BR2)} \qquad b = b : (a : a)$$

$$\text{(BR3)} \qquad a * (b : c) = (a * b) : c$$

$$\text{(BR4)} \qquad a : (b * a) = (b : a) * b$$

$$\text{(BR0)} \qquad 0 : (a * 0) = a\,.$$

BEWEIS. Zunächst gilt sukzessive:

$$\begin{array}{llcl} (i) & a * a & = & ((a * a) : (b : b)) * (a * a) \\ & & = & (b : b) : ((a * a) * (b : b)) \\ (ii) & & = & b : b =: 1\,. \end{array}$$

$$\begin{array}{llcl} (iii) & a * 1 & = & a * ((a : 1) * a) \\ & & = & a * (1 : (a * 1)) \\ & & = & (a * 1) : (a * 1) \\ & & = & 1\,. \end{array}$$

$$\begin{array}{llcl} (iv) & 0 * a & = & 0 * (0 : (a * 0)) \\ & & = & (0 * 0) : (a * 0) \\ & & = & 1 \end{array}$$

$$\begin{array}{llcl} (v) & a : 0 & = & ((a : 0) * a) : 0 \\ & & = & (a : 0) * (0 : a) \\ & & = & 1\,, \end{array}$$

$$\begin{array}{llcl} (vi) & (0 : a) * 0 & = & a : (0 * a) \end{array}$$

$$\begin{array}{llcl} (vii) & a * b & = & 1 \\ & & \Longrightarrow & \\ & b : a & = & (b : (a * b)) : a \\ & & = & ((a : b) * a) : a \\ & & = & (a : b) * (a : a) \\ & & = & 1 \\ & & \rightsquigarrow & \\ & a * b = 1 & \Longrightarrow & b : a = 1\,. \end{array}$$

Somit definiert $a \geq b \Longleftrightarrow a * b = 1$ eine Partialordnung. Denn:

$$\begin{array}{rcl}
a * a & = & 1 \\
 & \& & \\
a * b = 1 = b * a & \Longrightarrow & a = a : (b * a) = (b : a) * b = b\,, \\
 & \text{und} & \\
a * b = & 1 & = b * c \\
 & \Longrightarrow & \\
a * c & = & a * ((c : b) * c) \\
 & = & a * (b : (c * b)) \\
 & = & (a * b) : (c * b) = 1\,.
\end{array}$$

Das führt uns dann zu

$$a : (b * a) = b : (a * b) = a \wedge b = (a : b) * a = (b : a) * b\,, \tag{6.53}$$

was sich nach dem Beweis zu (6.15) aus den beiden Implikationen

$$\begin{array}{lrcl}
 & a & \geq & b \\
 & & \Longrightarrow & \\
 & (b : c) * (b : a) & = & 1 \\
 & & = & ((b : c) * b) : a \\
 & & = & a * (c : (b * c)) \\
 & & = & (a * c) : (b * c) = 1 \\
\text{und} & b & \geq & c \\
 & & \Longrightarrow & \\
 & (a * b) * (a * c) & = & (a * b) * (a * (b : (c * b))) \\
 & & = & (a * b) * ((a * b) : (c * b)) = 1
\end{array}$$

ergibt. Endlich folgt hiernach:

$$\begin{array}{rcl}
(a * b) * (a * c) & = & ((a * 0) : (b * 0)) * ((a * 0) : (c * 0)) \\
 & = & (((a * 0) : (b * 0)) * (a * 0)) : (c * 0) \\
 & = & (b * a) * (b * c)\,.
\end{array}$$
□

Nach diesem axiomatischen Diskurs liefern wir als ein zweites Einbettungsergebnis:

6. 5. 2 Das Brick-Theorem. *Jeder Kegel-Clan, also auch jede Kegel-Algebra, lässt sich einbetten in einen Brick, aufgefasst als* $*, :$*-Gruppoid.*

BEWEIS. In einem ersten Schritt können wir $\mathfrak{R}$ kanonisch einbetten in einen geeignet gewählten Verbandsgruppenkegel. Daher dürfen wir annehmen, dass $\mathfrak{R}$ schon ein Verbandsgruppenkegel ist. Wir betrachten die Mengen R und $R' := R \times \{1\}$ und symbolisieren $(a, 1)$ durch a'. Dann bildet, man rechne nach, $R \cup R' =: B$ einen Brick bezüglich:

$$
\begin{array}{lcl@{\qquad\qquad}lcl}
a \circledast b & := & a * b & b \odot a & := & b : a \\
a \circledast b' & := & (b \cdot a)' & b' \odot a & := & (a \cdot b)' \\
a' \circledast b & := & 1 & b \odot a' & := & 1 \\
a' \circledast b' & := & b * a & b' \odot a' & := & b * a
\end{array}
$$

wobei $1'$ die Rolle der 0 übernimmt. □

Wir haben den Brick erklärt als eine 0-*abgeschlossene Kegel-Algebra.* Nicht gefordert wurde $a*0 = 0 : a$, doch in der soeben konstruierten Erweiterung ist dieses Gesetz zusätzlich erfüllt.

6.6 Repräsentierbarkeit

Wir wollen hier nicht allzu detailliert auf Kongruenzen eingehen, da durch den Ausdehnungssatz ein enger Zusammenhang hergestellt ist zwischen den Kongruenzen einer Kegel-Algebra und den Kongruenzen des assoziierten Kegels und da Bricks ja zur Klasse der komplementären Halbgruppen gehören. Allerdings soll nicht unerwähnt bleiben, dass Kegel-Clans natürlich *kongruenz-distributiv* sind, nicht hingegen *kongruenzvertauschbar,* man betrachte etwa die um 1 erweiterte Menge der*Primzahlen* bezüglich $a * a := 1$ und $a * b := b$ im Falle $a \neq b$.
Doch soll die Standardfrage nicht ausgeklammert werden, unter welchen Bedingungen eine Kegel-Algebra *repräsentierbar* ist, d. h. subdirekt in linear geordnete Komponenten zerfällt. Hier gilt:

6. 6. 1 Proposition. *Eine Kegel-Algebra ist repräsentierbar genau dann, wenn sie die Bedingung erfüllt:*

(C0) $$a * b \wedge a : b \;=\; 1 \;.$$

BEWEIS. Wir zeigen zunächst, dass unter der formulierten Bedingung aus $a\perp b$ die Orthogonalität $a\perp c:(c:b)$ resultiert, was sich wie folgt herleitet:

$$\begin{array}{rcl}
a\perp b & \Longrightarrow & (c:(c:a))*(a\wedge c:(c:b)) \\
& \leq & (a\wedge c)\wedge((c:(c:a))*(c:(c:b))) \\
& = & ((c:a)*c\wedge(c:a):(c:b))) \\
& = & (c:a)*(c:b)\wedge(c:a):(c:b)=1\ , \\
& \leadsto & \\
a\wedge c:(c:b) & = & a\wedge c:(c:b)\wedge c:(c:a) \\
& \leq & c:(c:(b\wedge a))=1\ .
\end{array}$$

Sei hiernach $\mathfrak{C}$ subdirekt irreduzibel. Wären dann a und b unvergleichbar, so enthielten die Mengen $U:=a^{\perp}$ aller zu a orthogonalen Elemente und $V:=U^{\perp}$ aller zu jedem $u\in U$ orthogonalen Elemente mit jedem $x*y$ auch $y:(y:(x*y))=y:x$, und das lieferte uns zwei id-disjunkte Kongruenzen, ein Widerspruch!

Denn setzen wir $a\equiv_U b:\Longleftrightarrow a*b, b*a\in U$, so folgen

$$\begin{array}{rrcl}
& b\equiv_U c & \Longrightarrow & (a*b)*(a*c)=(b*a)*(b*c)\in U \\
& & \Longrightarrow & a*b\equiv_U a*c \\
\text{und} & a\equiv_U b & \Longrightarrow & (a*c):(b*c)=a*((c:(b*c))\in U \\
& & \Longrightarrow & (a*c)*(b*c)\in U \\
& & \Longrightarrow & a*c\equiv_U b*c\,.
\end{array}$$

Damit ist aus Gründen der Dualität alles gezeigt. □

Der Leser beachte noch, dass (C0) in Verbandsgruppenkegeln gleichbedeutend ist mit $(a\wedge b)^2=a^2\wedge b^2$,

WEGEN:

$$\begin{array}{ccc}
x*y & \perp & x:y \\
& \Longleftrightarrow & \\
(b*a)(a:b) & \perp & (a*b)(b:a) \\
& \Longleftrightarrow & \\
(a\wedge b)^2 & = & a^2\wedge b^2
\end{array}$$

und auch mit $(a\vee b)^2=a^2\vee b^2$,

WEGEN:

$$\begin{array}{rcl}
a * b \perp a : b & \Longrightarrow & (b * a)(a : b) \perp (a * b)(b : a) \\
& \& & \\
a \perp b \Longleftrightarrow a * b = b & \Longleftrightarrow & a(a * b) = a \vee b = a \cdot b \\
& & \\
& \Downarrow & \\
& & \\
a * b & \perp & a : b \\
& \Longrightarrow & \\
(b * a)(a * b)(a : b)(b : a) & = & (b * a)(a : b) \vee (a * b)(b : a) \\
& \Longleftrightarrow & \\
(a \vee b)^2 & = & a^2 \vee b^2 \\
& \& & \\
(a \vee b)^2 & = & a^2 \vee b^2 \\
& \Longrightarrow & \\
(b * a)(a * b)(a : b)(b : a) & = & (b * a)(a : b)(b : a) \\
& \vee & (b * a)(a * b)(b : a) \\
& \Longrightarrow & \\
(a * b)(a : b) & = & (a : b) \vee (a * b) \\
& \Longrightarrow & \\
a * b & \perp & a : b\,.
\end{array} \qquad \square$$

6.7 Schwache Kegelalgebren

In diesem Abschnitt wollen wir ein wenig Axiomatik betreiben.

6. 7. 1 Definition. Unter einer schwachen Kegelalgebra verstehen wir eine Algebra $\mathfrak{C} := (C, *, :)$ vom Typ $(2, 2)$, die den Bedingungen genügt:

$$\begin{array}{llcl}
(\mathrm{E}^*) & (a * a) * b & = & b \\
(\mathrm{E}^:) & b & = & b : (a : a) \\
(\mathrm{R3}) & a * (b : c) & = & (a * b) : c \\
(\mathrm{R4}) & a : (b * a) & = & (b : a) * b\,.
\end{array}$$

Aus (E^*),$(\mathrm{E}^:)$ und (R4) folgt sofort $a * a = b * b$ & $a : a = b : b$, was nach sich zieht

$$\begin{array}{lrcl}
(6.59) & a * a = b * b =: & 0 & = a : a = b : b \\
(6.60) & b * a = 0 & \Leftrightarrow & a : b = 0\,,
\end{array}$$

die letzte Gleichung, da aus $a * b = 1$ resultiert:

$$a = (b : (a * b)) : a = ((a : b) * a) : a = (a : b) * (a : a) = 1\,.$$

Hiernach folgt dann weiter, dass $a \geq b \Longleftrightarrow a{*}b = 0$ eine inf-abgeschlossene Partialordnung mit Minimum 0 liefert, man beachte $a{*}0 = a{*}(0 : (a{*}0)) = (a{*}0) : (a{*}0) = 0$. Somit kann die schwache Kegelalgebra betrachtet werden als Verallgemeinerung vom Typ $(2, 2)$ der kommutativen BCK-Algebra, die definiert ist vermöge:

$$\begin{array}{llcl}
\text{(BCK1)} & 0 * x & = & x \\
\text{(BCK2)} & x * 0 & = & 0 \\
\text{(BCK3)} & a * (b * c) & = & b * (a * c) \\
\text{(BCK4)} & (a * b) * b & = & (b * a) * a\,.
\end{array}$$

In [67] wird eine relative Kürzungseigenschaft (RCP) für kommutative BCK-Algebren vorgestellt und auf dem Wege über mehrere äquivalente Eigenschaften diskutiert. Allerdings haben die Autoren die Gleichung

$$\text{(W}^*\text{)} \qquad (a * b) * (a * c) \;=\; (b * a) * (b * c)$$

ausgespart. Aus diesem Grund sei in diesem Abschnitt das Versäumnis ausgeglichen. Genauer zeigen wir:

6. 7. 2 Proposition. *Sei $\mathfrak{C}$ eine schwache Kegelalgebra dann sind die folgenden Aussagen, jeweils erweitert durch ihre Dualen, paarweise äquivalent:*

$$\begin{array}{llcl}
\text{(RCP)} & a \leq b, c \;\&\; a * b & = & a * c \Longrightarrow b = c \\
\text{(NOR)} & (a * b) \wedge (b * a) & = & 1 \\
\text{(RCO)} & (a * b) * (b * a) & = & b * a \\
\text{(D I S)} & a * (b \wedge c) & = & a * b \wedge a * c \\
\text{(RES)} & (a * b) * (a * c) & = & (b * a) * (b * c)\,.
\end{array}$$

BEWEIS. (RCP)$\Longrightarrow$ (NOR). Nach (RCP) ist $a * d = b$ im Falle $a \leq d$ eindeutig bestimmt. Daher dürfen wir die Bezeichnung $ab := d$ wählen –

ohne hiermit ein Produkt im Sinn zu haben. Dies vor Augen erhalten wir zunächst:

$$\text{(6.71)} \qquad \begin{aligned} & a \leq d \;\&\; ab = d \\ \Longrightarrow\; & a * (d : (c * b)) = (a * d) : (c * b)) = b : (c * b) = b \wedge c \end{aligned}$$

was bedeutet, dass mit ab auch $a(b \wedge c)$ existiert. Hieraus resultiert dann weiter:

$$\text{(6.72)} \qquad \begin{array}{rcl} a * (ab \wedge ac) & \leq & a * ab \wedge a * ac \\ & = & b \wedge c \\ & = & a * a(b \wedge c) \\ & \leq & a * (ab \wedge ac) \\ & \Longrightarrow & \\ a * a(b \wedge c) & = & a * (ab \wedge ac) \\ & \Longrightarrow & \\ a(b \wedge c) & = & ab \wedge ac \end{array}$$

und damit

$$\text{(6.73)} \qquad a \leq b, c \Longrightarrow a * (b \wedge c) = a * b \wedge a * c\,,$$

also

$$\text{(NOR)} \qquad a * b \wedge b * a = (a \wedge b) * (a \wedge b) = 1\,.$$

(NOR)$\Longleftrightarrow$(RCO), man beachte

$$(a * b) * (b * a) = ((a * b) \wedge (b * a)) * (b * a)$$

und $x \wedge y = (x : y) * x$.

(NOR)$\Longrightarrow$(DIS), da aus $b \wedge c = c : (b * c)$ resultiert:

$$\begin{array}{rl} & (a * (b \wedge c)) * (a * b \wedge a * c) \\ \leq & ((a * (b \wedge c)) * (a * b)) \wedge ((a * (b \wedge c)) * (a * c)) \\ = & ((a * (b : (c * b)) * (a * b)) \wedge ((a * (c : (b * c)) * (a * c)) \\ = & (((a * b) : (c * b)) * (a * b)) \wedge (((a * c) : (b * c)) * (a * c)) \\ \leq & (c * b) \wedge (b * c) \\ = & 1 \\ \Longrightarrow & a * (b \wedge c) \geq (a * b \wedge a * c) \;\; (\geq a * (b \wedge c)) \end{array}$$

(DIS)$\Longrightarrow$(RES). Sei zunächst $\mathfrak{C}$ beschränkt mit Spitze 0. Dann folgt:

$$\begin{aligned}(a*b)*(a*c) &= ((a*0):(b*0))*((a*0):(c*0))\\ &= (((a*0):(b*0))*((a*0)):(c*0))\\ &=: f(a,b,c) = f(b,a,c)\\ &= (b*a)*(b*c)\,.\end{aligned}$$

Hieraus folgt dann allgemein

$$\begin{aligned}(a*b)*(a*c) &= ((a*b)\wedge(a*c))*(a*c)\\ &= (a*(b\wedge c))*(a*c)\\ &= ((a\wedge c)*(b\wedge c))*((a\wedge c)*c)\\ &=: g(a,b,c) = g(b,a,c)\\ &= (b*a)*(b*c)\end{aligned} \tag{6.75}$$

(RES)$\Longrightarrow$(RCP). Wir gehen aus von $a \leq b, c$ und $a*b = a*c$. Dann folgt $b*c = (b*a)*(b*c) = (a*b)*(a*c) = (a*b)*(a*b) = 1$, also $b \geq c$, und – aufgrund der Dualität – $c \geq b$. □

ZUSAMMENFASSEND erhalten wir damit aufgrund der Symmetrie, dass schwache Kegelalgebren genau dann Kegelalgebren sind, wenn sie eine der Bedingungen (RCP),...,(RES) zusammen mit deren Dualem erfüllen.

6.8 ℓ-Gruppen-Clans

Betrachten wir $(\mathbf{Z}, +, \min)$, so bildet etwa $\{0, 1, 2\}$ einen ℓ-Gruppen-Clan, doch auch $\{-1, 0, 1, 2\}$ ist in kanonischer Weise eingebettet in $(\mathbf{Z}, +, \min)$. Es sind diese Strukturen, die wir nun genauer anschauen wollen. Man beachte, im alltäglichen Rechnen bewegen wir uns in Clans. Spätestens nach Beendigung einer Kalkulation wird dies ja deutlich. Der Vorrat an Zahlen reicht für jede Rechnung, dennoch, im Konkreten waren am Ende stets nur endlich viele im Spiel.

6. 8. 1 Proposition. *Sei $\mathfrak{C} := (C, *, :)$ ein ℓ-Gruppen-Kegel-Clan. Dann gilt in $\mathfrak{C}$ bezüglich der Festsetzung:*

$$x = ab :\Longleftrightarrow a*x = b \ \&\ x:b = a$$

das System der Axiome:

(C1) $$a \leq b \implies \exists x, y : b = ax \ \&\ b = ya$$

$$
\begin{array}{lrcl}
\text{(C2)} & ax, ay \in C \;\&\; ax = ay & \Longrightarrow & x = y \\
 & xa, ya \in C \;\&\; xa = ya & \Longrightarrow & x = y \\
\text{(C3)} & ax, ay \in C & \Longrightarrow & ax \wedge ay = a(x \wedge y) \\
 & xa, ya \in C & \Longrightarrow & xa \wedge ya = (x \wedge y)a \\
\text{(C4)} & ab \in C \;\&\; (ab)c \in C & \Longrightarrow & bc \in C \;\&\; a(bc) = a(bc) \\
\text{(C5)} & (a \wedge b)c = c \;\&\; a \vee b \in C & \Longrightarrow & ab = a \vee b = ba\,.
\end{array}
$$

BEWEIS. (C1), (C2), (C3), (C5) folgen aus der Einbettung des Kegel-Clans in den Kegel und aus der Arithmetik der ℓ-Gruppe. Folglich bleibt zu zeigen, dass die oben definierte partielle Multiplikation auch Axiom (C4) erfüllt. Hier erhalten wir vorab $y = uv \;\&\; w \leq v \Longrightarrow uw \in C \;\&\; uw \leq uv$, wegen:

$$
\begin{array}{rl}
 & x * (y : (w * v)) = (u * y) : (w * v) = v : (w * v) = w \\
\& & (y : (w * v)) : w = (y : (w * v)) : (v : (w * v)) = y : v = u
\end{array}
$$

Nun ist aber ab eine obere Schranke zu a, und es bedingt die Existenz von $(ab)c$ die Existenz von bc. Ferner haben wir $(ab)c = u(bc)$ $(\exists u \in C)$. Das führt dann wegen

$$
\begin{array}{rcl}
x : bc & = & (x : bc) : (b * (bc : bc)) \\
 & = & (x : bc) : ((b * bc) : bc) \\
 & = & (x : bc) : (c : bc) \\
 & = & (x : c) : (bc : c) \\
 & = & (x : c) : b
\end{array}
$$

weiter zu

$$u = u(bc) : bc = (ab)c : bc = ((ab)c) : c) : b = ab : a = a\,.$$

Damit ist aus Gründen der Dualität alles gezeigt. □

Den letzten Satz nehmen wir zum Anlass einer Abschwächung des ℓ-Gruppen-Kegel-Clans. In [29] wurde diese Abschwächung als Semiclan eingeführt und studiert, doch scheint das Bezeichnungspaar ℓ-Gruppen-Clan, ℓ-Gruppen-Kegel-Clan, angemessener als das Paar ℓ-Gruppen-Clan, Semiclan, da es das Fehlen der Positivität nicht negativ herausstellt, sondern die Anwesenheit von Positivität positiv betont.

6. 8. 2 Definition. Sei $\mathfrak{C} := (C, \wedge, \cdot)$ ein Halbverband bezüglich $\wedge$ und ein partielles Gruppoid bezüglich $\cdot$. Dann heiße $\mathfrak{C}$ ein ℓ-Gruppen-Clan [1)], falls $\mathfrak{C}$ die Axiome (C1) bis (C5) erfüllt.

[1)] In [29] bezeichnet als Semiclan

Durch Axiom (C2) sind Links- und Rechtsquotienten eindeutig bestimmt. Somit macht es Sinn zu definieren:

$$a = c/b :\Longleftrightarrow ab = c \Longleftrightarrow: a\backslash c = b\,. \tag{6.81}$$

Als unmittelbare Folgerungen erhalten wir dann:

$$a/a = b/b \;=\; a\backslash a = b\backslash b \tag{6.82}$$

BEWEIS. $a\backslash a$ und $b\backslash b$ sind definiert, da $a \leq a$ und $b \leq b$ erfüllt sind. Bezeichne nun mit 1 das eindeutig bestimmte Element $(a \wedge b)\backslash(a \wedge b)$. Dann sind $a(a/(a \wedge b))(a \wedge b)$ und $(a \wedge b)1$ definiert, so dass wir schließen können:

$$a(a\backslash a) = (a/(a \wedge b))((a \wedge b)1) = ((a/(a \wedge b))(a \wedge b))1 = a1\,.$$

Dies liefert dann eine eindeutig bestimmte Rechtseins und dual eine eindeutig bestimmte Linkseins, also eine eindeutig bestimmte Eins. □

Als eine unmittelbare Folgerung erhalten wir nach Axiom (C4), dass sich die Elemente der Form $1 \wedge a$ mit allen Elementen multiplizieren lassen wegen der Implikation $x(1 \wedge a) = 1 \Longrightarrow x(1 \wedge a) \cdot y = x \cdot (1 \wedge a) = y \in C$. Da der ℓ-Gruppen-Clan offenbar rechts-/links-dual erklärt ist, gelten die nachfolgenden Sätze jeweils zusammen mit ihren dualen Versionen.

6. 8. 3 Lemma. *Ist ay erklärt und gilt $x \leq y$, so ist auch ax erklärt.*

DENN: Es ist ay erklärt, und es gilt $y = xz$ $(\exists z \in C)$. Also ist nach (C4) auch ax erklärt. □

Ist ax definiert, so folgt

$$a \leq ax \iff 1 \leq x\,. \tag{6.83}$$

DENN:
$$\begin{aligned} a \leq ax &\iff a = a1 \wedge ax = a(1 \wedge x) \\ &\iff 1 = 1 \wedge x \\ &\iff 1 \leq x\,. \end{aligned}$$ □

Sind ax und ay erklärt, so haben wir:

$$a \leq ax \iff ax \leq ay \tag{6.84}$$

DENN: Gilt die linke Seite, so resultiert:

$$x \leq y \implies ax = a(x \wedge y) = ax \wedge ay$$

und weiter folgt:
$$\begin{aligned} ax \le ay &\Longrightarrow ay = (ax)z = a(xz) \ \ (z \ge 1) \\ &\Longleftrightarrow xz = y \\ &\Longrightarrow x \le y \end{aligned}$$
□

Mit (a/x) und $(a/x)/y$ ist auch yx erklärt, und wir erhalten:

(6.85) $$(a/x)/y \ = \ a/(yx)$$

DENN:
$$\begin{aligned} (a/x)/y = b &\Longleftrightarrow a/x = by \\ &\Longleftrightarrow a = (by)x \\ &\Longleftrightarrow a = b(yx) \\ &\Longleftrightarrow b = a/(yx)\,. \end{aligned}$$
□

Ist a/b erklärt, so gilt offenbar:

(6.86) $$(a/b)\backslash a \ = \ b\,.$$

Sind a/x und a/y erklärt, so gilt:

(6.87) $$a/x \ge a/y \Longleftrightarrow x \le y\,.$$

DENN:
$$\begin{aligned} a/x \ge a/y &\Longrightarrow (a/y)z = a/x \ \ (\exists z \ge 1) \\ &\Longrightarrow a/y = (a/x)z \\ &\Longrightarrow (a/y)\backslash a = (a/(zx))\backslash a \\ &\Longrightarrow y = zx \ \ (z \ge 1) \\ &\Longrightarrow y \ge z \\ &\Longrightarrow (a/y)y = ((a/y)z)x \\ &\Longrightarrow a/x = (a/y)z \ \ (z \ge 1) \\ &\Longrightarrow a/x \ge a/y\,. \end{aligned}$$
□

Weiter können wir zeigen:

(6.88) $$c \ge a, b \Longrightarrow ((c/a) \wedge (c/b))\backslash c = a \vee b\,.$$

DENN:
$$\begin{aligned} c \ge z \ \&\ z \ge a \ \&\ z \ge b &\Longrightarrow c/z \le c/a \ \&\ c/z \le c/b \\ &\Longrightarrow c/z \le (c/a) \wedge (c/b) \\ &\Longrightarrow z \ge ((c \wedge a) \wedge (c/b))\backslash c\,, \end{aligned}$$

man beachte (6.87). □

(6.89) $$c/((c \wedge x) \vee (c \wedge y)) \ = \ c/(c \wedge x) \wedge c/(c \wedge y)\,.$$

DENN: (6.88) impliziert:

$$\begin{aligned} c/((c \wedge x) \vee (c \wedge y) &= c/((c/(c \wedge x) \wedge (c/(c \wedge y))\backslash c) \\ &= c/((c \wedge x) \wedge c/(c \wedge y))\,. \end{aligned}$$ □

(6.90) $$c \geq a, b \;\&\; a \wedge b = 1 \implies ab, ba \in C \;\&\; ab = ba\,.$$

DENN: nach (2.57) und (C5) sind ab und ba gleich $a \vee b$. □

Im folgenden setzen wir $a^- := 1 \wedge a$, $a^+ = 1 \vee a$ und $a^* := a^-\backslash 1$. Als spezielle Resultate erhalten wir dann für diese Elemente:

(6.91) $$a^*(1 \wedge a) = 1 \quad \& \quad a^+(1 \wedge a) = a\,.$$

DENN: $$\begin{aligned} &a^* = a^*(1 \wedge a)a^* \implies a^*(1 \wedge a) = a, \\ \& \quad &a^+(1 \wedge a)a^* = (1 \wedge a)a^*a^+ = (1 \wedge a)a^+a^* \end{aligned}$$ □

So wie oben erhalten wir hiernach, dass die Elemente vom Typ a^* mit allen Elementen multiplizierbar sind und damit insbesondere, dass alle $a^* \vee b^*$ existieren. Das liefert dann weiter die Formel

(6.92) $$a^* \vee b^* = (a \wedge b)^*\,.$$

DENN: Nach (C3) ist $(a \wedge b)(a^* \vee b^*) \geq 1$, also $(a^* \vee b^*) \geq (a \wedge b)^*$ und nach (2.54) haben wir $a^*, b^* \leq (a \wedge b)^*$ □

Insbesondere erhalten wir hiernach:

(6.93) $$a^+ \wedge a^* = 1\,.$$

DENN: $a^+(1 \wedge a) = 1 \;\&\; a^*(1 \wedge a) = 1 \implies (a^+ \wedge a^*)(1 \wedge a) = 1 \wedge a$. □

Weiter resultiert:

(6.94) $$a^+/a^* = a = a^*\backslash a^+\,.$$

Sei ab erklärt, dann ist auch ab^+ erklärt, und es gilt

(6.95) $$ab^+ = (ab)b^*\,.$$

DENN: nach Voraussetzung gilt: $ab = a(b^+(1 \wedge b)) = (ab^+)(1 \wedge b)$ □

Als nächstes erhalten wir:

(6.96) $$a/(a \wedge b) \wedge b/(a \wedge b) = 1$$

DENN:
$$\begin{aligned} a \wedge b &= (a/(a \wedge b))(a \wedge b) \wedge (b/(a \wedge b))(a \wedge b) \\ &= (a/(a \wedge b)) \wedge b/(a \wedge b))(a \wedge b)\,. \end{aligned}$$
□

Im weiteren betrachten wir den Positivbereich $C^+ := \{x \,\big|\, x \geq 1\}$. Wir werden zeigen, dass dieser Anteil bezüglich $a * b := (a \wedge b)\backslash b$ und $b : a := b/(a \wedge b)$ einen ℓ-Gruppen-Kegel bildet. Das Hauptproblem wird dabei sein, die Bedingungen (C11) und (C3) nachzuweisen, wohingegen die übrigen Axiome fast evident sind.
Sei bc definiert. Dann gilt

(6.97)
$$a \wedge bc \;=\; a \wedge (a \wedge b)c$$

BEWEIS. Im Sonderfall $a \wedge b = 1$ erhalten wir zunächst:
$$\begin{aligned} a \wedge bc = y &\Longrightarrow b \wedge y = 1 \;\&\; y \leq bc \\ &\Longrightarrow b \vee y = by \leq bc \\ &\Longrightarrow y \leq c\,. \end{aligned}$$
also
$$a \wedge bc \leq a \wedge c \leq a \wedge bc$$

Sei hiernach $a \wedge b$ beliebig gewählt. Dann folgt:
$$\begin{aligned} a \wedge bc &= (a \wedge b)((a \wedge b)\backslash a) \wedge (a \wedge b(((a \wedge b)\backslash b)c) \\ &= (a \wedge b)(((a \wedge b)\backslash a) \wedge ((a \wedge b)\backslash b)c)) \\ &= (a \wedge b)((a \wedge b)\backslash a) \wedge c) \;\; (\text{s. o.}) \\ &= a \wedge ((a \wedge b)c)\,. \end{aligned}$$

Damit sind wir am Ziel □

Insbesondere haben wir damit

(6.98)
$$a \wedge bc \;\leq\; (a \wedge b)c$$

(6.99)
$$a \leq bc \;\&\; a \wedge b = 1 \;\Longrightarrow\; a \leq c\,.$$

Weiter liefert Anwendung von (6.97)

(6.100)
$$x/(x \wedge y) \;\geq\; (x \wedge z)/(x \wedge y \wedge z)$$

DENN:
$$\begin{aligned} s(x \wedge y) = x &\Longrightarrow s(x \wedge y \wedge z) \geq x \wedge z \;\; ((6.101)) \\ &\Longrightarrow s = x/(x \wedge y) \geq (x \wedge z)x/(x \wedge y \wedge z) \end{aligned}$$
□

Damit gilt als nächstes:

(6.101)
$$c/(a \wedge b) \wedge b/(\wedge b) \;=\; (b \wedge c)(a \wedge b \wedge c)$$

DENN: die linke Seite enthält die rechte nach (6.100) und die rechte Seite enthält die linke wegen:

$$(c/(a \wedge c) \wedge b/(a \wedge b)) \cdot (a \wedge b \wedge c) \leq b \wedge ec\,. \qquad \square$$

Schließlich erhalten wir:

$$c = a \vee b \implies c = a((a \wedge b)\backslash b)\,. \tag{6.102}$$

DENN:

$$\begin{array}{rcll} x \geq a & \& & x \geq b & \\ & \Rightarrow & & \\ x = ay & \geq & b & (\exists y \geq 1) \\ & \Rightarrow & & \\ (a \wedge b)((a \wedge b)\backslash a)y & \geq & (a \wedge b)((a \wedge b)\backslash b) & \\ & \Rightarrow & & \\ ((a \wedge b)\backslash a)y & \geq & (a \wedge b)\backslash b & \\ & \Rightarrow & & \\ y & \geq & (a \wedge b)\backslash b & ((6.91), (6.94)) \\ & \Rightarrow & & \\ x = ay & \geq & a((a \wedge b)\backslash b)\,. & \end{array} \qquad \square$$

Nun sind wir in Lage zu zeigen:

6. 8. 4 Proposition. *Ist $\mathfrak{C}$ ein ℓ-Gruppen-Clan, so bildet C^+ einen Kegel bezüglich*

$$a * b := (a \wedge b)\backslash b \ \ \textit{und} \ \ b : a := b/(a \wedge b) \tag{6.103}$$

BEWEIS. Axiom (C21) gilt, denn nach (6.95), (6.96) und (2.56) folgt

$$\begin{array}{rcl} (b \wedge c) \vee (a \wedge c) & = & (a \wedge c)((a \wedge b)\backslash b \wedge (a \wedge c)\backslash c) \\ & \Rightarrow & \\ ((b \wedge c) \vee (a \wedge c))\backslash c & = & ((a \wedge c)((a \wedge b)\backslash b \wedge (a \wedge c)\backslash c))\backslash c \\ & \Rightarrow & \\ ((b \wedge c) \vee (a \wedge c))\backslash c & = & ((a \wedge b\backslash b) \wedge (a \wedge c)\backslash c))\backslash((a \wedge c)\backslash c) \\ & = & (a * b \wedge a * c)\backslash(a * c) \\ & = & (a * b) * (a * c) \\ & = & (b * a) * (b * c)\,, \end{array}$$

da die linke Seite a, b-symmetrisch ist.

Analog erhalten wir Axiom (C11) . Weiterhin sind (C12) und (C22) evident, und es ist (C4) eine unmittelbare Konsequenz aus (6.91). Damit bleibt nur noch (C3) zu verifizieren. Hier gilt zunächst unmittelbar:

$$\begin{aligned} a * (b : c) &= (a \wedge (b : c)) * (b : c) \\ &= ((a \wedge b) \wedge (b : c)) * (b : c) \\ &= (a \wedge b) * (b : (b \wedge c)) . \end{aligned}$$

Daher dürfen wir ausgehen von $a, c \leq b$. Dann ist $a(a * b)$ und damit auch $a((a * b) : c)$ definiert. Deshalb können wir schließen:

$$\begin{aligned} a((a * b) : c)((a * b) \wedge c = a \ \vee \ b &\geq (b : c)((a * b) \wedge c) \\ &\Rightarrow \\ a((a * b) : c) &\geq b : c \\ &\Rightarrow \\ a((a * b) : c) &\geq a \wedge (b : c) \\ &= a(a * (b : c)) \\ &\Rightarrow \\ (a * b) : c) &\geq (a * b) : c . \end{aligned}$$

Damit sind wir aus Gründen der Dualität am Ziel. □

Hiernach kommen wir zum Hauptergebnis dieses Kapitels.

6. 8. 5 Theorem. *Sei $\mathfrak{C}$ ein ℓ-Gruppen-Clan und sei ϕ^+ eine Funktion, die $(C^+, *, :)$ - betrachtet als Kegel - einbettet in einen Verbandsgruppenkegel. Dann lässt sich ϕ^+ ausdehnen zu einer Funktion ϕ , die $\mathfrak{C}$ - als ℓ-Gruppen-Clan - supremumtreu einbettet in die korrespondierende ℓ-Gruppe $\mathfrak{G}$.*

BEWEIS. Wir schreiben in diesem Beweis die existierenden Produkte von $\mathfrak{C}$ als Summen $a + b$ etc. und die Suprema und Infima aus $\mathfrak{G}$ als $a \cup b$ bzw. $a \cap b$ und definieren:

$$\phi(a) := \phi^+(a^+) \cdot (\phi^+(a^*))^{-1} .$$

Dann folgt:

$$\begin{aligned} a^+ \wedge a^* &= 0 \\ &\Rightarrow \\ \phi(a^+) \cap \phi(a^*) &= 1 \\ &\Rightarrow \\ \phi(a^+) \cdot (\phi(a^*))^{-1} \cap 1 &= (\phi(a^*))^{-1} \end{aligned}$$

$$\begin{array}{rcl}\phi(a^+)\cdot(\phi(a^*))^{-1}\cap 1 &=& (\phi(a^*))^{-1}\\ \rightsquigarrow \quad (\phi(a^*))^{-1} &=& \phi(a)\cap 1\\ &\Rightarrow& \\ \phi(a^*) &=& (\phi(a))^*\,,\end{array}$$

und damit weiter:

$$\begin{array}{rcl}\phi(a^+) &=& \phi(a^+)(\phi(a^*))^{-1}\phi(a^*)\\ &=& \phi(a)\cdot\phi(a^*)\\ &=& \phi(a)\cdot(\phi(a))^*\\ &=& (\phi(a))^+\end{array}$$

(i) Anwendung dieser beiden letzten Formeln führt uns dann weiter zu:

$$\begin{array}{rcll}\phi(a)\cap\phi(b) &=& \phi(a^+)(\phi(a^*))^{-1}\cap\phi(b^+)(\phi(b^*))^{-1} & \\ &=& ((\phi(a^+)\cap(\phi(b))^+)\cdot((\phi(a))^*\cup(\phi(b))^*)^{-1} & \\ &=& (\phi(a^+)\cap(\phi(b))^+)\cdot(\phi(a^*)\cup(\phi(b^*))^{-1} & \\ &=& (\phi(a^+\wedge b^+))\cdot(\phi(a^*\vee b^*))^{-1}, & \\ &=& (\phi((a\wedge b)^+))\cdot(\phi(a\wedge b)^*)^{-1} & ((6.92))\\ &=& \phi(a\wedge b)\,. & \end{array}$$

(ii) Sei nun $a+b^+=x$ in $\mathfrak{C}$. Dann folgt:

$$\begin{array}{rcl}a+b^+=x^+/x^* &\Longrightarrow& a^*\backslash a^++b^+=x^+/x^*\\ &\Longrightarrow& a^++b^+=a^*+x^+/x^*\\ &\Longrightarrow& a^++b^++x^*=a^*+x^+\\ &\Longrightarrow& (\phi(a))\cdot(\phi(b^+))=\phi(x)\,,\end{array}$$

woraus sich weiter ergibt:

$$\begin{array}{rcll}a+b=c &\Longrightarrow& (a+b^+)/b^*=c & ((6.91))\\ &\Longrightarrow& \phi(a)\cdot\phi(b^+)=\phi(c)\cdot\phi(b^*) & \\ &\Longrightarrow& \phi(a)\cdot\phi(b^+)\cdot((\phi(b^*))^{-1}=\phi(c) & \\ &\Longrightarrow& \phi(a)\cdot\phi(b)=\phi(c) & \end{array}$$

(iii) Schließlich gilt für existierende $a\cup b$:

$$\phi(a)\cup\phi(b) \;=\; \phi(a\vee b)\,,$$

denn diese Gleichung folgt unmittelbar aus $(i),(ii)$ und (6.102). $\square$

Kapitel 7

Sup-Clans

7.1 Vorbemerkungen

Wie schon im Kapitel über Residuationsgruppoide angekündigt, werden wir uns nun den brouwerschen und den booleschen Clans zuwenden. Die Vorgehensweise ist ähnlich der oben praktizierten.
Um von einer möglichst allgemeinen Basis zu starten, werden wir ausgehen von *dualen Residuationsgruppoiden,* kurz *DR-Gruppoiden.* Sie sind als Residuationsstruktur abgehoben von der Struktur der komplementären Halbgruppe. Allerdings wird es uns nicht gelingen, den Clan der komplementären Halbgruppe zu charakterisieren. Während dies im rechtskomplementären Fall in überraschend erfreulicher Weise gelang, stellen sich hier ganz wesentliche Hindernisse in den Weg. Zwar erhalten wir natürlich eine $*$ - Erweiterung im Sinne des allgemeinen Clan-Theorems 5.2.12 und ebenso eine :-Erweiterung, es ist aber nicht zu erkennen, wie diese beiden Ausdehnungen in eins geführt werden könnten. Ein Hauptproblem: es gibt keinen Hinweis auf eine Formel der Art $a * bc = f \cdot g$ mit $*$, :-Polynomen f, g. Andererseits ist natürlich nicht auszuschließen, dass sich eine Lösung auf dem Wege einer geschickten „Verschmelzung" der beiden genannten einseitigen Erweiterungen anbietet.
So bleibt uns zunächst nur eine Untersuchung der Residuationsarithmetik in DR-Gruppoiden, um auf ihrer Grundlage in einem ersten Schritt, ausgehend von einem $\mathfrak{R}$ zu einem $\vee$-abgeschlossenen $\mathfrak{S}$ zu gelangen. Dies wird möglich sein über die Formel

$$\text{(V)} \qquad (a \vee b) * (c \vee d) \;=\; ((a * b) * (a * c)) \vee ((a * b) * (a * d))$$

Doch obwohl diese Formel auf den ersten Blick sehr „griffig" erscheint, erweist sich schon das allgemeine Problem der Einbettung eines DR-Gruppoids $\mathfrak{R}$ in ein $\vee$-abgeschlossenes $\mathfrak{S}$ als sehr technisch, und dies gilt erst recht für Fragen der Vererbung gewisser algebraischer Merkmale.

Nach diesem Schritt wenden wir uns den so genannten *normalen* DR-Gruppoiden zu, also den DR-Gruppoiden mit $a * b \perp b * a$. Nicht ganz überraschend stellt sich hier als erstes ein, dass diese Bedingung die duale Bedingung $b : a \perp a : b$ nach sich zieht. Dies führt natürlich zu technischen Erleichterungen in späteren Beweisführungen. Dass wir in diesem Abschnitt zu vielen Formeln der bereits bekannten Arithmetik komplementärer Halbgruppen gelangen, versteht sich von selbst, und natürlich hätten wir Teile jenes Kapitels durch dieses Kapitel ersetzen können. Es schien aber, als sei diese Überlappung von der Organisation des Stoffes her vertretbar.

Wie sich herausstellt, besitzen normale DR-Gruppoide sogar einen normalen $\vee$-Abschluss, und dies wird der Ausgangspunkt beim Studium boolescher Clans sein.

Engen wir DR-Gruppoide ein vermöge der Forderung

$$\text{(B)} \qquad a * (b * c) \;=\; (a * b) * (a * c)\,,$$

so gelangen wir zum Clan des brouwerschen Halbverbandes.

Dies führt uns zum Clan des booleschen Ringes, der als weiteres Gesetz die Gleichung respektiert;

$$\text{(S)} \qquad (a * b) * b \;=\; (b * a) * a\,,$$

Abschließend zeigen wir, wie sich ein boolescher Ring konstruktiv in einen booleschen Verband einbetten lässt. Dabei gehen wir ähnlich vor, wie bei der Konstruktion der Brick-Erweiterung für Verbandsgruppenkegel.

7.2 Arithmetik der DR-Gruppoide

Wie in der Einleitung angekündigt, starten wir in diesem Kapitel so allgemein wie möglich, ausgehend von evidenten Residuationsgesetzen der komplementären Halbgruppe. Dabei streben wir weniger Unabhängigkeit der Beschreibung als evidente Selbstdualität an.

Um es zu betonen: Wir legen in 7.2.1 vorrangig Wert auf Evidenz und Transparenz.

7. 2. 1 Definition. Eine Algebra $\mathfrak{R} = (R, *, :)$ vom Typ (2,2) heiße ein Residuations-gruppoid, kurz ein DR-Gruppoid, wenn es den Bedingungen

$$\text{(R01)} \qquad (a * a) * b \; = \; b$$

$$\text{(R11)} \qquad (a * b) * (a * c) \; = \; (b * a) * (b * c)$$

$$\text{(R21)} \qquad a * (b * a) \; = \; c * c$$

$$\text{(R31)} \qquad (a * b) * (a * c) \; = \; a * ((b : a) * c)$$

$$\text{(R14)} \qquad a * b = c * c \; = \; b * a \Rightarrow a = b$$

$$\text{(R5)} \qquad a * (b : c) \; = \; (a * b) : c$$

sowie den hierzu $:, *$ - dualen Bedingungen genügt.

Der Leser beachte, dass (R5) selbstdual ist.
Aufgrund der Rechts-Links-Symmetrie ist ein DR-Gruppoid sowohl ein Rechts- als auch ein Links-Residuationsgruppoid.

$$\text{(7.10)} \qquad a * b = 1 \iff b : a = 1$$

DENN: $a * b = 1 \Longrightarrow b : a = b : ((a * b) * a) = (b : a) : (b : a)\,.$ $\square$

Damit ist eine ganz wesentliche Verwebung von $*$ - und $:$ - Struktur gesichert. Wir können also einheitlich $\leq$ für die zunächst formal verschiedenen Partialordnungen der beiden Gruppoide schreiben. Klar sind nach (R21) und seinem Dualen zunächst:

$$\text{(7.11)} \qquad a \geq b * a \quad \& \quad a \geq a : b\,.$$

$$\text{(7.12)} \qquad \begin{array}{c} a \;\; \geq \;\; b \\ \Longrightarrow \\ a * c \leq b * c \quad \& \quad d * a \geq d * b \end{array}$$

Dies liefert $x \geq x : (y * x) \leq y$ vermöge (R5) und damit

$$\text{(7.13)} \qquad a * b \; = \; (b : (a * b)) * b\,.$$

Wir setzen:

$$\begin{aligned} t &:= ((b : (a * b)) \, * \, (a : (b * a))) * ((b : (a * b)) * b) \\ &= ((b : (a * b)) \, * \, (a : (b * a))) * (a * b)\,, \end{aligned}$$

und erhalten
$$t \;\leq\; a*b\,. \tag{7.13}$$

Es ist aber auch $t \geq a*b$, Denn es gilt allgemein die Implikation

$$\begin{array}{rcll}
A \leq X & \& & B \leq X & \\
& \Longrightarrow & & \\
(A*B)*(A*C) & \geq & (A*X)*(A*C) & (7.12)\\
& = & (X*A)*(X*C) & (\mathrm{R}11)\\
& = & X*C\,, &
\end{array}$$

also mit $A = b:(a*b)$ und $B = a:(b*a)$ dann unter Berücksichtigung von (7.13)

(7.14) $$a*b = ((b:(a*b))*(a:(b*a)))*((b:(a*b))*b)\ .$$

Weiter haben wir:

(7.15) $$(a*b)*(b*a) \;=\; b*a$$

(7.16) $$(a:b)*(b:a) \;=\; b:a\,.$$

DENN:
$$\begin{array}{cll}
& (a*b)*(b*a) & \\
= & ((b:(a*b))*(a:(b*a)))*((b:(a*b))*b) & \\
* & ((a:(b*a))*(b:(a*b)))*((a:(b*a))*a) & \\
= & ((b:(a*b))*(a:(b*a)))*((b:(a*b))*b) & \\
= & ((b:(a*b))*(a:(b*a)))*((b:(a*b))*a) & \\
= & ((b:(a*b))*b)*((b:(a*b))*a) & (\mathrm{R}11)\\
= & b*a\,, & (\mathrm{R}11)
\end{array}$$

UND:
$$\begin{array}{lrcll}
& (a:((a:b)*b))*b & \leq & (a:b)*b & \\
\Longrightarrow & ((a:((a:b)*b))*b):((a:b)*b) & = & 1 & \\
\Longrightarrow & (a:((a:b)*b))*(b:((a:b)*b)) & = & 1 & \\
\Longrightarrow & (b:((a:b)*b)):(a:((a:b)*b)) & = & & (7.10)\\
\Longrightarrow & (b:a):(((a:b)*b):a) & = & 1 & (\mathrm{R}12)\\
\Longrightarrow & (b:a):((a:b)*(b:a)) & = & 1 & \\
\Longrightarrow & (a:b)*(b:a) & \geq & b:a\ . & \square
\end{array}$$

Ein DR-Gruppoid muss nicht $\vee$-abgeschlossen sein. Existiert aber zu den Elementen a, b in R das Supremum $a \vee b$, so ist es eindeutig ausgezeichnet als Lösung eines Forderungssystems. Genauer:

7. 2. 2 Proposition. *Sei $\mathfrak{R}$ ein RR-Gruppoid. Dann hat das System*

$$\text{(F)} \qquad \begin{aligned} a * x &\doteq a * b \\ x * a &\doteq 1 \end{aligned}$$

höchstens eine Lösung und diese ist dann notwendig gleich $\sup(a, b)$.

BEWEIS. Seien c und auch d Lösungen zu (F). Dann folgt zunächst:

$$\begin{aligned} c * d &= (c * a) * (c * d) \\ &= (a * c) * (a * d) = 1 \\ &\Longrightarrow \\ c &\geq d\,. \end{aligned}$$

Weiter haben wir

$$\begin{aligned} c * b &= (c * a) * (c * b) \\ &= (a * c) * (a * b) \\ &= 1\,. \end{aligned}$$

Also gilt $c \geq a$ nach Annahme und $c \geq b$, wie soeben gezeigt. Sei hiernach

$$v \geq a \quad \& \quad v \geq b\,.$$

erfüllt. Dann folgt:

$$\begin{aligned} v * c &= (v * a) * (v * c) \\ &= (a * v) * (a * c) \\ &= (a * v) * (a * b) \\ &= (v * a) * (v * b) \\ &= (v * a) * 1 = 1 \\ &\Longrightarrow \\ v &\geq c\,. \end{aligned}$$

□

7. 2. 3 Definition. Unter einem sup-abgeschlossenen RR-Gruppoid verstehen wir ein RR-Gruppoid, in dem alle $a \vee b$ existieren, derart dass $a * (a \vee b) = (a * b)$ erfüllt ist.
Als erstes erhalten wir

$$a * (a \vee b) = a * b \iff (a \vee b) : a \; = \; b : a\,. \tag{7.18}$$

DENN: Nach (7.12) folgt $(a \vee b) : a \geq a$ und $a * (a \vee b) = a * b$ impliziert

$$\begin{aligned} ((a \vee b) : a) : (b : a) &= ((a \vee b) : (a * b)) : a && \text{(R32)} \\ &= ((a \vee b) : (a * (a \vee b))) : a && \text{(NV)} \\ &= ((a \vee b) : a) : ((a \vee b) : a) && \text{(R32).} \end{aligned}$$

Damit sind wir am Ziel. □

Insbesondere ist also auch das $\vee$-abgeschlossene DR-Gruppoid selbstdual. Sei für den Rest dieses Abschnitts $\mathfrak{R}$ ein sup-abgeschlossenes DR-Gruppoid. Dann folgt:

7. 2. 4 Lemma. *In $\mathfrak{R}$ gilt die Äquivalenz:*

$$a \wedge b = 1 \Longleftrightarrow ((a * x) * (b * x)) * ((a * x) * y) = x * y\,. \tag{7.19}$$

DENN:
$$\begin{array}{rcl} a \wedge b = 1 & \Longrightarrow & ((a * x) * (b * x)) * ((a * x) * y) \\ & = & ((a * x) \vee (b * x)) * y \\ & = & ((a \wedge b) * x) * y \\ & = & x * y \end{array}$$ □

$$(a \vee b) * c \;=\; (a * b) * (a * c)\,, \tag{7.20}$$

DENN:
$$\begin{array}{rcl} (a \vee b) * c & = & ((a \vee b) * a) * ((a \vee b) * c) \\ & = & (a * (a \vee b)) * (a * c) \\ & = & (a * b) * (a * c)\,. \end{array}$$ □

$$a * (b \vee c) \;=\; a * b \vee a * c \tag{7.21}$$

DENN:
$$\begin{array}{rcl} (a * b) * (a * (b \vee c)) & = & (b * a) * (b * (b \vee c)) \\ & = & (b * a) * (b * c) \\ & = & (a * b) * (a * c)\,, \end{array}$$

womit nach (7.12) alles gezeigt ist □

7.3 Normalität

Im Abschnitt über die Arithmetik komplementärer Halbgruppen haben wir den Sonderfall der normalen komplementären Halbgruppe studiert. Hier werden die dortigen Ergebnisse los gelöst von der Multiplikation hergeleitet.

7. 3. 1 Definition. Ein DR-Gruppoid heiße normal im Falle

$$x \le a * b \;\&\; x \le b * a \;\Longrightarrow\; x = 1\,. \tag{N*}$$

Sei in diesem Abschnitt $\mathfrak{R}$ stets ein DR-Gruppoid. Dann folgt:

7. 3. 2 Lemma. $\mathfrak{R}$ *ist genau dann normal, wenn gilt:*

$$\begin{gathered} a * c = \quad 1 \quad = b * c \\ \Longrightarrow \\ ((b : (a * b)) * (a : (b * a))) * ((b : (a * b)) * c) = 1\,. \end{gathered}$$

BEWEIS. (a) Sei (N^*) erfüllt. Dann erhalten wir nach 7.14

$$\begin{aligned} & ((b : (a * b)) * (a : (b * a))) * ((b : (a * b)) * c) \\ \leq\ & (b : (a * b)) * c \\ \leq\ & (b : (a * b)) * b \\ =\ & a * b \end{aligned}$$

und wegen (R11) gilt

$$\begin{aligned} ((b : (a * b)) * (a : (b * a))) * ((b : (a * b)) * c) &\leq (a : (b * a)) * c \\ &\leq (a : (b * a)) * a \\ &= b * a\,. \end{aligned}$$

(b) Sei nun die aufgestellte Implikation erfüllt und gelte $x \leq a : b, b : a$. Setzen wir dann x für c, $a : b$ für a und $b : a$ für b, so folgt $x = 1$. Somit gilt das Duale unserer Implikation und folglich resultiert (N^*), da wir aus dem Dualen das Duale des Dualen, nämlich (N^*) herleiten können. □

Als ein weiteres Resultat hat uns der Beweis von 7.3.2 geliefert:

7. 3. 3 Proposition. *Ein DR-Gruppoid ist genau dann normal, wenn es die beiden dualen Gleichungen* (N^*) *und* $(\mathrm{N}^{\cdot})$ *erfüllt.*

Obwohl nicht dual erklärt, ist also das normale DR-Gruppoid selbstdual. Sei von nun an bis zum Ende $\mathfrak{R}$ ein $\vee$-geschlossenes normales DR-Gruppoid. Dann gelten

7. 3. 4 Proposition. $\mathfrak{R}$ *ist nicht nur* $\vee$- *sondern auch* $\wedge$*-abgeschlossen, genauer gilt:*

$$a : (b * a) \vee b : (a * b) \;=\; a \wedge b\,. \tag{7.23}$$

BEWEIS.

$$\begin{aligned} & a * (a : (b * a)) = 1 \\ \& \quad & a * (b : (a * b)) = (a * b) : (a * b) = 1 \end{aligned}$$

impliziert

$$a, b \;\geq\; (a : (b * a)) \vee (b : (a * b))$$

aufgrund der Symmetrie, und wir erhalten nach (7.20) und 7.3.2

$$a, b \geq x \Longrightarrow ((a : (b * a)) \vee (b : (a * b))) * x = 1\,,$$

fertig! □

(7.24) $$(a \wedge b) * b \;=\; a * b\,,$$

DENN: Nach (7.12) gelten

$$\begin{array}{rcl} (a \wedge b) * b & \geq & a * b\,, \\ & \& & \\ (a \wedge b) * b & \leq & (b : (a * b)) * b \\ & = & a * b\,. \end{array}$$ □

(7.25) $$(a * (b \wedge c)) * (a * c) \;=\; (a * b) \wedge (a * c)\,.$$

DENN:
$$\begin{array}{rrcll} & (a * (b \wedge c)) * (a * c) & \geq & (a * b) * (a * c) & (7.12) \\ \& & (a * (b \wedge c)) * (a * c) & = & ((b \wedge c) * a) * ((b \wedge c) * c) & \\ & & = & ((b \wedge c) * a) * (b * c) & (7.24) \\ & & \leq & (b * a) * (b * c) & (7.12) \\ & & = & (a * b) * (a * c)\,. & \end{array}$$ □

Hiernach kommen wir zu den Hauptregeln:

(7.26) $$a \vee (b \wedge c) \;=\; (a \vee b) \wedge (a \vee c)$$

BEWEIS. Aus Gründen der Symmetrie reicht es zu zeigen:

$$\begin{array}{rll} & (a \vee (b \wedge c)) * ((a \vee b) : ((a \vee c) * (a \vee b))) & \\ = & ((a \vee (b \wedge c)) * (a \vee b)) : ((a \vee c) * (a \vee b)) & \\ = & ((a * (b \wedge c)) * (a * (a \vee b))) : ((a * c) * (a * (a \vee b))) & (7.21) \\ = & ((a * (b \wedge c)) * (a * b)) : ((a * c) * (a * b)) & (7.21) \\ = & ((a * c) * (a * b)) : ((a * c) * (a * b)) = 1\,. & (7.25) \end{array}$$

□

(7.27) $$a * (b \wedge c) \;=\; a * b \wedge a * c\,.$$

DENN: Dies folgt aus der Abschätzung:

$$\begin{array}{rcll}
(a*(b\wedge c)) & * & ((a*b):((a*c)*(a*b)))\vee((a*c):((a*b)*(a*c))) & \\
& = & (a*(b\wedge c))*((a*b):((a*c)*(a*b))) & \\
& \vee & (a*(b\wedge c))*((a*c):((a*b)*(a*c))) & (7.20) \\
& = & ((a*(b\wedge c))*(a*b)):((a*c)*(a*b)) & \\
& \vee & ((a*(b\wedge c))*(a*c)):((a*b)*(a*c)) & \\
& = & ((a*c)*(a*b)):((a*c)*(a*b))\,(7.25) & \\
& \vee & ((a*b)*(a*c)):((a*b)*(a*c))\,(7.25) & \\
& = & 1\vee 1=1\,, & \square
\end{array}$$

(7.28) $$(a\wedge b)*c \;=\; a*c\vee b*c$$

BEWEIS. Seien x, y zunächst orthogonal. Dann erhalten wir

$$\begin{array}{rcll}
x*(c:(y*c)) & = & (x\wedge(c:(y*c)))*(c:(y*c)) & \\
& = & c:(y*c) & (7.24) \\
& \Longrightarrow & & \\
(c:(y*c))*(x*(c:(y*c))) & = & 1 & \\
& \Longrightarrow & & \\
(c:(y*c))\;:\;((x*c):(y*c)) & = & 1 & \\
& \Longrightarrow & & \\
c:((x*c)\vee(y*c)) & = & 1 & (7.20) \\
\Longrightarrow\quad (x*c)\vee(y*c) & = & c\,. &
\end{array}$$

Hiernach gelingt der allgemeine Beweis vermöge

$$\begin{array}{rcll}
(a\wedge b)*c & = & (a*b\wedge b*a)*((a\wedge b)*c) & \\
& = & ((a*b)*((a\wedge b)*c)) & \\
& \vee & ((b*a)*((a\wedge b)*c)) & \\
& = & (((a\wedge b)*b)*((a\wedge b)*c)) & \\
& \vee & ((a\wedge b)*a)*((a\wedge b)*c) & \\
& = & b*c\vee a*c\,. & (\mathrm{R}11)
\end{array}$$

Damit sind wir am Ziel. $\square$

(7.29) $$(a\vee b)*c \;=\; a*c\wedge b*c$$

BEWEIS.
$$\begin{array}{rcl} a \vee b \leq c & \Longrightarrow & ((a \vee b) * c) * ((a * (a \vee b)) * d) \\ & = & ((a * b) * (a * c)) * ((a * b) * d) \\ & = & ((a * c) * (a * b)) * ((a * c) * d) \\ & = & (a * c) * d\,, \quad \text{beachte} \quad b \leq c\,, \end{array}$$

und dies bedeutet $(a\vee b)*c = a*c\wedge b*c$, wegen $x*d = y*d \ (\forall\, d) \Longleftrightarrow x = y$. Weiter haben wir für alle d

$$\begin{array}{rl} & ((a \vee b) * c) * d \\ = & ((a \vee b) * c) * (((a * b) \wedge (b * a)) * d) \\ = & ((a \vee b) * c) * (((a * (a \vee b)) \wedge (b * (a \vee b))) * d) \\ = & (((a \vee b) * c) * ((a * (a \vee b)) * d)) \\ \vee & (((a \vee b) * c) * ((b * (a \vee b)) * d)) \\ = & ((a * c) * d) \vee ((b * c) * d) \qquad \text{(siehe oben)} \\ = & ((a * c) \wedge (b * c)) * d\,, \end{array}$$

und hieraus folgt

$$\begin{array}{rcl} (a \vee b) * c & = & ((a \vee b) \wedge c) * c \\ & = & ((a \wedge c) \vee (b \wedge c)) * c \\ & = & ((a \wedge c) * c) \wedge ((b \wedge c) * c) \\ & = & (a * c) \wedge (b * c)\,. \end{array}$$

Damit sind wir am Ziel. □

Als Hauptsatz dieses Abschnitts können wir also festhalten:

7. 3. 5 Proposition. *Ein normales DR-Gruppoid $\mathfrak{R}$ erfüllt – zusammen mit den korrespondierenden Dualen – die Gleichungen:*

(N11) $$a * (b \vee c) = a * b \vee a * c$$

(N12) $$a * (b \wedge c) = a * b \wedge a * c$$

(N13) $$(a \wedge b) * c = a * c \vee b * c$$

(N14) $$(a \vee b) * c = a * c \wedge b * c$$

Im weiteren lenken wir unsere Aufmerksamkeit auf verbandsorientierte Clans bzw. auf die Klasse der

7.4 Sup-Clans

In diesem Abschnitt stellen wir zwei Sup-Einbettungssätze vor. Sei $\mathfrak{R}$ zunächst ein RR-Gruppoid. Wir erklären

$$[a\,|\,b] * [c\,|\,d] \;:=\; \big[(a*b)*(a*c)\,\big|\,(a*b)*(a*d)\big]\,, \tag{7.34}$$

und es sei im Falle eines DR-Gruppoides die Operation : dual erklärt.

7. 4. 1 Proposition. *In* $(R \times R, *)$ *gelten*

$$([a\,|\,b]*[a\,|\,b])*[c\,|\,d] \;=\; [c\,|\,d]\,. \tag{7.35}$$

$$[a\,|\,b]*([c\,|\,d]*[c\,|\,d]) \;=\; [1\,|\,1]\,. \tag{7.36}$$

$$\begin{array}{l} ([a\,|\,b]*[c\,|\,d])*([a\,|\,b]*[u\,|\,v]) \\ = \\ ([c\,|\,d]*[a\,|\,b])*([c\,|\,d]*[u\,|\,v])\,. \end{array} \tag{7.37}$$

BEWEIS. (7.35) und (7.36) folgen *geradeaus,* und (7.37) ergibt sich *via*:

$$\begin{array}{rcl}
 & & \big[(a*b)*(a*c)\,\big|\,(a*b)*(a*d)\big] \\
 & * & \big[(a*b)*(a*u)\,\big|\,(a*b)*(a*v)\big] \\
 & = & \Big[\,(((a*b)*(a*c))*((a*b)*(a*d))) \\
 & * & (((a*b)*(a*c))*((a*b)*(a*u))) \quad \Big|\,\ldots \\
 & = & \Big[\,(((a*c)*(a*b))*((a*c)*(a*d))) \\
 & * & (((a*c)*(a*b))*((a*c)*(a*u))) \quad \Big|\,\ldots \\
 & = & \Big[\,(((c*a)*(c*b))*((c*a)*(c*d))) \\
 & * & *(((c*a)*(c*b))*((c*a)*(c*u))) \;\Big|\,\ldots \\
 & = & \Big[\,(((c*a)*(c*d))*((c*a)*(c*b))) \\
 & * & (((c*a)*(c*d))*((c*a)*(c*u))) \quad \Big|\,\ldots \\
Q & = & \Big[\,(((c*d)*(c*a))*((c*d)*(c*b))) \\
 & * & (((c*d)*(c*a))*((c*d)*(c*u))) \quad \Big|\,\ldots \\
 & = & \big([c\,|\,d]*[a\,|\,b]\big)*\big([c\,|\,d]*[u\,|\,v]\big)\;.
\end{array}$$

Damit sind wir am Ziel □

Der Leser beachte, dass wir Axiom (R5) nicht herangezogen haben.

7. 4. 2 Lemma. *Sei* $\mathfrak{R}$ *ein DR-Gruppoid. Dann gilt in* $(R \times R, *, :)$

$$([a \mid b] * [c \mid d]) : [u \mid v] \;:=\; [a \mid b] * ([c \mid d]) : [u \mid v]) \,. \tag{7.38}$$

DENN:
$$\begin{aligned}
&\big([a \mid b] * [c \mid d]\big) : [u \mid v]\\
=\;& \big[(a*b)*(a*c) \,\big|\, (a*b)*(a*d)\big] : [u \mid v]\\
=\;& \Big[\,(((a*b)*(a*c)) : v) : (u:v) \,\Big|\, (((a*b)*(a*d)) : v) : (u:v)\Big]\\
\overset{(R4)}{=}\;& \Big[\,((a*b)*((a*c) : v)) : (u:v) \,\Big|\, ((a*b)*((a*d) : v)) : (u:v)\Big]\\
\overset{(R4)}{=}\;& \Big[(a*b)*(((a*c) : v) : (u:v)) \,\Big|\, (a*b)*(((a*d) : v) : (u:v))\Big]\\
\overset{(R4)}{=}\;& \Big[(a*b)*((a*(c:v)) : (u:v)) \,\Big|\, (a*b)*((a*(d:v)) : (u:v))\Big]\\
\overset{(R4)}{=}\;& [a \mid b] * \big[(c:v) : (u:v) \,\big|\, (d:v) : (u:v)\big]\\
=\;& [a \mid b] * \big([c \mid d] : [u \mid v]\big) \;.
\end{aligned}$$
□

Der Leser beachte, dass wir dieses Mal (R31) (und (R32)) nicht eingesetzt haben.

7. 4. 3 Lemma. *Sei* $\mathfrak{R}$ *ein DR-Gruppoid. Dann gilt in der Erweiterung* $(R \times R, *, :)$ *die Gleichung:*

(7.39)
$$([u \mid v] : [a \mid b]) : ([c \mid d] : [a \mid b]) \;=\; ([u \mid v] : ([a \mid b] * [c \mid d]) : [a \mid b] \,.$$

BEWEIS. Zunächst gilt

$$[a \mid 1] * [b \mid 1] = [a*b \mid 1] \;\;\&\;\; [a \mid 1] : [b \mid 1] = [a:b \mid 1] \,.$$

Das bedeutet weiter:

$$\begin{aligned}
&\big([a \mid 1] * [b \mid 1]\big) * \big([a \mid 1] * [c \mid d]\big)\\
=\;& \Big[a*((b:a)*c) \,\Big|\, a*((b:a)*d)\,\Big]\\
=\;& [a \mid 1] * \Big(\big([b \mid 1] : [a \mid 1]\big) * [c \mid d]\Big) \,,
\end{aligned}$$

Und dies liefert uns

$$
\begin{aligned}
\rightsquigarrow \qquad & [u:a \,|\, v:a] : [b:a \,|\, c:a] \\
= \; & \Big[\, ((u:a):(c:a)):((b:a):(c:a)) \,\Big|\, \big((v:a)\ldots \\
= \; & \Big[\, ((u:a):((c:a)*(b:a))):(c:a) \,\Big|\, \big((v:a):\ldots \\
= \; & \Big[\, ((u:a):(((c:a)*b):a)):(c:a) \,\Big|\, \big((v:a):\ldots && \text{(R4)} \\
= \; & \Big[\, (((u:(a*((c:a)*b))):a)):(c:a) \,\Big|\, \big((v:a)\ldots && \text{(R32)} \\
= \; & \Big[\, ((u:(a*((c:a)*b))):(a*c)):a \,\Big|\, \big((v:(\ldots && \text{(R32)} \\
= \; & \big([u \,|\, v]:[a*b \,|\, a*c]\big):[a \,|\, 1] \\
= \; & \big([u \,|\, v]:\big([a \,|\, 1]*[b \,|\, c]\big)\big):[a \,|\, 1]
\end{aligned}
$$

$$
\begin{aligned}
\rightsquigarrow \qquad & \big([u \,|\, v]:[a \,|\, b]\big):\big([c \,|\, d]:[a \,|\, b]\big) \\
= \; & \big([u:b \,|\, v:b]:[a:b \,|\, 1]\big):\big(\big([c \,|\, d]:[b \,|\, 1]\big):[a:b|1]\big) \\
= \; & \big([u:b \,|\, v:b]:\big([a:b \,|\, 1]*\big([c \,|\, d]:[b \,|\, 1]\big)\big)\big):[a:b \,|\, 1] \\
= \; & \big(\big([u \,|\, v]:[b \,|\, 1]\big):\big(\big([a:b \,|\, 1]*[c \,|\, d]\big):[b \,|\, 1]\big)\big):[a:b \,|\, 1] \\
= \; & \big(\big([u \,|\, v]:\big([b \,|\, 1]*([a:b \,|\, 1]*[c \,|\, d])\big)\big):[b \,|\, 1]\big):[a:b \,|\, 1] \\
= \; & \big(\big([u \,|\, v]:\big([b \,|\, 1]*\big(([a \,|\, 1]:[b \,|\, 1])*[c \,|\, d]\big)\big)\big):[b \,|\, 1]\big):[a:b \,|\, 1] \\
= \; & \big([u \,|\, v]:\big(\big([b \,|\, 1]*[a \,|\, 1]\big)*\big([b \,|\, 1]*[c \,|\, d]\big)\big)\big):[a \,|\, b] \\
= \; & \big([u \,|\, v]:\big(\big([a \,|\, 1]*[b \,|\, 1]\big)*\big([a \,|\, 1]*[c \,|\, d]\big)\big)\big):[a \,|\, b] && \text{(R11)} \\
= \; & \big([u \,|\, v]:[(a*b)*(a*c) \,|\, (a*b)*(a*d)]\big):[a \,|\, b] \\
= \; & \big([u \,|\, v]:\big([a \,|\, b]*[c \,|\, d]\big)\big):[a \,|\, b]\,.
\end{aligned}
$$

□

Hiernach gehen wir über zu einem homomorphen Bild. Wir setzen in Anlehnung an „bewährte" Methoden:

$$
\begin{array}{c}
[a \,|\, b] \quad \equiv \quad [c \,|\, d] \\
:\Longleftrightarrow \\
[a \,|\, b]*[c \,|\, d] = \; [1 \,|\, 1] \; = [c \,|\, d]*[a \,|\, b]
\end{array}
\tag{7.40}
$$

7. 4. 4 Proposition. *Die Relation* $\equiv\; =: \;\theta$ *ist eine Kongruenzrelation.*

BEWEIS. Zunächst folgt fast unmittelbar die Äquivalenz

(7.41) $$[a \,|\, b] * [c \,|\, d] = [1 \,|\, 1] \iff [c \,|\, d] : [a \,|\, b] = [1 \,|\, 1],$$

DENN:
$$\begin{array}{rcl} [a \,|\, b] * [c \,|\, d] & = & [1 \,|\, 1] \\ & \Longrightarrow & \\ [c \,|\, d] : [a \,|\, b] & = & \big([c \,|\, d] : ([a \,|\, b] * [c \,|\, d])\big) : [a \,|\, b] \\ & = & \big([c \,|\, d] : [a \,|\, b]\big) : \big([c \,|\, d] : [a \,|\, b]\big) \\ & = & [1 \,|\, 1]\,. \end{array}$$

Weiter gelten – im Blick auf die Verträglichkeit:

(7.42)
$$\begin{array}{rcl} [a \,|\, b] \equiv [c \,|\, d] & \& & [c \,|\, d] \equiv [u \,|\, v] \\ & \Longrightarrow & \\ [a \,|\, b] & \equiv & [u \,|\, v] \end{array}$$

WEGEN:
$$\begin{array}{rcl} [a \,|\, b] \equiv [c \,|\, d] & \& & [c \,|\, d] \equiv [u \,|\, v] \\ & \Longrightarrow & \\ [a \,|\, b] * [u \,|\, v] & = & \big([a \,|\, b] * [c \,|\, d]\big) * \big([a \,|\, b] * [u \,|\, v]\big) \\ & = & \big([c \,|\, d] * [a \,|\, b]\big) * \big([c \,|\, d] * [u \,|\, v]\big) \\ & = & [1 \,|\, 1] * [1 \,|\, 1] = [1 \,|\, 1] \end{array}$$

SOWIE:
$$\begin{array}{rcl} [x \,|\, y] & \equiv & [u \,|\, v] \\ & \Longrightarrow & \\ [x \,|\, y] * [a \,|\, b] & = & \big([x \,|\, y] * [u \,|\, v]\big) * \big([x \,|\, y] * [a \,|\, b]\big) \\ & = & \big([u \,|\, v] * [x \,|\, y]\big) * \big([u \,|\, v] * [a \,|\, b]\big) \\ & = & [u \,|\, v] * [a \,|\, b] \\ & \& & \\ \big([a \,|\, b] * [x \,|\, y]\big) * \big([a \,|\, b] * [u \,|\, v]\big) & = & \big([x \,|\, y] * [a \,|\, b]\big) * \big([x \,|\, y] * [u \,|\, v]\big) \\ & = & [1 \,|\, 1] \\ & \Longrightarrow & \\ [a \,|\, b] * [x \,|\, y] & \equiv & [a \,|\, b] * [u \,|\, v]\,. \end{array}$$

Der Rest ergibt sich aus Gründen der Dualität. □

Nun können wir zeigen

7. 4. 5 Proposition. *Mit $\mathfrak{R}$ ist auch $(R \times R, *\,, :)/\,\theta$ ein DR-Gruppoid.*

DENN:

$$\begin{array}{ccc} [a \,|\, b] \equiv [1 \,|\, 1] & \Rightarrow & [a \,|\, b] = [1 \,|\, 1] \\ & \Longrightarrow & \\ [a \,|\, b] * [c \,|\, d] \equiv & [1 \,|\, 1] & \equiv [c \,|\, d] * [a \,|\, b] \\ & \Longrightarrow & \\ [a \,|\, b] * [c \,|\, d] = & [1 \,|\, 1] & = [c \,|\, d] * [a \,|\, b] \\ & \Longrightarrow & \\ [a \,|\, b]\,\theta & = & [c \,|\, d]\,\theta\,. \end{array}$$

□

Als eine erste Anwendung erhalten wir

7. 4. 6 Proposition. *Jedes DR-Gruppoid besitzt eine Erweiterung, in der das oben formulierte Gleichungssystem* (F) *für alle $a, b \in R$ lösbar ist.*

BEWEIS. Wir betrachten die Erweiterung $(R \times R\,, *\,, :)/\,\theta =: \mathfrak{R}_1$. Hier können wir die Elemente $[x \,|\, 1]$ jeweils ersetzen durch x und danach die Behauptung routinemäßig her rechnen. □

Proposition 7.4.6 liefert die Basis für

7. 4. 7 Das Sup-Clan-Theorem. *Jedes DR-Gruppoid besitzt eine kanonische engste* sup-*abgeschlossene Erweiterung.*

BEWEIS. Wir konstruieren – im Sinne von 7.4.6 – eine Ausdehnungsfolge

$$\mathfrak{R} =: \mathfrak{R}_0 \subseteq \mathfrak{R}_1 \subseteq \mathfrak{R}_2 \subseteq \mathfrak{R}_3 \subseteq \ldots\ldots \subseteq \mathfrak{R}_n \subseteq \ldots\ldots$$

und definieren $S = \bigcup R_n \ (n \in \mathbf{N})$. Hiernach setzen wir $a * b = c$ gdw. im ersten $\mathfrak{R}_i$ mit $a, b \in B_i$ $a * b = c$ erfüllt ist. Dual verfahren wir im Blick auf $:$. Dann ist $(\mathfrak{S} = (S, *, :)$ eine sup-abgeschlossene Erweiterung, in der jedes Paar a, b eine Lösung bezüglich (F) besitzt.

Ist nun auch $\mathfrak{T}$ eine solche Erweiterung, so können wir zeigen, dass die Menge aller Suprema aus $\mathfrak{S}$ abgeschlossen ist bezüglich $*$ und $:$ und mit Blick auf diese Operationen isomorph ist zu $\mathfrak{S}$.

(*i*) Offenbar ist $T_1 := \{a \vee b \in S \,|\, a, b \in R\}$ $*$- und $:$-abgeschlossen.

(ii) $\Phi :\ [a \mid b]\,\theta \longmapsto a \vee b$ bildet $\mathfrak{R}_1$ bijektiv ab auf $\mathfrak{T}_1$. Denn es gilt:

$$\begin{array}{rl} & [a \mid b]\,\theta \geq [c \mid d]\,\theta \\ \Longleftrightarrow & [a \mid b] * [c \mid d] = [1 \mid 1] \\ \Longleftrightarrow & [(a*b)*(a*c) \mid (a*b)*(a*d)] = [1 \mid 1] \\ \Longleftrightarrow & (a*b)*(a*c) = 1 = (a*b)*(a*d) \\ \Longleftrightarrow & (a*b)*(a*c) \vee (a*b)*(a*d) = 1 \\ \Longleftrightarrow & (a \vee b)*(c \vee d) = 1 \\ \Longleftrightarrow & (a \vee b) \geq (c \vee d)\,. \end{array}$$

(iii) Φ ist ein Homomorphismus. Denn es gilt:

$$\begin{array}{rl} & \Phi\big([a \mid b]\,\theta * [c \mid d]\,\theta\big) \\ = & \Phi\big([(a*b)*(a*c) \mid (a*b)*(a*d)]\,\theta\big) \\ = & ((a*b)*(a*c)) \vee ((a*b)*(a*d)) \\ = & (a \vee b)*(c \vee d) \\ = & \Phi\big([a \mid b]\,\theta\big) * \Phi\big([c \mid d]\,\theta\big)\ . \end{array}$$

Damit gelangen wir induktiv ans Ziel. □

Schließlich ein Hinweis auf die Kongruenzen in $\mathfrak{S}$.

7. 4. 8 Proposition. *Seien* $\mathfrak{R}$ *und* $\mathfrak{S}$ *erklärt wie oben. Dann lässt sich jede Kongruenz* $\equiv$ *aus* $\mathfrak{R}$ *mit* $a*b \equiv 1 \Longleftrightarrow a*b = 1$ *eindeutig ausdehnen zu einer Kongruenz auf* $\mathfrak{S}$ *.*

DENN: Ist $\equiv$ eine Kongruenz auf $\mathfrak{R}$ mit $a*b \equiv 1$ & $b*a \equiv 1 \Longrightarrow a = b$, so liefert

$$\begin{array}{rcl} (a \vee b)\,\theta(c \vee d) & :\Longleftrightarrow & (a*b)*(a*c) \equiv 1 \equiv (a*b)*(a*d) \\ & \& & (c*d)*(c*a) \equiv 1 \equiv (c*d)*(c*b) \end{array}$$

eine Kongruenz mit Restriktion $\equiv$, was man leicht nachrechnet, und es kann wie unter 5.4.3 leicht eingesehen werden, dass es keine anderen Fortsetzungen gibt. Schließlich ist die erklärte Relation in $\mathfrak{S}$ auch eine Kongruenz bezüglich $\vee$. □

Wir zeigen nun, dass bei der vorgestellten Einbettung die Eigenschaft der Normalität mitgeht.

7. 4. 9 Der Haupteinbettungssatz. *Ist $\mathfrak{R}$ ein normales DR-Gruppoid, so ist auch die Erweiterung $\mathfrak{S}$ ein normales DR-Gruppoid.*

BEWEIS. (i) Wir beweisen zunächst den Sonderfall

$$\begin{array}{rcl}
\big([a\,|\,1]*[c\,|\,d]\big)*[u\,|\,1] & \equiv & [1\,|\,1] \\
\&\ \big([c\,|\,d]*[a\,|\,1]\big)*[u\,|\,1] & \equiv & [1\,|\,1] \\
& \Longrightarrow & \\
[a*c\,|\,a*d]*[u\,|\,1] & = & [1\,|\,1] \\
\&\ \big[(c*d)*(c*a)\,\big|\,1\big]*[u\,|\,1] & = & [1\,|\,1] \\
& \Longrightarrow & \\
((a*c)*(a*d))*((a*c)*u) & = & 1 \\
\&\quad ((c*d)*(c*a))*u & = & 1 \\
& \Longrightarrow & \\
((a*c)*(a*d))*((a*c)*u) & = & 1 \\
\&\quad ((c*d)*(c*a))*((c*d)*u) & = & 1\,.
\end{array} \tag{7.12}$$

Hier führt die letzte Zeile nach (7.12) zu

$$(c*a)*((c*d)*u) \;=\; 1\,, \tag{7.43}$$

und es liefern die beiden letzten Zeilen zusammen mit (R11) und (7.12)

$$\begin{array}{rcl}
((c*a)*(c*d))*((a*c)*((c*d)*u)) & = & 1 \\
\&\quad ((c*d)*(c*a))*((a*c)*((c*d)*u)) & = & 1\,,
\end{array}$$

woraus dann wegen (N*)

$$(a*c)*((c*d)*u) \;=\; 1 \tag{7.44}$$

resultiert.
(7.43) und (7.44) liefern aber weiter die beiden Gleichungen

$$(c*d)*u \;=\; 1 \tag{7.45}$$
$$(d*c)*u=1 \;\rightsquigarrow\; u=1\,, \tag{7.46}$$

(ii) Gelte nun

$$\begin{array}{rcl}
\big([a\,|\,b]*[c\,|\,d]\big)*[u\,|\,1] & \equiv & [1\,|\,1] \\
\big([c\,|\,d]*[a\,|\,b]\big)*[u\,|\,1] & \equiv & [1\,|\,1]\,.
\end{array}$$

Wir dürfen $=$ statt $\equiv$ lesen und haben außerdem

$$\big([a \,|\, 1] * [c \,|\, d]\big) * [u \,|\, 1] \;=\; [1 \,|\, 1]\,.$$

Daher ist nur noch die Gleichung

$$\big([c \,|\, d] * [a \,|\, 1]\big) * [u \,|\, 1] \;=\; [1 \,|\, 1]$$

nachzuweisen. Hier gelangen wir wie folgt zum Ziel:

$$\begin{array}{rl} & \big([a \,|\, b] * [c \,|\, d]\big) * [u \,|\, 1] \;=\; [1 \,|\, 1] \\ \& & \big([c \,|\, d] * [a \,|\, b]\big) * [u \,|\, 1] \;=\; [1 \,|\, 1] \end{array}$$

impliziert:

$$\begin{array}{rl} & (((a*b)*(a*c))*((a*b)*(a*d)))*(((a*b)*(a*c))*u) \\ = & (((a*c)*(a*b))*((a*c)*(a*d)))*(((a*b)*(a*c))*u) \\ =: & (P*Q)*(R*u) = 1 \\ \& & (((c*d)*(c*a))*((c*d)*(c*b)))*(((c*d)*(c*a))*u) \\ = & (((c*a)*(c*d))*((c*a)*(c*b)))*(((c*d)*(c*a))*u) \\ = & (((a*c)*(a*d))*((a*c)*(a*b)))*(((c*d)*(c*a))*u) \\ =: & (Q*P)*(S*u) = 1 \end{array}$$

$$\Longrightarrow \quad (P*Q)*(R*(S*u)) = 1 \tag{7.12}$$
$$\& \quad (Q*P)*(R*(S*u)) = 1\,. \tag{7.12}$$

Auf diese Weise erhalten wir

$$\begin{array}{rrcl} & R*(S*u) & = & 1 \\ \& & P*(S*u) & = & 1\,, \end{array}$$

und wegen $P = (a*c)*(a*b)$ & $R = (a*b)*(a*c)$ folgt hieraus

$$\begin{array}{rcl} \big([c \,|\, d] * [a \,|\, 1] * [u \,|\, 1]\big) & = & \big[\,((c*d)*(c*a))*u \,\big|\, 1\big] \\ & = & [S*u \,|\, 1] = [1 \,|\, 1]\,. \end{array}$$

(iii) Hieraus folgt dann der allgemeine Fall mit $[u \,|\, v]$ an der Stelle von $[u \,|\, 1]$ mittels *(i)* und *(ii)*, da $[a \,|\, b] * [u \,|\, v] = [1 \,|\, 1]$ zu $[a \,|\, b] * [u \,|\, 1] = [1 \,|\, 1]$ & $[a \,|\, b] * [v \,|\, 1] = [1 \,|\, 1]$ führt. $\square$

7.5 Der brouwersche und der boolesche Clan

7. 5. 1 Proposition. *Ein RR-Gruppoid ist ein brouwerscher Halbverband gdw. $\mathfrak{R}$ der Gleichung genügt:*

$$\text{(B)} \qquad a * (b * c) \;=\; (a * b) * (a * c)$$

und zudem jedes Gleichungssystem (F) *lösbar ist.*

DENN: Setzen wir die eindeutige Lösung von (F) gleich ab, so folgt

$$a * (b * c) = (a * b) * (a * c) = (a * ab) * (a * c) = (ab * a) * (ab * c) = ab * c\,,$$

also insbesondere $\qquad a * (b * c) \;=\; b * (a * c)$

und hiermit dann weiter (A1), (A2), (A3) vermöge

$$\begin{aligned}
a * a(b * b) &= a * (b * b) \\
&= 1 \\
&= a(b * b) * a\,, \\
ab * c &= (ab * a) * (ab * c) \\
&= (a * b) * (a * c) \\
&= a * (b * c) \\
&= b * (a * c) \\
(a * b) * b(b * a) &= (a * b) * (a * b(b * a) \\
&= (b * a) * (b * b(b * a) \\
&= (b * a) * (b * a) \\
&= 1\,.
\end{aligned}$$

Damit sind wir am Ziel. □

Da sich die Bedingung (B), wie man leicht nachrechnet, bei unserem Einbettungsverfahren fortpflanzt, erhalten wir als weiteren Sonderfall

7. 5. 2 Das brouwersche Clan-Theorem. *Ein RR-Gruppoid ist Clan eines brouwerschen Halbverbandes, gdw. es zusätzlich der Bedingung* (B) *genügt.*

Browersche Clans sind gleichungsdefiniert, denn es gilt, siehe [31]:

7. 5. 3 Proposition. *$\mathfrak{R}$ ist ein brouwerscher Clan gdw. $\mathfrak{R}$ eine Hilbert-Algebra ist, d. h.* – siehe [61] – *den Gleichungen genügt:*

$$\text{(H1)} \qquad (a * a) * b \;=\; b$$

$$\text{(H2)} \qquad a * (b * c) \;=\; (a * b) * (a * c)$$

$$\text{(H3)} \qquad (a * b) * ((b * a) * b) \;=\; (b * a) * ((a * b) * a)\,.$$

BEWEIS. Die Bedingung ist notwendig, denn ist $\mathfrak{R}$ ein brouwerscher Clan, so folgt, wenn wir die linke Seite von (H3) mit ℓ, die rechte mit r abkürzen:

$$\begin{array}{rcl}
\ell * r & = & ((b * a) * ((a * b) * b)) \\
 & * & ((b * a) * ((a * b) * a)) \\
 & = & (b * a) * (((a * b) * b) * ((a * b) * a)) \\
 & = & (b * a) * ((a * b) * (b * a)) \\
 & = & (b * a) * (b * a) \\
 & = & 1\,.
\end{array}$$

Und ist $\mathfrak{R}$ eine Hilbert-Algebra, so folgt zunächst aus (H1) und (H3) fast unmittelbar das Axiom (R3), und es gilt $a * (b * a) = (a * b) * (a * a) = 1$. Und das führt zu

$$\begin{array}{rcl}
a * (b * c) & = & ((a * b) * (a * a)) * (a * (b * c) \\
 & = & (a * (b * a)) * (a * (b * c)) \\
 & = & a * (b * (a * c))\,. \\
 & \rightsquigarrow & \\
(a * (b * c)) * (b * (a * c)) = & 1 & (= (b * (a * c)) * (a * (b * c)) \\
 & \rightsquigarrow & \\
(a * b) * (a * c) = a * (b * c) & = & b * (a * c) = (b * a) * (b * c)\,,
\end{array}$$

was zu beweisen war. □

Ist $\mathfrak{R}$ Clan eines ℓ-Gruppenkegels, so gilt zudem die Gleichung

$$\text{(C)} \qquad a : (b * a) \;=\; (b : a) * b\,,$$

und es ist $\mathfrak{R}$ normal, wie wir im Kapitel über Kegelalgebren sahen. Wir zeigen nun, dass sich (C) fortpflanzt. Dies ist natürlich indirekt schon über die Kegeleinbettung gezeigt, soll hier aber mit Blick auf boolesche Algebren noch einmal direkt nachgewiesen werden.

7. 5. 4 Proposition. *Mit* $\mathfrak{R}$ *erfüllt auch* $\mathfrak{R}_1$ *Bedingung* (C).

BEWEIS. Wir beweisen zunächst den Sonderfall

$$(i) \qquad a \wedge (c \vee d) \;=\; (c \vee d) : (a * (c \vee d))$$

der aus dem Nachweis von

$$(ii) \qquad ((c \vee d) : (a * (c \vee d))) \ * \ (a \wedge (c \vee d)) = 1$$

resultiert, bei dem wir uns auf die Normalität von $\mathfrak{R}_1$ stützen. Sie gewährleistet:

$$\begin{array}{rrcl} & (a : (b * a)) * a & = & b * a \\ \& & (a : (b * a)) * b & = & a * b \\ & & \rightsquigarrow & \\ \multicolumn{2}{r}{((c \vee d) : (a * (c \vee d))) * (a \wedge (c \vee d))} & = & 1\,. \end{array}$$

Hieraus ergibt sich dann der allgemeine Fall vermöge:

$$\begin{array}{rl} & (a \vee b) : ((c \vee d) * (a \vee b)) \\ = & (a \vee b) : ((c * (a \vee b)) \wedge (d * (a \vee b))) \\ = & ((a \vee b) : (c * (a \vee b))) \vee ((a \vee b) : (d * (a \vee b))) \\ = & ((a \vee b) \wedge c) \vee ((a \vee b) \wedge d) \\ = & (a \vee b) \wedge (c \vee d)\,. \end{array}$$

Fertig! □

7. 5. 5 Das boolesche Clan-Theorem. *Ein RR-Gruppoid ist genau dann Clan eines booleschen Ringes, wenn es zusätzlich den Bedingungen* (B) *und* (C) *genügt.*

Hinweis. Sei $(P, \leq)$ eine po-set mit Minimum 0. Dann liefert die Festsetzung $a * b = 0$ im Falle $a \geq b$ und $a * b = b$ sonst, eine Hilbert-Algebra. Demzufolge lassen sich die po-sets als Hilbert-Algebren algebraisieren.
Ferner: Da die Kongruenzen umkehrbar eindeutig den Ordnungsfiltern $(a \geq b \in F \Longrightarrow a \in F)$ vermöge

$$a \equiv b :\Longleftrightarrow a * b, b * a \in F$$

entsprechen, ist der zugehörige Kongruenzverband ein $\cap$-distributiver algebraischer Verband, d.h. ein algebraischer Verband mit

$$a \cap \sum b_i = \sum (a \cap b_i) \ \ (i \in I)\,.$$

Ist umgekehrt $\mathfrak{V} := (V, \Sigma, \cap)$ ein $\cap$-distributivery algebraischer Verband, so hat jedes Element eine eindeutige Zerlegung $a = \bigcap p_i$ mit vollständig

$\bigcap$-primen Elementen p_i . Das bedeutet, dass die Menge der vollständig $\bigcap$-primen Element bezüglich $*$ ein Gruppoid bildet, dessen Kongruenzverband isomorph ist zu $\mathfrak{V}$.
Damit gilt nach dem Bisherigen:

7. 5. 6 Theorem. *Jeder vollständig $\cap$-distributive algebraische Verband ist Kongruenzverband eines brouwerschen Halbverbandes.*

7.6 Der boolesche 0-Abschluss

Ist $\mathfrak{R}$ ein boolescher Ring, so können wir über jede subdirekte Zerlegung von $\mathfrak{R}$ in subdirekt irreduzible Faktoren zu einer Einbettung von $\mathfrak{R}$ – betrachtet als Residuationsgruppoid – in einen booleschen Verband – betrachtet als Residuationsgruppoid – gelangen. Dabei geht allerdings das Zorn'sche Lemma wesentlich ein. Wir wählen hier die unter 6.5.2 praktizierte Methode.

7. 6. 1 Das BV-Theorem. *Jeder boolesche Clan lässt sich einbetten in einen booleschen Verband, aufgefasst als RR-Gruppoid.*

BEWEIS. In einem ersten Schritt können wir $\mathfrak{R}$ kanonisch einbetten in ein $\vee$-abgeschlossenes boolesches Residuationsgruppoid, also einen booleschen Ring, betrachtet als Residuationsgruppoid. Daher dürfen wir annehmen, dass $\mathfrak{R}$ schon ein boolescher Ring ist. Wir betrachten die Mengen R und $R' := R \times \{1\}$ und symbolisieren $(a, 0)$ durch a'. Dann bildet die Menge $R \cup R' =: B$ einen booleschen Verband bezüglich mit 1 als *Null* und $(1 \,|\, 0)$ als *Eins*.
Denn, dies bestätigt der Leser durch Nachrechnen, was exemplarisch für die Formel $A * (B * C) = B * (A * C)$ gezeigt sei. Hier sind die Tripel (i) a, b, c' , (ii) a, b', c , (iii) a, b', c' , (iv) a', b', c und (v) a', b', c' zu berücksichtigen.

(i)
$$\begin{aligned} a * (b * c') &= (a \vee b \vee c)' \\ &= b * (a * c' . \end{aligned}$$

(ii)
$$\begin{aligned} a * (b' * c) &= a * ((b * c) * c) \\ &= (a * (b * c)) * (a * c) \\ &= (b * (a * c)) * (a * c) \\ &= b' * (a * c) . \end{aligned}$$

(*iii*)
$$\begin{aligned} a * (b' * c') &= a * (c * b) \\ &= (a \vee c) * b \\ &= b' * (a \vee c)' \\ &= b' * (a * c') \end{aligned}$$

(*iv*)
$$\begin{aligned} a' * (b' * c) &= a' * ((b * c) * c) \\ &= (a * ((b * c) * c)) * ((b * c) * c) \\ &= ((b * c) * (a * c)) * ((b * c) * c) \\ &= (b * c) * ((a * c) * c) \\ &= b' * (a' * c)\,. \end{aligned}$$

(*v*)
$$\begin{aligned} a' * (b' * c') &= a' * (c * b) \\ &= ((a * (c * b)) * (c * b) \\ &= (c * (a * b)) * (c * b) \\ &= c * ((a * b) * b) \\ &= b' * (a' * c')\,. \end{aligned}$$

□

Kapitel 8

Verbandsgruppen-Verbände

In diesem Abschnitt möchten wir die Verbände beschreiben, die als Träger einer Verbandsgruppe infrage kommen. Zu diesem Zweck vertiefe sich der Leser vorweg noch einmal in die Arithmetik der ℓ-Gruppen, wie sie im Kapitel über Verbände entwickelt wurde. Aus dieser Arithmetik resultiert zunächst:

8. 0. 2 Lemma. *Sei P ein beliebiger ℓ-Gruppen-Kegel. Dann liefert $\Phi_s : x \to x * s$ einen y* Antiautomorphismus *von $I(s) := \{x \mid x \leq s\}$.*

BEWEIS. Seien a, b beliebig. Dann gibt es ein s mit $a\Phi_s = b$, nämlich $s := ab$, und es gilt die Implikation:

$$a\Phi_s = b \;\&\; a\Phi_t = b \;\&\; a \leq s \wedge t \Rightarrow s = t, \tag{8.1}$$

man beachte:

$$a \leq s \wedge t \Rightarrow s = a(a * s) = a(a\Phi_s) \;\&\; t = a(a * t) = a(a\Phi_t)\,.$$

Also liefert $a \leq s \wedge t$ die Implikation $a\Phi_s = a\Phi_t \Longrightarrow s = t$. □

Diese beiden letzten Ergebnisse liefern uns zusammen mit (A3), (A4), (A5) die beiden folgenden Eigenschaften für (abelsche) ℓ-Gruppen-Kegel:

8. 0. 3 Lemma. *$P \times P$ ist Vereinigung paarweise fremder involutorischer Antiautomorphismen $\Phi_s : (I(s), \leq) \to (I(s), \leq)$.*

8. 0. 4 Lemma. *Definieren wir $\overline{\Phi}_s$ vermöge $a\overline{\Phi}_s = a\Phi_{a\vee s}$, so folgt die Gleichung $a\overline{\Phi}_b\overline{\Phi}_{a\overline{\Phi}_c} = (a \vee b)\overline{\Phi}_c$.*

Damit haben wir als notwendige Verbands-Bedingungen die Aussagen der Lemmata 8.0.3 und 8.0.4 gewonnen. Betrachten wir hiernach den Verband $\mathfrak{L}$ einer ℓ-Gruppe $\mathfrak{G} := (G, \wedge, \vee, \cdot, ^{-1})$. Hier gilt unmittelbar:

(L0) $\mathfrak{L}$ ist distributiv.

(L1) Jedes $F(x) := \{x \,|\, x \geq s \in L\}$ erfüllt 8.0.3 und 8.0.4,

DENN: $\Phi : x \to ax$ ist ein Isomorphismus von $(P, \vee, \wedge)$ auf $(aP, \vee, \wedge)$ ist, vgl. (2.52), (2.53).

(L2) Es existiert ein ausgezeichnetes Element 1 und hierzu ein Antiisomorphismus Φ von $I(1) = \{x \,|\, x \leq 1\}$ auf $F(1) = \{x \,|\, x \geq 1\}$ mit $(1 \vee a) \wedge (1 \wedge a)\Phi = 1$.

DENN: Beispielsweise ist $a \to a^{-1}$ ein solcher Antiisomorphismus, mit $(1 \vee a) \wedge (1 \wedge a)^{-1} = 1$, vgl. (2.56), (2.57) und (2.58), (2.59).

(L3) Das Gleichungssystem

$$1 \vee x := a \tag{8.2}$$

$$1 \wedge x := b \tag{8.3}$$

ist lösbar für alle $a \geq 1 \geq b$, die $a \wedge b\Phi = 1$, erfüllen,

DENN: $a \wedge b\Phi = a \wedge b^{-1} = 1 \Rightarrow 1 \vee ab = a \;\&\; 1 \wedge ab = b$, vgl. (2.58).

Somit sind die Bedingungen (L0), (L1), (L2), (L3) in jeder ℓ-Gruppe erfüllt. Im folgenden werden wir zeigen, dass die herausgestellten notwendigen Bedingungen auch hinreichend sind. Das bedeutet dann einen Beitrag zu Problem 7 of Fuchs [2].

8.1 Verbände von ℓ-Gruppen-Kegeln

8. 1. 1 Theorem. *Sei $(L, \vee)$ ein Halbverband. Dann ist $(L, \vee)$ der Halbverband eines (abelschen) ℓ-Gruppen-Kegels gdw. die beiden nachfolgenden Bedingungen erfüllt sind:*

(P1) *$L \times L$ ist Vereinigung von paarweise disjunkten (involutorischen) Anti-Ordnungsautomorphismen*

$$\Phi_s : (I(s), \leq) \to (I(s), \leq)\,,$$

aufgefasst als Mengen von Paaren.

(P2) *Definieren wir* $x\overline{\Phi}_s := x\Phi_{x\vee s}$, *so folgt:* $a\,\overline{\Phi}_b\,\overline{\Phi}_{a\overline{\Phi}_c} = (a\vee b)\,\overline{\Phi}_c.$

BEWEIS. Es folgt fast unmittelbar aus (P1), dass $(L,\vee)$ sogar ein Verband ist – und zwar mit Minimum 0. Wir bezeichnen nun mit Φ_s den eindeutig bestimmten Antiautomorphismus, der 1 auf s abbildet. Auf diese Weise ist dann auch $\overline{\Phi}_s$ eindeutig bestimmt. Wir beachten als nächstes, dass (P1) zu jedem a,b ein x mit $a\Phi_x = b$ gewährleistet – und definieren:

$$\begin{aligned} x = ab &\;:\Leftrightarrow\; a\Phi_x = b \\ a * b &\;:=\; a\Phi_{a\vee b} \\ b : a &\;:=\; a\Phi^{-1}_{a\vee b}. \end{aligned}$$

Dann gelten für diese Festsetzungen zunächst $a,b \le ab$ und $(b:a)\Phi_{a\vee b} = a$ und somit weiter:

$$\text{(A1)} \qquad a * ab = b,$$

$$\text{(A2)} \qquad ab : b = b\Phi^{-1}_{ab} = a,$$

$$\text{(A31)} \qquad a(a*b) = a\vee b = b(b*a)$$

$$\text{(A32)} \qquad (b:a)a = a\vee b = (a:b)b,$$

Anwendung von (A2) führt wegen der Symmetrie in a,b weiter zu:

$$\begin{aligned} (a*b)*(a*c) &= a\overline{\Phi}_b\overline{\Phi}_{a\overline{\Phi}_c} \\ &= (a\vee b)\overline{\Phi}_c \\ &= (b*a)*(b*c) \end{aligned}$$

Und das liefert:

$$\begin{aligned} ab*c &= 1*(ab*c) \\ &= (ab*a)*(ab*c) \\ &= (a*ab)*(a*c) \\ &= b*(a*c). \end{aligned}$$

Auf diese Weise folgt, dass $(L,\vee)$ der *Halbverband* eines geeigneten ℓ-Gruppen-Kegels ist.
Bleibt der abelsche Fall zu klären. Hierzu fordern wir, dass alle Φ_s *involutorisch* seine. Dann erhalten wir:

$$\begin{aligned} a*ba &= (b*ba)*ba \\ &= b\Phi_{ba}\Phi_{ba} \\ &= b \end{aligned}$$

und damit
$$\begin{aligned} ab &= a(a * ba) \\ &= ba(ba * a) \\ &= ba, \end{aligned}$$

wegen $ab * a = ab\Phi_{ab\vee a} = ab\Phi_{ab} = 1$ und $s\Phi_s = 1$, also $s \cdot 1 = s$
Da die Notwendigkeit der Bedingungen (P1), (P2) schon gezeigt wurde sind wir hiermit am Ziel. □

8.2 ℓ-Gruppen-Verbände

Ist $(V, \vee, \wedge)$ ein ℓ-Gruppen-Verband, so lässt sich mittels der ℓ-Gruppen-Operationen nach (2.54) und (2.59) jedes Element auffassen als ein Produkt $(1 \vee a) \cdot (1 \wedge a)$ mit $1 \vee a) \wedge (1 \wedge b)^{-1} = 1$ und es gelten nach (2.58) die Gleichungen

$$\begin{aligned} & (1 \vee a) \cdot (1 \wedge a) \vee (1 \vee b) \cdot (1 \wedge b) \\ = \ & (1 \vee a) \vee (1 \vee b)) \cdot ((1 \wedge a) \vee (1 \wedge b)) \\ \text{UND} \quad & (1 \vee a) \cdot (1 \wedge a) \wedge (1 \vee b) \cdot (1 \wedge b) \\ = \ & (1 \vee a) \wedge (1 \vee b)) \cdot ((1 \wedge a) \wedge (1 \wedge b)), \end{aligned}$$

denn die linken Seiten sind gleich $a \vee b$ bzw. gleich $a \wedge b$.
Dies vor Augen gelingt uns eine Charakterisierung der ℓ-Gruppen-Verbände.

8. 2. 1 Theorem. $(L, \vee, \wedge)$ *ist ein ℓ-Gruppen-Verband gdw. er die Bedingungen* (L0), (L1), (L2), (L3) *erfüllt, was insbesondere einschließt, dass* $(\{x \mid x \geq 1\}, \vee, \wedge)$ *isomorph sei zu einem ℓ-Gruppen-Kegel-Verband.*

BEWEIS. Alles, was wir zu zeigen haben, ist die Hinlänglichkeit. Sei also $(L, \vee, \wedge)$ ein Verband, der die Bedingungen (L0), (L1), (L2), (L3) erfüllt mit dem ausgezeichneten Element 1 und * als fixiertem Antiisomorphismus von $N := \{x \mid x \leq 1\}$ auf $P := \{x \mid 1 \leq x\}$. Dann betrachten wir

$$L^* := \{(a \mid b) \,\Big|\, a \geq 1 \geq b \ \& \ a \wedge b^* = 1\}$$

unter
$$\begin{aligned} (a \mid b) \vee (c \mid d) &:= (a \vee c \mid b \vee d) \\ (a \mid b) \wedge (c \mid d) &:= (a \wedge c \mid b \wedge d). \end{aligned}$$

$(L^*, \vee, \wedge)$ ist abgeschlossen bezüglich $\vee$ und $\wedge$, wegen:

$$\begin{aligned} a \wedge b^* = 1 = c \wedge d^* \;&\Rightarrow\; (a \vee c) \wedge (b \vee d)^* \\ &= (a \vee c) \wedge (b^* \wedge d^*) \\ &= (a \wedge b^* \wedge d^*) \vee (c \wedge b^* \wedge d^*) \\ &= 1. \end{aligned}$$

und
$$\begin{aligned} a \wedge b^* = 1 = c \wedge d^* \;&\Rightarrow\; (a \wedge c) \wedge (b \wedge d)^* \\ &= (a \wedge c) \wedge (b^* \vee d^*) \\ &= (a \wedge c \wedge b^*) \vee (a \wedge c \wedge d^*) \\ &= 1. \end{aligned}$$

Als nächstes gilt:

(i) $(L, \vee, \wedge)$ ist isomorph zu $(L^*, \vee, \wedge)$.

(ii) $(L^*, \vee)$ ist isomorph zu dem Verband einer jeden ℓ-Gruppe deren Kegel *verbandsisomorph* ist zu $(\{x \mid x \geq 1\}, \vee, \wedge)$.

Ad (i) : $(L^*, \vee, \wedge)$ ist distributiv wegen (L0). Wir definieren $\psi : L \to L^*$ mittels $\psi(x) := (1 \vee x \mid 1 \wedge x)$. Dann liegt nach (L2) $\psi(x)$ in L^*. Weiterhin ist ψ nach (L3) surjektiv, und wegen der Verbands-Distributivität ist ψ auch *injektiv,* wegen $1 \vee x = 1 \vee y \;\&\; 1 \wedge x = 1 \wedge y \Longrightarrow x = y$.
Schließlich folgt:

$$\begin{aligned} \psi(x \vee y) &= \Big(1 \vee (x \vee y) \,\Big|\, 1 \wedge (x \vee y)\Big) \\ &= \Big((1 \vee x) \vee (1 \vee y) \,\Big|\, (1 \wedge x) \vee (1 \wedge y)\Big) \\ &= (1 \vee x \mid 1 \wedge x) \vee (1 \vee y \mid 1 \wedge y) \\ &= \psi(x) \vee \psi(y), \end{aligned}$$

und es ergibt sich analog

$$\psi(x \wedge y) = \psi(x) \wedge \psi(y),$$

Ad (ii) : Wir erinnern zunächst daran, dass in $(L, \vee, \wedge)$ der Unterverband $(\{x \mid x \geq 1\}, \vee, \wedge)$ isomorph angenommen ist zu einem ℓ-Gruppen-Kegel-Verband.
Sei hiernach $(G, \vee, \wedge)$ ein solcher ℓ-Gruppen-Kegel-Verband der ℓ-Gruppe $(G, \cdot, ^{-1}, \vee, \wedge, e)$. Dann erfüllt $(G, \cdot, ^{-1}, \vee, \wedge, e)$ die aufgestellten Bedingungen bezüglich $^{-1}$ für Φ mit e als 1.
Weiter ist jedes $x \in L$ aufgespalten in $(1 \vee x \mid 1 \wedge x)$ so wie jedes $a \in G$ aufgespalten ist in $(1 \vee a) \cdot (1 \wedge a)$.

Wir stiften nun in $\mathfrak{G}$ die Zuordnung

$$\phi : a = (1 \vee a) \cdot (1 \wedge a) \mapsto (1 \vee a \,|\, 1 \wedge a).$$

Diese Zuordnung ist bijektiv, wie wir oben sahen, und es gelten:

$$\begin{aligned}
\phi(a \vee b) &= (1 \vee a \vee b \,|\, 1 \wedge (a \vee b)) \\
&= ((1 \vee a) \vee (1 \vee b) \,|\, (1 \vee a) \wedge (1 \vee b)) \\
&= ((1 \vee a) \,|\, (1 \wedge a)) \vee ((1 \vee b)(1 \wedge b)) \\
&= \phi(a) \vee \phi(b)
\end{aligned}$$

und analog

$$\phi(a \wedge b) = \phi(a) \wedge \phi(b)$$

Damit sind wir am Ziel. $\square$

Kapitel 9

Kommutative Bricks

9.1 Vorbemerkungen

Schon im Kapitel über Kegelalgebren haben wir den Brick eingeführt und gesehen, dass sich jeder Verbandsgruppenkegel, aufgefasst als Kegelalgebra, in einen Brick einbetten lässt. Somit sind Bricks aufs engste gekoppelt mit der Verbandsgruppe und andererseits aufs engste *assoziiert* mit der booleschen Algebra. Genauer: Theorie der Bricks ist zum einen in einer gewissen Weise nichts anderes als Theorie der Verbandsgruppen, und sie ist zum anderen nichts anderes als eine abgeschwächte Theorie der booleschen Algebra. Denn, es lässt sich jeder Brick auffassen als eine selbstduale Algebra $\mathfrak{B} := (B, \bigtriangledown, \bigtriangleup, *, \star)$ vom Typ $(2, 2, 1, 1)$, deren Gesetze bei entsprechender Deutung der Operationen ausnahmslos auch erfüllt werden von der booleschen Algebra.
So gesehen scheint eine Theorie der Bricks *cum grano salis* längst geschrieben, doch ist zu beachten, dass beim Übergang vom Kegel zu seiner Brickerweiterung ganz wesentliche *algebraische* und *ordnungstheoretische* Eigenschaften verloren gehen. So werden beispielsweise Archimedizität und Vollständigkeit zwangsläufig „zerstört“, wie man sofort sieht! Es ist ja jedes a' obere Grenze zu allen a des Kegels. Andererseits pflanzen sich Kongruenzen des Kegels eindeutig auf den Brick fort.
Denn: $a \equiv b'$ führt zu $0 = b \cdot b' \equiv b \cdot a = 0$. Es ist aber das Bild eines Kegels stets wieder ein Kegel, also multiplikativ kürzbar, und folglich dann für alle Elemente der Brickerweiterung eines Kegels $0 \equiv x$ erfüllt. Somit bleibt nur der Fall, in dem kein Kegelelement a zu einem hinzu genommenen b' kongruent ist, also $a' \equiv b'$ genau dann gilt, wenn $a \equiv b$ erfüllt ist.
Auch ist zu bedenken, dass sich der Brick noch dort als Hilfsstruktur

bewährt, wo eine Verbandsgruppe nicht unmittelbar auszumachen ist, man denke etwa an den Kommutativitätsbeweis für *archimedische d-Halbgruppen.* Andererseits: Die Nähe des Brick zur Verbandsgruppe und zur booleschen Algebra ist deutlich, so dass sich Fragen nach Gemeinsamkeiten dieser Strukturen als Fragen der Bricktheorie geradezu aufdrängen.

Unser Anliegen kann es an dieser Stelle natürlich höchstens sein, durch einige *Proben* zu vermitteln, wie Brick-Theorie arbeitet, um auf diese Weise exemplarisch zu unterlegen, wie sich Verbandsgruppen und boolesche Algebren ineins führen lassen.

Hierzu gehen wir von vorne herein aus von *symmetrischen* Bricks.

Brick bedeute also in diesem Kapitel stets: **Symmetrischer Brick.**
Wir haben uns für die Bezeichnung symmetrischer Brick entschieden, obwohl viele äquivalente Beschreibungen im Umlauf sind und die Wahl MV-Algebra zu Ehren von CHANG eine Alternative ist. Tatsächlich betont aber MV den logischen Aspekt, wohingegen Brick neutralisiert.[1)]

Imd en Voirdergrund rücken wir zunächst einige

9.2 Axiomatische Aspekte

Unser erstes Ziel ist die Untersuchung einiger Gleichungssysteme, die Bricks unter verschiedenen Sichtweisen beschreiben, so wie wir es bei Booleschen Algebren schon kennen gelernt haben.

9. 2. 1 Proposition. *Sei* $\mathfrak{B}$ *ein Brick. Definiere* $a \circ b := (b * (a * 0)) * 0$ *und* $a' := a * 0$. *Dann erfüllt* $\mathfrak{B}$ *die Gleichungen:*

$$\begin{array}{llcl}
\text{(CS1)} & a \circ (b \circ c) & = & b \circ (a \circ c) \\
\text{(CS2)} & a \circ 0 & = & 0 \\
\text{(CS3)} & a \circ 0' & = & a \\
\text{(CS4)} & a \circ (a \circ b')' & = & b \circ (b \circ a')'.
\end{array}$$

DENN: Es gelten nacheinander:

$$\text{(9.5)} \qquad a \circ b = b \circ a$$

[1)] **Der interessierte Leser sei hingewiesen auf [126], wo eine Theorie der Bricks gegeben wird, allerdings unter weitgehender Außerachtlassung der nachfolgenden Herleitungen, die so gesehen als eine Ergänzung des wissenschaftsdidaktischen hochkarätigen Beitrages von** CIGNOLI, D'OTTAVIANO, MUNDICI **angesehen werden dürfen.**

$$\begin{aligned}
a \circ (b \circ c) &= ((b \circ c) * (a * 0)) * 0 \\
&= (((c * (b * 0)) * 0) * (a * 0)) * 0 \\
&= (a * (c * (b * 0))) * 0 \\
&= (b * (c * (a * 0))) * 0 \\
&= c \circ (b \circ a) \\
&= a \circ (b \circ c)\,.
\end{aligned} \tag{9.6}$$

$$\begin{aligned}
a \circ 0 &= (0 * (a * 0)) * 0 \\
&= (a * (0 * 0)) * 0 \\
&= 0\,.
\end{aligned} \tag{9.7}$$

$$\begin{aligned}
a \circ 0' &= (0' * (a * 0)) * 0 \\
&= (1 * (a * 0)) * 0 \\
&= (a * 0) * 0 \\
&= a\,.
\end{aligned} \tag{9.8}$$

$$\begin{aligned}
a \circ (a \circ b')' &= a \circ (((b' * (a * 0)) * 0) * 0) \\
&= a \circ ((a * (b' * 0)) \\
&= a \circ (a * b) \\
&= ((a * b) * (a * 0)) * 0 \\
&= ((b * a) * (b * 0)) * 0 \\
&= b \circ (b \circ a')'.
\end{aligned} \tag{9.9}$$

□

Mit anderen Worten: ein Brick lässt sich auch auffassen als ein kommutatives Monoid mit involutorischem Operator $'$. Nun zeigen wir

9. 2. 2 Proposition. *Sei* $\mathfrak{S} := (S, \circ, ', 0)$ *eine Algebra vom Typ* $(2, 1, 0)$, *die den Gleichungen* (CS1) *bis* (CS4) *genügt. Dann bildet* S *einen Brick bezüglich* 0 *und der Operation* $a * b := (a \circ b')'$.

BEWEIS. Nach (CS1) und (CS3) gilt $a \circ b = b \circ a$. Weiter haben wir mit $1 := 0'$ zunächst nach (CS4) auch $1' = 0$ und damit:

$$0'' = 1 \circ 1' = 0\,. \tag{9.10}$$

$$\begin{aligned} a'' &= 1\circ(1\circ a')' \\ &= a\circ(a\circ 1')' \\ &= a\circ(a\circ 0)' \\ &= a\circ 0' \\ &= a. \end{aligned} \tag{9.11}$$

Hieraus folgt weiter

$$a\circ a' = a\circ(a\circ 0')' = 0\circ(0\circ a')' = 0\,. \tag{9.12}$$

$$\begin{aligned} (a*a)*b &= ((a\circ a')'\circ b')' \\ &= (0'\circ b')' \\ &= b'' = b \end{aligned} \tag{9.13}$$

und damit

$$\begin{aligned} a*(b*c) &= (a\circ(b*c)')' \\ &= (a\circ((b\circ c')')')' \\ &= (a\circ(b\circ c'))' \\ &= ((a\circ b)\circ c'))' \\ &= (a\circ b)*c)\,, \\ &= b*(a*c)\,. \end{aligned} \tag{9.14}$$

Tatsächlich gilt also etwas mehr, nämlich

$$(a\circ b)*c = b*(a*c))\,. \tag{9.15}$$

Somit ist $(S,\circ,*)$ eine komplementäre Halbgruppe, und es gilt offenbar $a*b=(b*0)*(a*0)$. Das sichert als nächstes

$$\begin{aligned} (a*b)*b &= \big((b*0)*(a*0))\big)*\big((b*0)*0\big) \\ &= (b*a)*a \end{aligned} \tag{9.16}$$

Zu zeigen bleibt:

$$\begin{aligned} 0*a &= (0\circ a')' \\ &= 0' \\ &= (a\circ a')' \\ &= a*a\,. \end{aligned} \tag{9.17}$$

□

9. 2. 3 Definition. Unter einer kommutativen *Halbgruppe mit Komplementen* verstehen wir eine Algebra $(S,\circ,{}',0)$, die den Axiomen (CS1) bis (CS4) genügt.

9. 2. 4 Proposition. *Sei $\mathfrak{B}$ ein Brick. Definiere $a * b$ und a' wie oben. Dann bildet B bezüglich $\circ$ und $'$ eine Halbgruppe mit Komplementen $\mathfrak{C}(\mathfrak{B})$. Sei $\mathfrak{C}$ eine kommutative Halbgruppe mit Komplementen. Definiere $*$ und 0 wie oben. Dann bildet C bezüglich 0 und $*$ einen Brick $\mathfrak{B}(\mathfrak{C})$. Darüber hinaus gelten die Operatorgleichungen:*

$$\mathfrak{B} \cong \mathfrak{B}(\mathfrak{C}(\mathfrak{B})) \quad \text{und} \quad \mathfrak{C} \cong \mathfrak{C}(\mathfrak{B}(\mathfrak{C}))\,. \tag{9.18}$$

BEWEIS. Es ist nur noch die Gültigkeit der behaupteten Gleichungen zu zeigen.

(a) Wir gehen aus von einem Brick $\mathfrak{B}$. Bezeichnen wir die Operationen von $\mathfrak{B}(\mathfrak{C}(\mathfrak{B}))$ mit $\bar{*}$ und $\bar{0}$, so erhalten wir:

$$\begin{aligned} a\bar{*}b &= (a \circ b')' \\ &= ((b' * (a * 0)) * 0)' \\ &= (((b * 0) * (a * 0)) * 0)' \\ &= (b * 0) * (a * 0) \\ &= a * ((b * 0) * 0) \\ &= a * b \end{aligned} \tag{9.19}$$

$$\bar{0} = a \circ a' = (\,a' * a'\,)' = 0\,. \tag{9.20}$$

(b) Hiernach gehen wir aus von einer kommutativen Halbgruppe mit Komplementen $\mathfrak{C}$ und bezeichnen die Operationen von $\mathfrak{C}(\mathfrak{B}(\mathfrak{C}))$ mit $\bar{\circ}$ und $^+$. Dann resultiert die Behauptung aus den beiden Gleichungen:

$$\begin{aligned} a\bar{\circ}b &= (a * (b * 0)) * 0 \\ &= ((a \circ (b * 0)')')' \\ &= a \circ (b * 0)' \\ &= a \circ ((b \circ 0')')' \\ &= a \circ b \end{aligned} \tag{9.21}$$

$$a^+ = a * 0 = (a \circ 0')' = a'\,. \tag{9.22}$$ □

Wie schon erwähnt, ist die Theorie der Bricks eng verbunden mit der Theorie der Verbandsgruppen, da jeder Brick kanonisch in einen Verbandsgruppenkegel und jeder Verbandsgruppenkegel kanonisch in einen Brick eingebettet werden kann.

Auf der anderen Seite stellt sich heraus, dass $'$ ein involutorischer Operator ist, weshalb mit $a \triangledown b := a \circ b$ und $a \vartriangle b := (a' \circ b')'$ jeder Brick zu einer selbstdualen Algebra $(B, \triangledown, \vartriangle, {}')$ wird.
Folglich kann der Brick als eine nicht idempotente boolesche Algebra aufgefasst werden, die *per definitionem* die DE MORGANschen Gesetze erfüllt. Der Vollständigkeit halber scheint es wünschenswert, hierfür einen gesonderten Begriff und eine typische selbstduale Menge von Axiomen zu haben. Wir schlagen den Namen *dualer Brick* vor und erklären:

9. 2. 5 Definition. Sei $\mathfrak{B} := (B, \triangledown, \vartriangle, {}')$ eine Algebra vom Typ $(2, 2, 1)$. Dann heiße $\mathfrak{B}$ ein *dualer Brick,* wenn $\mathfrak{B}$ die Gleichungen des Brick sowohl bezüglich $\vartriangle$ und $'$ als auch bezüglich $\triangledown$ und $'$ erfüllt und zudem bezüglich $\triangledown$ und $\vartriangle$ mindestens eine und damit beide DE MORGANschen Regeln gelten.

Offensichtlich folgt aus dieser Definition, dass $a \vartriangle a'$ bezüglich $\triangledown$ und $a \triangledown a'$ bezüglich $\vartriangle$ die Rolle einer Eins übernehmen, denn aus den DE MORGANschen Regeln resultiert $a \triangledown (b \vartriangle b') = a \triangledown ((b \vartriangle b')')' = a \triangledown (b' \triangledown b)' = a$ und analog die duale Gleichung.
Schließlich kommen wir zu einer Verallgemeinerung eines Satzes von GLIVENKO, nach dem die abgeschlossenen Elemente eines brouwerschen Halbverbandes mit 0 einen booleschen Verband bilden:

9. 2. 6 Proposition. *Sei $(S, \cdot, *)$ eine kommutative komplementäre Halbgruppe und sei c beliebig aus S. Dann bilden die Elemente $a_c := a * c$ einen Brick bezüglich $*$.*

BEWEIS. Wir haben zu zeigen, dass die Menge aller a_c abgeschlossen ist unter $*$ und dass diese Menge die Gleichung $(a_c * b_c) * b_c = (b_c * a_c) * a_c$ erfüllt. Es ist aber $a_c * b_c = (a * c) * (b * c) = b(a * c) * c$, und es gilt:

$$
\begin{aligned}
& (a_c * b_c) * b_c \\
= \; & ((a * c) * (b * c)) * (b * c) \\
= \; & ((a * c) * (((b * c) * c) * c)) * (((b * c) * c) * c) \\
= \; & (((b * c) * c) * ((a * c) * c)) * (((b * c) * c) * c) \\
= \; & (b_c * a_c) * a_c,
\end{aligned}
\tag{9.23}
$$

da die vorletzte *Termfunktion* symmetrisch ist in a und b. □

9.3 Darstellungen

In diesem Abschnitt geben wir zwei Darstellungssätze für beliebige Bricks, die im klassischen Fall boolescher Algebren mit dem STONEschen Darstellungssatz zusammenfallen und die an wohlbekannte Sätze von JAFFARD und KEIMEL angelehnt sind.
Wie üblich verstehen wir unter einem BÉZOUT-Ring einen kommutativen Ring $\mathfrak{R}$ mit Eins, dessen endlich erzeugten Ideale Hauptideale sind, und wir bezeichnen die Halbgruppe $\mathfrak{D}$ aller Hauptideale von $\mathfrak{R}$ als die Teilbarkeitshalbgruppe von $\mathfrak{R}$. In Übereinstimmung hiermit sprechen wir von einem BÉZOUT-Bereich, wenn der unterliegende Ring sogar ein Integritätsbereich ist.

9. 3. 1 Lemma. *In einem* BÉZOUT*-Bereich ist jedes Quotientenideal* $(a):(b)$ *ein Hauptideal.*

DENN: $(a,b)=(d)$ impliziert $b \,\big|\, ax \Longrightarrow b \,\big|\, (a,b)x \Longrightarrow b \,\big|\, dx \Longrightarrow (b/d) \,\big|\, x$ und damit $(b):(a)=(b/d)$. □

Als nächstes erhalten wir:

9. 3. 2 Proposition. *Sei* $\mathfrak{R}$ *ein Bézout-Bereich und* c *verschieden von* 0. *Dann bilden die Hauptideale von* $\mathfrak{R}/(c) := \mathfrak{R}_c$ *einen Brick bezüglich*

$$(\overline{a})\cdot(\overline{b}) = (\overline{a\cdot b}) \quad \textit{und} \quad (\overline{a})' = (\overline{c}):(\overline{a},\overline{c})$$

BEWEIS. Zunächst gilt die Implikation

$$\begin{aligned}(a,c)=(t) \;&\Longrightarrow\; t = ax+cy\\ &\Longrightarrow\; \overline{t} = \overline{a}\cdot\overline{x}\\ &\Longrightarrow\; \overline{t}\,\big|\,\overline{a} \;\&\; \overline{a}\,\big|\,\overline{t}\\ &\Longrightarrow\; (\overline{a}) = (\overline{t})\,,\end{aligned}$$

also ist jedes Ideal aus $\mathfrak{R}_c$ ein Hauptideal $(\overline{t})$ mit $t \,\big|\, c$.
Weiter gilt im Falle $b \,\big|\, c$ die Implikation

$$\begin{aligned}\overline{b}\,\big|\,\overline{a}\cdot\overline{x} \;&\Longrightarrow\; \overline{b}\overline{y} = \overline{ax}\\ &\Longrightarrow\; c\,\big|\,ax-by\\ &\Longrightarrow\; cu+by = ax\\ &\Longrightarrow\; b\,\big|\,ax\\ &\Longrightarrow\; \overline{b}\,\big|\,\overline{a}\cdot\overline{x}\end{aligned}$$

und damit

$$\bar{b} \,\big|\, \bar{a} \cdot \bar{x} \iff b \,\big|\, ax\,,$$

woraus wegen der Bézout-Eigenschaft von $\mathfrak{R}$ die Behauptung resultiert. □

Sei hiernach $\mathfrak{B}$ ein Brick und $\mathfrak{C}(\mathfrak{B})$ der zu $\mathfrak{B}$ gehörige Verbandsgruppenkegel. Es ist nach einem Satz von Jaffard wohlbekannt, dass $\mathfrak{C}(\mathfrak{B})$ darstellbar ist als Teilbarkeitshalbgruppe eines Integritätsbereiches ([101]). Hier soll nun unter Anwendung einer Methode aus [79] ein kommutativer Ring konstruiert werden, dessen Teilbarkeitshalbgruppe isomorph ist zu $\mathfrak{B}$.

9. 3. 3 Proposition. *Sei $\mathfrak{B}$ ein Brick. Dann gibt es einen Bézout-Ring $\mathfrak{R}$, derart, dass $(B, \cdot\,)$ eine Unterhalbgruppe von $(R, \cdot\,)$ und $\mathfrak{B}$ isomorph zur Teilbarkeitshalbgruppe $\mathfrak{D}$ von $\mathfrak{R}$ ist.*

BEWEIS. Wir gehen aus von Summen $\alpha = a_1 + a_2 + \cdots + a_n \ \ (a_i \in C)$, aufgefasst als Elemente des Gruppenrings von $\mathfrak{G}(\mathfrak{C}(\mathfrak{B}))$ über dem zweielementigen Körper $\mathfrak{Z}_2$. Die Elemente sind kanonisch von der Form $a_1 + \ldots + a_n$, und definieren wir $d(\alpha) := a_1 \wedge a_2 \wedge \ldots \wedge a_n$, so erhalten wir nach [79] $d(\alpha)d(\beta) = d(\alpha\beta)$.
Es ist nun ein spezieller Bézout-Ring zu konstruieren. Dazu beachten wir, dass die Menge E der Elemente

$$a_1 + \cdots + a_n \ \ (a_1 \wedge \cdots \wedge a_n = 1)$$

multiplikativ abgeschlossen ist. Folglich können wir nach dieser Menge *lokalisieren.* Auf diese Weise gelangen wir zu einem Ring, dessen Elemente sich in der Form

$$\alpha \cdot (a_1 + \cdots + a_n) \ \ (a_1 \wedge \cdots \wedge a_n = 1)\,,$$

schreiben lassen, worin α und die $a_i \ \ (1 \leq i \leq n)$ Produkte aus B sind.
Vorweg bezeichnen wir als ein ε jedes Element aus E. Gilt dann $a, b \in C$, so sind die Hauptideale $(a\varepsilon_a)$ und $(b\varepsilon_b)$ genau dann gleich, wenn $a = b$ erfüllt ist. Denn wegen der Eindeutigkeit der Summendarstellungen teilen die beiden Elemente a, b in $\mathfrak{C}(\mathfrak{B})$ einander, wenn $a\varepsilon_a$ und $b\varepsilon_b$ in $\mathfrak{C}(\mathfrak{B})$ einander teilen. Dies bedeutet natürlich im Sonderfall $a, b \in B$, dass a und b schon im Ausgangsbrick einander teilen.
Also ist $\phi \,:\, a \longrightarrow (a)$ ein Isomorphismus von $\mathfrak{C}(\mathfrak{B})$ auf die Teilbarkeitshalbgruppe von $\mathfrak{I}$. Zusätzlich dürfen wir annehmen, dass B eine Teilmenge von I ist.

Es ist zu zeigen, dass $\mathfrak{J}$ ein BÉZOUT-Ring ist. Dies resultiert aber aus $(a\varepsilon_a, b\varepsilon_b) = (a,b) = (a \wedge b) \cdot (a * b, b * a) = (a \wedge b)(1)$ nach unserer Konstruktion.

Hiernach gelangen wir wie folgt ans Ziel: Sei c die 0 von $\mathfrak{B}$. Wir betrachten $\mathfrak{D}_c$. Dann induziert ϕ einen Isomorphismus zwischen der Teilbarkeitshalbgruppe $\mathfrak{D}_c$ von $\mathfrak{J}/(c)$ und $\mathfrak{B}$. Denn man beachte:

(*i*) $\overline{\phi} : a \longrightarrow (\overline{a})$ ist eine Funktion.

(*ii*) Es gilt $(\overline{a}) = (\overline{a \wedge c})$ für alle $a \in C(B)$, denn $(\overline{a \wedge c})$ besitzt einen Erzeuger der Form $\overline{a} \bar{\cdot} \overline{x} \mathbin{\overline{+}} \overline{y} \bar{\cdot} \overline{c}$, woraus die Existenz eines Erzeugers der Form $\overline{a \cdot x}$ resultiert und damit die Gleichung $(\overline{a}) = (\overline{a \wedge c})$, wie behauptet.

(*iii*) $\overline{\phi}$ ist ein Homomorphismus, denn wegen (*ii*) erhalten wir $(\overline{a})\ (\overline{b}) = (\overline{ab}) = (\overline{c \wedge ab}) = (\overline{a \circ b})$.

(*iv*) $\overline{\phi}$ ist bijektiv, denn haben wir $(\overline{a}) = (\overline{b})$ mit $a, b \mid c$, so folgt vorweg für geeignete x, y die Beziehung $c \mid (ax - b)\ \&\ c \mid (by - a)$, woraus weiter $a \mid b\ \&\ b \mid a$ und somit $a = b$ resultiert.

□

Als Sonderfall liefert 9.3.3:

9. 3. 4 Proposition. *Sei $\mathfrak{B}$ eine boolesche Algebra und sei weiter $\mathfrak{J}_0$ der im Sinne von 9.3.3 zu $\mathfrak{B}$ gehörige Ring. Dann ist $\mathfrak{B}$ als Verband isomorph zu $\mathfrak{D}_0$ und $\mathfrak{D}_0$ seinerseits isomorph zum Verband der Idempotenten von $\mathfrak{J}_0$. Folglich lässt sich auf $\mathfrak{D}_0$ eine Addition definieren, so dass D_0 zu einem booleschen Ring wird, derart dass diese Addition überein stimmt mit $(a' \vee b) \wedge (b' \vee a)$.*

BEWEIS. Es ist zu zeigen, dass sich $+$ als boolesche Operation darstellen lässt, wie im Satz behauptet. Offenbar gilt aber für idempotente Elemente aus $\mathfrak{J}_0$

$$xa = 0 \Longleftrightarrow x(a+1) = x \Rightarrow x \geq a+1\,,$$

und damit $a * 0 = a + 1$, und wir haben $a \wedge b = a + ab + b$ sowie $ab = a \vee b$.

und hieraus resultiert

$$\begin{aligned} a+b &= (a+ab+b)+ab \\ &= (a\wedge b)+(a\vee b) \\ &= (a\wedge b)(1+((b*a)\vee(a*b))) \\ &= (a\wedge b)(1+((b'\wedge a)\vee(a'\wedge b)) \\ &= (a\wedge b)((a'\vee b)\wedge(b'\vee a)) \\ &= (a'\vee b)\wedge(b'\vee a). \end{aligned}$$

Also ist gezeigt, dass wir den Ring von STONE erhalten, wenn wir auf $(B,\cdot)$ die von $(R,+,\cdot)$ induzierte Addition definieren. □

Im zweiten Teil dieses Abschnitts diskutieren wir topologische Darstellungen. Im klassischen Fall boolescher Algebren besagt ein Theorem von M. H. STONE, dass jeder booleschen Algebra umkehrbar eindeutig ein *boolescher Raum* zugeordnet ist, also ein *total unzusammenhängender kompakter* HAUSDORFF-*Raum.* Dieser Raum wird mit Hilfe der irreduziblen Ideale von $\mathfrak{B}$ auf wohlbekannte Weise konstruiert. Des weiteren ist gut bekannt, dass die lange Reihe von Beiträgen zu *topologischen Darstellungen* algebraischer Strukturen initiiert wurde von STONE [146] und schließlich zu einer erweiterten Theorie der *Garbendarstellungen* führte – siehe [114],[115]. Daher sind wir in der erfreulichen Situation, auf KEIMEL [114] [2] verweisen zu können, und es ist leicht zu sehen, dass diese Resultate bereits aus viel schwächeren Bedingungen als denen der abelschen Verbandsgruppe folgen. Deshalb beschränken wir uns an dieser Stelle darauf, ein Ergebnis aus [114] wie folgt zu übernehmen:
Studiere die Abschnitte 2 und 3 aus [114]. Dann folgt:

9. 3. 5 Proposition. *Sei $\mathfrak{B}$ ein Brick. Dann ist $\mathfrak{B}$ isomorph zum Brick aller Schnitte der Garbe $F(\mathfrak{B}, \mathrm{Spec}\,\mathfrak{B})$ über* $\mathrm{Spec}\,\mathfrak{B}$*, (wobei die Halme dieser Garbe linear geordnete Bricks sind).*

BEWEIS. Man konsultiere KEIMEL, [114]. □

Ist $\mathfrak{B}$ sogar boolesch, so ist klar, dass diese Darstellung aus 9.3.5 überein stimmt mit der STONEschen Darstellung boolescher Algebren als boolesche Räume, denn in diesem Fall sind die Halme zweielementige Algebren, weshalb die Schnitte mit ihrem (*clopen*) Träger identifiziert werden können.

[2] Man beachte, dass die dort eingehenden Begriffe, wie c-Ideal, primes c-Ideal, direkter Faktor, Polare, die boolesche Algebra der direkten Faktoren bzw. der Polaren, Projizierbarkeit und Repräsentierbarkeit untersucht und damit bereit gestellt werden, so dass eine Übertragung der zentralen Ergebnisse aus [115] auf Bricks zur Sache der Routine wird.

9.4 Vollständige Bricks

Vollständige Bricks waren bereits Gegenstand unserer Untersuchungen in [25]. Dort spielten sie eine entscheidende Rolle beim Beweis des Satzes

Archimedische d-Halbgruppen sind kommutativ.

Insbesondere sahen wir in diesem Zusammenhang, dass sich ein Brick genau dann in einen *vollständigen* Brick einbetten lässt, wenn er *ganz-abgeschlossen* ist, d. h., wenn er die Bedingung erfüllt:

$$\text{(G)} \qquad \forall t \neq 1, a \in Q\ \exists\, n \in \mathbf{N}:\ t^n * a \not\geq t \not\leq a : t\ .$$

Ferner sahen wir, dass vollständige Bricks eine optimale *Grenz-Arithmetik* besitzen, die sich ausdrückt in

$$
\begin{array}{llcl llcl}
(\mathrm{D1}\bigwedge) & x\big(\bigwedge a_i\big) & = & \bigwedge(xa_iy) & (\mathrm{D1}\bigvee) & x\big(\bigvee a_i\big)y & = & \bigvee(xa_iy) \\
(\mathrm{D2}\bigwedge) & x \vee \bigwedge a_i & = & \bigwedge(x \vee a_i) & (\mathrm{D2}\bigvee) & x \wedge \bigvee a_i & = & \bigvee(x \wedge a_i) \\
(\mathrm{D3}\bigwedge) & x * (\bigwedge a_i) & = & \bigwedge(x * a_i) & (\mathrm{D3}\bigvee) & x * (\bigvee a_i) & = & \bigvee(x * a_i) \\
(\mathrm{D4}\bigwedge) & (\bigwedge a_i) * x & = & \bigvee(a_i * x) & (\mathrm{D4}\bigvee) & (\bigvee a_i) * x & = & \bigwedge(a_i * x)
\end{array}
$$

Vollständige Bricks sind vollständige d-Halbgruppen und damit kommutativ. Da ihre spezielle *Grenz-Arithmetik* bereits in [25] geklärt wurde, wollen wir uns hier auf Darstellungsmöglichkeiten konzentrieren.

9. 4. 1 Lemma. *Sei $\mathfrak{B}$ ein Brick. Dann bilden die Idempotenten von $\mathfrak{B}$ eine boolesche Unteralgebra von $\mathfrak{B}$ bezüglich der Operationen $\cdot, \wedge$ und $'$.*

BEWEIS. Dies wurde bereits allgemein unter 3.3.13 gezeigt. □

Schon beim Studium vollständiger d-Halbgruppen sind wir auf subdirekte Zerlegungen nach Idempotenten gestoßen. Zu beachten bleibt jedoch, dass die Operation $*$ dort im Hintergrund stand. Auch ist klar, dass ein vollständiger Brick wegen seiner starken Arithmetik sehr viel stärkere Resultate erwarten lässt als d-Halbgruppen.

9. 4. 2 Proposition. *Sei $\mathfrak{B}$ ein vollständiger Brick und sei $a \not\leq b$ & $b \not\leq a$ erfüllt. Dann gibt es eine direkte Zerlegung $\mathfrak{U} \times \mathfrak{V}$ von $\mathfrak{B}$, so dass die Komponenten von a und b paarweise vergleichbar sind.*

BEWEIS. Definiere

$$U := \{x \,\big|\, a*b \wedge x = 1\} \quad \text{und} \quad V := \{y \,\big|\, \forall\, x \in U : x \wedge y = 1\}\,.$$

Dann erfüllt $u := \bigvee x\,(x \in U)$ nach den Regeln der Arithmetik vollständiger Bricks,

$$(a*b)*u \;=\; \bigvee (a*b)*x = \bigvee x \;\; (x \in U) = u\,.$$

Also gilt $(a*b) \wedge u = 1$ und damit

$$u := \bigvee\nolimits_{x \in U} x \in U \quad \text{und} \quad v := \bigvee\nolimits_{y \in V} y \in V\,.$$

Wir betrachten u^2 und v^2. Hier folgt $u^2 \wedge v^2 = (u \wedge v)^2 = 1$ und somit $u^2 \in U$ und $v^2 \in V$. Also sind u und v *orthogonale* Idempotente. Andererseits haben wir $uv = 0$, denn aus $u*u' = u*(u*0) = u*0 = u'$ folgt $u \wedge u' = 1$ und damit $u' \leq v$, also $uv \geq uu' = 0$.
Hiernach konstruieren wir einen Isomorphismus zwischen $\mathfrak{B}$ und $(U,*,u) \times (V,*,v)$. Wir erklären:

$$\phi : c \;\longrightarrow\; (u \wedge c, v \wedge c)\,.$$

Offensichtlich ist ϕ eine Funktion. Weiter ist ϕ injektiv, denn

$$\begin{array}{rcl} u \wedge c = u \wedge d & \& & v \wedge c = v \wedge d \\ & \Longrightarrow & \\ c & = & (u \wedge v \wedge c)c \wedge 0 \\ & = & (u \wedge c)(v \wedge c) \\ & = & (u \wedge d)(v \wedge d) = d\,. \end{array}$$

Ferner ist ϕ surjektiv, denn im Fall $x \leq u$ & $y \leq v$ erhalten wir

$$\begin{array}{lrcll} & xy \wedge u & = & (x \vee y) \wedge u = (x \wedge u) \vee (y \wedge u) & = x \\ \text{und} & xy \wedge v & = & \ldots & = y. \end{array}$$

Zu zeigen bleibt $\phi\,(c) * \phi\,(d) = \phi\,(c*d)$, d.h.

$$\begin{array}{rcl} u \wedge (c*d) & = & (u*(c*d))*(c*d) \\ & = & ((u*c)*(u*d))*(c*d) \\ & = & ((c*u)*(c*d))*(c*d) \\ & \overset{(6.20)}{=} & c*((d*u)*u) \\ & = & (d*u)*(c*u) \\ & = & ((c*u)*u)*((d*u)*u) \\ & = & (u \wedge c)*(u \wedge d)\,. \end{array}$$

Damit sind wir am Ziel. □

9. 4. 3 Definition. Sei $\mathfrak{B}$ ein Brick. Dann bezeichnen wir mit $\mathfrak{B}(I)$ die *boolesche Unteralgebra der Idempotenten* aus $\mathfrak{B}$.

9. 4. 4 Definition. Im weiteren bezeichne $\mathfrak{E}$ *das reelle Einheitsintervall* $\mathbf{E}$, betrachtet als Brick bezüglich der Operation $a * b := \max(0, b - a)$.
Ferner bezeichne $\mathfrak{S}_n$ die Menge $\{1, \ldots, n\} \subseteq \mathbf{N}$, betrachtet als Brick bezüglich $a * b := \max(n, b - a)$.
Schließlich bedeute *Würfel* im weiteren ein *direktes Produkt,* dessen Faktoren ausnahmslos isomorph sind zu $\mathfrak{E}$ und *Gitterwürfel* ein direktes Produkt, dessen Faktoren ausnahmslos isomorph sind zu einem $\mathfrak{S}_n$.

Dann folgt als ein erster Struktursatz:

9. 4. 5 Proposition. *Sei* $\mathfrak{B}$ *ein vollständiger Brick und* p *ein* Atom *von* $\mathfrak{B}(I)$ *d. h. es gebe kein Idempotent* u *mit* $1 < u < p$. *Dann ist das* Intervall $[1, p]$ *isomorph zu* $\mathfrak{E}$ *oder zu einem* $\mathfrak{S}_n$.

BEWEIS. Aus dem Beweis von 9.4.2 wissen wir, dass $[1, p]$ betrachtet als vollständiger Brick *direkt zerlegbar* ist, sofern es zwei *unvergleichbare* Elemente in $[1, p]$ gibt. Folglich sind je zwei Elemente a, b *vergleichbar,* weshalb $[1, p]$ nach HÖLDER-CLIFFORD vom Typ $\mathfrak{E}$ oder $\mathfrak{S}_n$ ist. Siehe etwa [30]. □

Offenbar ist das *Komplement* p' eines Atoms p von $\mathfrak{B}(I)$ ein *Hyperatom* von $\mathfrak{B}(I)$ und der letzte Satz besagt, dass das von p' erzeugte Ideal maximal ist. Umgekehrt sei nun angenommen, dass M ein *maximales Ideal* von $\mathfrak{B}$ ist. Dann ist $\mathfrak{B}/M$ *einfach* und daher isomorph zu einer Unterstruktur von $\mathfrak{E}$. Also stellt sich die natürliche Frage, ob sich jeder vollständige Brick subdirekt oder sogar direkt zerlegen lässt in Komponenten des angegebenen Typs. Im folgenden entwickeln wir einige Ergebnisse in dieser Richtung. Als erstes erhalten wir:

9. 4. 6 Proposition. *Jeder vollständige Brick besitzt eine subdirekte Zerlegung, deren Komponenten ausnahmslos isomorph zu* $\mathfrak{E}$ *oder zu* $\mathfrak{S}_n$ *sind.*

BEWEIS. Es genügt zu zeigen, dass der Durchschnitt D der Familie aller maximalen Ideale gleich $\{1\}$ ist. Angenommen also, es wäre $c \neq 1$ und $c \in D$. Wir bezeichnen mit u das Element $\bigvee c^n \ (n \in N)$ und wählen ein maximales Ideal I, das u' enthält. Es folgt $c \in I$, aber $u \notin I$.

Wir betrachten nun u. Es gilt $c * (c^k * u) \le u$, und wegen $u^2 = u$ und nach Definition und den Regeln der $*$-Arithmetik bildet das Intervall $[1, u]$ einen vollständigen Brick bezüglich $*, u$. Weiter erhalten wir für ein geeignetes ℓ die Formeln $c * (c^\ell * u) \neq 1$, und $(c^\ell * u) * c \neq 1$, die erste, da anderenfalls $u = c^m \in D$ erfüllt wäre – trotz $u \notin I \rightsquigarrow u \notin D$, und die zweite, da $\mathfrak{B}$ nach Annahme vollständig ganz-abgeschlossen ist.
Also gibt es nach 9.4.5 Idempotente v, w mit

$$vw = u \;\&\; v \wedge w = 1 \;\&\; v \ge c * (c^\ell * u) \neq 1 \;\&\; w \ge (c^\ell * u) * c \neq 1\,.$$

Hiermit erhielten wir $u'vw = 0$ mit $w \neq 0$ und $w \wedge u'v = 1$ für ein w, woraus sich die Existenz eines *maximalen Ideals* J mit $u'v \in J$, also auch mit $u' \in J$ ergäbe mit Widerspruch zu

$$\begin{aligned} c \in J \;\&\; c * (c^\ell * u) \in J &\Longrightarrow c(c * (c^\ell * u)) \in J \\ &\Longrightarrow c \vee (c^\ell * u) \in J \\ &\Longrightarrow c^\ell \in J \;\&\; c^\ell * u \in J \\ &\Longrightarrow c^\ell (c^\ell * u) = u \in J\,. \end{aligned}$$

Fertig! □

Wir erinnern: Eine boolesche Algebra heißt *atomar,* wenn jedes Element zumindest ein Atom übertrifft.

9. 4. 7 Proposition. *Sei $\mathfrak{B}$ ein vollständiger Brick mit atomarer boolescher Unteralgebra $\mathfrak{B}(I)$. Dann ist $\mathfrak{B}$ ein direktes Produkt vom Typ $\mathfrak{C}^\omega$.*

BEWEIS. Seien $p_i \;\, (i \in I)$ die Atome von $\mathfrak{B}(I)$. Dann gelten:

$$\forall\, a : \;\; a \;=\; a \wedge 0 = \bigvee (a \wedge p_i) \;\; (i \in I) \tag{9.29}$$

$$a \neq b \;\Longrightarrow\; \exists\, j \in I : a \wedge p_j \neq b \wedge p_j \tag{9.30}$$

$$x_i \le p_i \;\Longrightarrow\; \bigvee x_i = \bigvee ((\bigvee x_i) \wedge p_i) \;\; (i \in I)\,. \tag{9.31}$$

Also gibt es eine Bijektion ϕ zwischen B und dem Produkt $\prod P_i$, aller P_i definiert *via* $P_i := \{x \,|\, x \le p_i\} \;\; (i \in I)$, vermöge

$$\phi\,(a) \;:=\; \{(p_i \wedge a) \,\big|\, i \in I\}\,,$$

und es gilt ganz allgemein im Fall $p = p^2$ wie im Beweis zu 9.4.2 gezeigt:

$$\begin{aligned} \phi\,(a * b) &= u \wedge (a * b) \\ &= (u \wedge a) * (u \wedge b) \\ &= \phi\,(a) * \phi\,(b) \end{aligned}$$

Fertig! □

Als Sonderfall von 9.4.7 und als Verallgemeinerung eines Satzes von TARSKI [151] erhalten wir:

9. 4. 8 Proposition. *Ein Brick ist ein* Würfel, *wenn er vollständig, atomlos und vollständig distributiv ist.*

BEWEIS. Nach der schon in der Theorie der d-Halbgruppen eingesetzten Methode von ALFRED TARSKI bilden wir alle Durchschnitte $\bigwedge u_i \ \ (i \in I)$ mit idempotenten u_i, die aus jedem Paar $u_i, u_i{}'$ genau ein Element berücksichtigen. Dann ist 0 die Vereinigung all dieser Durchschnitte und diese Durchschnitte sind entweder gleich 1 oder ein Atom in $\mathfrak{B}(I)$. Nach 9.4.7 folgt die Behauptung, da B atomlos und die Notwendigkeit der Bedingung offenbar ist. □

Ersetzen wir *atomlos* durch *atomar,* so erhalten wir aus 9.4.5

9. 4. 9 Proposition. *Ein Brick ist ein Gitterwürfel, wenn er vollständig, atomar und vollständig distributiv und.*

Für den Rest dieses Abschnitts betrachten wir die speziellen Würfel $\mathfrak{C}^n$ aus topologischer Sicht.

9. 4. 10 Proposition. *Ein Brick* $\mathfrak{B}$ *ist ein Würfel vom Typ* $\mathfrak{C}^n$*, wenn* (B, y) bezüglich der *Intervall-Toplogie kompakt, jedes maximale Ideal* abgeschlossen *und jedes* minimale Ideal *zusammenhängend ist.*

BEWEIS. Offenbar sind die aufgestellten Bedingungen notwendig. Erfülle also $\mathfrak{B}$ die angegebenen Bedingungen.
Nach einem Satz von O.FRINK [76], siehe auch [10], ist $(B, \leq)$ kompakt bezüglich der Intervalltopologie genau dann, wenn $(B, \leq)$ einen *vollständigen Verband* bildet. Daher ist $\mathfrak{B}$ vollständig. Sei nun I ein maximales Ideal. Da I *abgeschlossen* ist, besitzt es ein *Maximum* oder kann durch endlich viele Mengen der Art $B \setminus [x, 0]$ mit $x \in I$ *überdeckt* werden. Also hat I ein Maximum, da es andernfalls ein Element $x_1 \vee x_2 \vee \ldots \vee x_n \in I$ gäbe, das nicht überdeckt würde.
Wir betrachten nun das Maximum u. Dieses u ist idempotent und hat ein (idempotentes) *Komplement,* das ein Atom in $\mathfrak{B}(I)$ ist. Umgekehrt ist jedes *Hyperatom* Maximum eines maximalen Ideals aus $\mathfrak{B}$.
Es kann aber $\mathfrak{B}(I)$ nur endlich viele Atome besitzen, da anderenfalls die Menge aller Elemente aus B, die höchstens endlich viele Atome übertreffen,

Teilmenge eines Maximalideals $[1, u]$ wäre. Deshalb müsste u' ein Teiler von u sein, mit Widerspruch zu $u' \not\leq u$.
Hiernach bilden wir $\bigvee p_i$. Es folgt $\bigvee p_i = 0$, da es sonst ein maximales $u \in B(I)$ gäbe, dessen Komplement ein Atom wäre, das $\bigvee p_i$ nicht teilt. Damit folgt die Behauptung aus der dritten Voraussetzung in Verbindung mit 9.4.5 □

Analog zur obigen Situation erhalten wir als „Gegentheorem“

9. 4. 11 Proposition. *Ein Brick $\mathfrak{B}$ ist ein endlicher Gitterwürfel, wenn $(B, \leq)$ bezüglich der Intervall-Toplogie kompakt ist, jedes maximale Ideal abgeschlossen ist und jedes minimale Ideal unzusammenhängend ist.*

9.5 Würfelalgebren

9. 5. 1 Definition. Ein Brick heiße *Würfelalgebra,* wenn er Unterbrick eines $\mathfrak{C}^\omega$ ist.
Natürlich ist damit jeder Würfel und auch jeder Gitterwürfel eine Würfelalgebra. Ferner ist, wie wir oben sahen, insbesondere jeder vollständige Brick eine Würfelalgebra, aber es ist natürlich nicht jede Würfelalgebra vollständig. Im folgenden gehen wir allgemeiner der Frage nach, durch welche Eigenschaften sich Würfelalgebren auszeichnen. Zunächst haben wir hier als einen grundlegenden Satz ein Ergebnis, das sich implizit in der Theorie der d-Halbgruppen einstellte:

9. 5. 2 Proposition. *Ein Brick ist ein Würfel gdw. er ganz-abgeschlossen ist.*

Wenden wir dieses Resultat auf spezielle Strukturen an, so erhalten wir den Satz von Dedekind, dass die *angeordnete Gruppe* der rationalen Zahlen durch *Schnitte* vervollständigt werden kann zu der *vollständig angeordneten Gruppe* der reellen Zahlen, und den Satz von Glivenko-Stone, dass die Schnittvervollständigung einer booleschen Algebra wieder eine boolesche Algebra liefert (s. [1]).
Betrachten wir als nächstes Würfelalgebren aus topologischer Sicht. Nach Methoden, eingeführt von M. H. Stone ist es heutzutage eine Sache der Routine, einen gegebenen Brick in eine Algebra *stetiger Funktionen* von einem *kompakten Hausdorffraum* in das *Einheitsintervall* einzubetten, sobald dieser Brick *subdirekt zerlegt* ist in *Faktoren,* die sich einbetten lassen

in $\mathfrak{E}$. Doch aus Gründen der Vollständigkeit seien die wesentlichen Ideen hier noch einmal aufgeführt.
Zunächst versehen wir $\mathbf{E}^B$ mit der *Produkttopologie* und erhalten auf diese Weise einen kompakten Hausdorffraum $\mathbf{H}$.
Hiernach betrachten wir die Menge aller Homomorphismen von $\mathfrak{B}$ nach $\mathfrak{E}$. Diese Menge ist eine *abgeschlossene* Teilmenge von $\mathbf{E}^B$ und somit ein kompakter Hausdorffraum bezüglich der *Relativtopologie,* was aus den Eigenschaften der Produkttopologie folgt. Wir bezeichnen diesen Raum mit $\mathbf{D}$.
Offensichtlich bildet die Menge aller stetigen Funktionen $\phi : \mathbf{D} \longmapsto \mathbf{E}$, versehen mit seiner *natürlichen Topologie,* einen ganz-abgeschlossenen Brick bezüglich der *punktweise* definierten Operationen. Wir erklären nun

$$\hat{a} : \mathbf{D} \longmapsto \mathbf{E} \quad \text{vermöge} \quad \hat{a}(\phi) := \phi\,(a).$$

Dann ist $a \longrightarrow \hat{a}$ ein *Monomorphismus* von $\mathfrak{B}$ in den Brick aller stetigen Funktionen von $\mathbf{D}$ nach $\mathbf{E}$, denn $a \neq b$ impliziert $\hat{a} \neq \hat{b}$, wegen 9.4.5, sowie die Gleichung

$$(\widehat{a * b})(\phi) = \phi\,(a * b) = \phi\,(a) * \phi\,(b) = \hat{a}(\phi) * \hat{b}(\phi)\,.$$

Also erhalten wir auf der Basis von TYCHONOFFs fundamentaler Pionierarbeit über Produkträume in Anlehnung an Darstellungsideen von M. H. STONE den Satz:

9. 5. 3 Proposition. *Ein Brick ist eine Würfelalgebra gdw. er ein Unterbrick des Bricks aller stetigen Funktionen von einem geeignet gewählten Hausdorff-Raum in den Raum des Einheitsintervalls – betrachtet als Brick – ist.*

Dieser Satz ist offenbar eng verwandt mit FANs Theorem über die Darstellbarkeit *Archimedischer Vektorverbände* [73]. Siehe auch FLEISCHER [75].
Wie wir gesehen haben, hat jeder Brick eine Garbendarstellung, deren Halme subdirekt irreduzible und damit linear geordnete Bricks sind. Für den speziellen Fall des Würfels bedeutet dies

9. 5. 4 Proposition. *Ein Brick $\mathfrak{B}$ ist eine Würfelalgebra genau dann, wenn er eine Garbendarstellung über der Menge aller maximalen Ideale von $\mathfrak{B}$ besitzt, deren Halme sich einbetten lassen in $\mathfrak{E}$.*

Hiernach befassen wir uns mit *Maßfunktionen* auf Bricks, vgl. 5.4.4. Als Notation vereinbaren wir, dass $\mathfrak{B}$ im folgenden stets ein beliebiger Brick, $\mathfrak{P}$

seine Produkterweiterung und $\mathfrak{G}$ die verbandsgeordnete Quotientengruppe von $\mathfrak{P}$ sei.
Offenbar haben wir in einem Brick im Falle $\mu : a \longrightarrow |\, a\,|$ die Gleichungen

$$\begin{aligned} |\, a \wedge b\,| + |\, a * b\,| &= |\, b\,| \\ |\, a\,| + |\, a * b)\,| &= |\, a \vee b\,| \end{aligned}$$

und daher für den Verband $(B, \wedge, \vee)$ die Gleichung

$$|\, a \wedge b\,| + |\, a \vee b\,| = |\, a\,| + |\, b\,| .$$

Spezielle Maße auf $\mathfrak{B}$ sind die Homomorphismen von $\mathfrak{B}$ nach $\mathfrak{E}$. Dies führt uns zu einer ersten Charakterisierung der Würfelalgebren mittels Maßfunktionen.

9. 5. 5 Proposition. *Ein Brick $\mathfrak{B}$ ist eine Würfelalgebra genau dann, wenn zu jedem $1 \neq a \in B$ ein Maß μ existiert mit $\mu(a) = 1$.*

BEWEIS. Gibt es zu jedem $a \neq 1$ ein Maß μ mit $\mu(a) = 1$, so muss $\mathfrak{B}$ ganz-abgeschlossen sein, da andernfalls 0 keinen reellen Wert annehmen könnte.
Existiere nun für jedes $a \neq 1$ aus B ein Homomorphismus h von $\mathfrak{B}$ nach $\mathfrak{E}$, so dass $h(a) \neq 0 \in \mathbf{R}$. Dann erhalten wir ein Maß μ mit $\mu(a) = 1$ *via* Multiplikation aller $h(b)$ $(b \in B)$ mit dem Faktor $1/h(a)$. □

9. 5. 6 Definition. Sei A eine Teilmenge der Trägermenge P von $\mathfrak{P}$ und sei f eine Funktion von A nach $\mathbf{R}^{\geq 0}$. Dann heiße f eine *partielle Bewertung* von $\mathfrak{B}$, wenn die kanonische Erweiterung von f auf die von A erzeugte Unterhalbgruppe $\mathfrak{A}$ von $\mathfrak{P}$ der Gleichung $f(ab) = f(a) + f(b)$ genügt.

Offenbar haben wir $f(1) = f(1) + f(1) \rightsquigarrow f(1) = 0$ und wir wissen nach 5.4.1, dass jede Maßfunktion auf einem Brick eine eindeutige Erweiterung auf die korrespondierende abelsche Verbandsgruppe besitzt.
Weiterhin ist die Menge der partiellen Bewertungen einer Verbandsgruppe nicht leer und erfüllt die Voraussetzungen des ZORN schen Lemmas. Folglich lässt sich jede partielle Bewertung einbetten in eine *maximale partielle* Bewertung.

9. 5. 7 Proposition. *Sei f eine maximale partielle Bewertung auf dem abelschen Verbandsgruppenkegel $\mathfrak{P}$. Dann ist der Definitionsbereich $D(f)$ von f multiplikativ abgeschlossen und* konvex *bezüglich $\leq$.*

BEWEIS. $D(f)$ ist *per definitionem* multiplikativ abgeschlossen.
Weiter gilt $1 \in D(f)$, denn sonst lieferte $f(1) := 0$ eine Erweiterung.
Sei hiernach $1 \leq a \leq b \in D$ & $a \notin D$. Dann besteht die von D und a erzeugte Unterhalbgruppe aus allen Produkten der Form $a^n \cdot d$ mit einem $d \in D$. Zu zeigen ist offenbar, dass sich unter dieser Annahme ein $|\,a\,|$ finden lässt, das für alle $c, d, u, v \in D$ den Implikationen genügt:

$$c \leq a^p d \implies \frac{f(c) - f(d)}{p} \leq |\,a\,|$$

und
$$a^q u \leq v \implies |\,a\,| \leq \frac{f(v) - f(u)}{q}\ .$$

Denn dann lässt sich f ausdehnen, wie wir sehen werden.
Hierzu beachten wir zunächst, dass aus $c, d, u, v \in D(f)$ die Implikation resultiert:

$$\begin{aligned} c \leq a^p d \ \&\ a^q u \leq v &\implies (cd^{-1})^q \leq a^{pq} \leq (vu^{-1})^p \\ &\implies c^q d^{-q} \leq v^p u^{-p} \\ &\implies c^q u^p \leq v^p d^q \\ &\implies q \cdot f(c) - q \cdot f(d) \leq p \cdot f(v) - p \cdot f(u) \\ &\implies \frac{f(c) - f(d)}{p} \leq \frac{f(v) - f(u)}{q}\ . \end{aligned}$$

Sie sichert, dass die Menge $S(a)$ der nicht negativen reellen Zahlen s mit

$$\begin{array}{ccc} c, d \in D(f) & \& & c \leq a^p d \\ & \implies & \\ \dfrac{f(c) - f(d)}{p} & \leq & s \end{array}$$

und

$$\begin{array}{ccc} u, v \in D(f) & \& & a^q u \leq v \\ & \implies & \\ s & \leq & \dfrac{f(v) - f(u)}{q} \end{array}$$

nicht leer ist.

Also können wir ein Element aus $S(a)$ als $|\,a\,|$ wählen und eine Funktion $|\quad|$ definieren vermöge

$$|\,x\,| \quad := \quad \begin{cases} f(x) & \text{falls} \quad x \in D \\ |\,a\,| & \text{falls} \quad x = a\,. \end{cases}$$

Dies liefert eine Erweiterung von f, wie die noch zu beweisende Implikation

$$\begin{array}{rcl} a^m c & \leq & a^n d \\ & \Longrightarrow & \\ m \cdot |\,a\,| + f(c) & \leq & n \cdot |\,a\,| + f(d) \end{array} \tag{9.32}$$

zeigen wird. Denn (9.32) sichert zum einen, dass die Festsetzung $|\,a^q c\,| := q\,|\,a\,| + f(c)$ eindeutig und damit auch *multiplikativ* ist, und zum anderen, dass sie *isoton* ist. Wir führen den Beweis durch Fallunterscheidung:
Sei $m = n$. In diesem Fall ist die angegebene Implikation evident.
Sei hiernach $m < n$. In diesem Falle erhalten wir mit $p := n - m$ die Implikation

$$\begin{aligned} a^m c \leq a^n d \implies & \frac{f(c) - f(d)}{p} \leq |\,a\,| \\ \implies & f(c) \leq p \cdot |\,a\,| + f(d) \\ \implies & m \cdot |\,a\,| + f(c) \leq n \cdot |\,a\,| + f(d)\,. \end{aligned}$$

Sei endlich $m > n$. Dann können wir ähnlich schließen wie im Falle $m < n$.
Also könnte f erweitert werden, wenn es ein a mit $1 \leq a \leq b \in D$ & $a \notin D$ gäbe – mit Widerspruch zur angenommenen Maximalität!
Damit ist die Behauptung bewiesen. □

Als unmittelbare Folge von 9.5.7 erhalten wir

9. 5. 8 Proposition. *Ein Brick $\mathfrak{B}$ ist eine Würfelalgebra genau dann, wenn sich jedes $D = \{a(\neq 1), 0\}$ derart positiv bewerten lässt, dass die kanonische Fortsetzung auf das von $\{a, b\}$ in $\mathfrak{P}$ erzeugte Untermonoid eine partielle Bewertung liefert.*

DENN: Die Bedingung ist notwendig, soll $\mathfrak{B}$ eine Würfelalgebra sein.
Sie ist aber nach 9.5.7 auch hinreichend, da die korrespondierende partielle Bewertung von $\mathfrak{G}$ zu einer maximalen Bewertung ausgedehnt werden kann,

deren Definitionsbereich zum einen die Elemente 0 und 1 enthält und sich zum anderen als *konvex* erweist. □

Als eine mittelbare Folge erhalten wir weiter eine Brickversion eines Satzes von HORN und TARSKI über die Ausdehnbarkeit *partieller Maße* auf booleschen Algebren.

9. 5. 9 Proposition. *Sei $\mathfrak{B}$ ein Brick und $\mathfrak{U}$ ein Unterbrick von $\mathfrak{B}$. Dann kann jede Maßfunktion auf $\mathfrak{U}$ zu einer Maßfunktion auf $\mathfrak{B}$ erweitert werden.*

BEWEIS. Da 0 ein Element aus U ist, kann eine Maßfunktion auf $\mathfrak{U}$ zu einer Maßfunktion auf $\mathfrak{B}$ erweitert werden gdw. $\mathfrak{P}$ die Implikation erfüllt:

$$\text{(PS)} \qquad \prod_1^n a_\nu \leq \prod_1^n b_\nu \implies \sum_1^n |\, a_\nu \,| \leq \sum_1^n |\, b_\nu \,| \,.$$

Dies resultiert aber aus 5.4.5 □

Wir merken noch an, dass (PS) „schon" in $\mathfrak{B}$ formuliert werden kann, mittels:

$$\begin{aligned} a = b &\iff (a * b)(b * a) = 1 \\ ab * c &= b * (a * c) \\ \text{und } a * bc &= (a * b)((b * a) * c)\,. \end{aligned}$$

HORN & TARSKI haben in [96] für boolesche Algebren die Beschreibung

$$\text{(TH)} \qquad \sigma_i(a) \leq \sigma_i(b) \implies \sum f(a_i) \leq \sum f(b_i) \ \ (1 \leq i \leq n)$$

gegeben. Hier steht $\sigma_k(a_1, \ldots, a_n)$ für den Durchschnitt aller k-stelligen (Verbands-) Schnitte von Elementen aus $\{a_1, \ldots, a_n\}$. Wir streben eine direkte Herleitung von (HT) aus (PS) im allgemeinen Fall und von (PS) aus (HT) im booleschen Falle an. Zu diesem Zweck starten wir mit:

9. 5. 10 Lemma. *Sei $\mathfrak{B}$ ein Brick und n eine natürliche Zahl. Dann gilt*

$$\prod_1^n a_\nu = \prod_1^n \sigma_k(a_1, \ldots, a_n)\,, \tag{9.35}$$

wobei σ_k die obere Grenze aller Durchschnitte von genau k Faktoren aus $a_1 \cdot a_2 \cdot \ \ldots \ \cdot a_n$ symbolisiere.

BEWEIS. Man beachte, dass man zwischen a_i und a_j für $i \neq j$ auch dann zu unterscheiden hat, wenn $a_i = a_j$.
Offenbar gilt (9.35) für $n = 1$ und weiterhin für $n = 2$ wegen der Gleichung $ab = (a \vee b)(a \wedge b)$. Sei hiernach $n = 3$. Dann ist der folgende Induktions-

schritt symptomatisch:

$$\begin{aligned} & a_1a_2a_3 \\ = \; & (a_1 \vee a_2)(a_1 \wedge a_2)a_3 \\ = \; & (a_1 \vee a_2 \vee a_3)((a_1 \vee a_2) \wedge a_3)(a_1 \wedge a_2) \\ = \; & (a_1 \vee a_2 \vee a_3)((a_1 \wedge a_3) \vee (a_2 \wedge a_3))(a_1 \wedge a_2) \\ = \; & (a_1 \vee a_2 \vee a_3)((a_1 \wedge a_2) \vee (a_2 \wedge a_3) \vee (a_3 \wedge a_1))(a_1 \wedge a_2 \wedge a_3) \\ = \; & \sigma_1(a_1, a_2, a_3) \cdot \sigma_2(a_1, a_2, a_3) \cdot \sigma_3(a_1, a_2, a_3) \,. \end{aligned}$$ □

9.5.10 gilt – natürlich – sowohl für boolesche Algebren als auch für abelsche Verbandsgruppenkegel, da diese symmetrische Brickerweiterungen besitzen.
Als Folgerung erhalten wir, dass $\prod_1^n a_\nu$ immer dann kleiner oder gleich $\prod_1^n b_\nu$ ist, wenn nach Auffüllen mit Faktoren 1 auf gleiche Länge ℓ alle σ_k $(1 \leq k \leq \ell)$ bezüglich $(a_1, \ldots, a_\ell)$ kleiner oder gleich den entsprechenden σ_k bezüglich $(b_1, \ldots, b_\ell)$ sind.
Sei $\mathfrak{B}$ hiernach eine boolesche Algebra. Dann folgt auch die Umkehrung:

9. 5. 11 Proposition. *Sei $\mathfrak{B}$ ein boolescher Brick. Gilt dann für die Elemente $a_1, \ldots, a_m, b_1, \ldots, b_m$ aus B in $\mathfrak{P}$ die Abschätzung $a_1 \cdot a_2 \cdot \;\cdots\; \cdot a_m \leq b_1 \cdot b_2 \cdot \;\cdots\; \cdot b_m$, so resultiert für alle $k \leq m$:*

$$\sigma_k(a_1, \ldots, a_m) \;\leq\; \sigma_k(b_1, \ldots, b_m) \tag{9.36}$$

BEWEIS. Zunächst erhalten wir aus $a_1 \leq b_1 \cdot \ldots \cdot b_m$

$$a_1 \;\leq\; b_1 \vee \ldots \vee b_m \,, \tag{9.37}$$

denn wir haben $a_1 \leq b_1 \cdot b_2 \cdot \;\ldots\; \cdot b_m$ in $\mathfrak{P}$ und

$$a_1 \leq c_1c_2 \implies (c_1 \wedge a_1) \leq c_1 \;\&\; (c_1 * a_1) \leq c_2$$

und folglich wegen $c_1 \wedge c_1 * a_1 = 1$

$$\begin{aligned} a_1 \leq c_1c_2 \Longrightarrow a_1 \;&=\; (c_1 \wedge a_1)(c_1 * a_1) \\ &=\; (c_1 \wedge a_1) \vee (c_1 * a_1) \\ &\leq\; c_1 \vee c_2 \,. \end{aligned}$$

Hieraus erhalten wir (9.37) durch Induktion, wenn wir n-stellige Produkte schreiben als $(b_1 \cdot b_2 \cdot \;\ldots\; \cdot b_{n-1}) \cdot b_n$.
DENN: Die Behauptung für $k = 1$.

Angenommen nun, die Aussage gilt – schon – für alle i mit $1 \leq i \leq k$ bezüglich aller $\ell \geq k$.
Wir betrachten zunächst den Sonderfall

$$c_1 \cdot \ \ldots \ \cdot c_k \cdot c_{k+1} \ \leq \ d_1 \cdot \ \cdots \ \cdot d_k d_{k+1}$$

und bezeichnen mit $\sigma_i(c)$ das Element $\sigma_i(c_1, \ldots, c_{k+1})$ und mit $\sigma_i(d)$ das Element $\sigma_i(d_1, \ldots, d_{k+1})$. Es folgt $\sigma_{k+1}(c) \leq \sigma_{k+1}(d)$, d. h.

$$c_1 \wedge \ldots \wedge c_{k+1} \ \leq \ d_1 \wedge \ldots \wedge d_{k+1} \, .$$

Denn nach Voraussetzung gilt, dass $\sigma_i(c) \leq \sigma_i(d)$ für alle i mit $1 \leq i \leq k$ und damit

$$\begin{array}{rcl}
 & & \left(\prod_1^k \sigma_i(c)\right) \sigma_{k+1}(c) \\
 & \leq & \left(\prod_1^k \sigma_i(d)\right) \sigma_{k+1}(d) \\
 & = & \left(\prod_1^k \sigma_i(c)\right) \left(\prod_1^k (\sigma_i(c) * \sigma_i(d))\right) \sigma_{k+1}(d) \\
 & \Longrightarrow & \\
\sigma_{k+1}(c) & \leq & \left(\prod_1^k (\sigma_i(c) * \sigma_i(d))\right) \sigma_{k+1}(d)
\end{array}$$

erfüllt ist und zudem – erneut aus booleschen Gründen – dass

$$\sigma_{k+1}(c) \leq \sigma_i(c) \ \ (1 \leq i \leq k) \ \Longrightarrow \ \sigma_{k+1}(c) \wedge (\sigma_i(c) * \sigma_i(d)) = 1$$

gesichert ist, was die Induktion abschließt.
Endlich erhalten wir $\sigma_{k+1}(a) \leq \sigma_{k+1}(b)$ aus (9.37) und $x \wedge yz \leq (x \wedge y)(x \wedge z)$ und kommen so ans Ziel vermöge der Implikation

$$\begin{array}{rcl}
a_{i,1} \wedge \ldots \wedge a_{i,k+1} & \leq & b_1 \wedge b_2 \wedge \ldots \wedge (b_{k+1} b_{k+2} \ldots b_m) \\
 & \leq & \prod_{\nu=1}^{m-k} ((b_1 \wedge \ldots \wedge b_k) \wedge b_{k+\nu}) \\
 & \Longrightarrow & \\
a_{i,1} \wedge \ldots \wedge a_{i,k+1} & \leq & \bigvee_{\nu=1}^{m-k} ((b_1 \wedge \ldots \wedge b_k) \wedge b_{k+\nu}) \\
 & \leq & \sigma_{k+1}(b) \, .
\end{array}$$

□

Hiernach können wir reformulieren:

9. 5. 12 Das Theorem von Horn und Tarski. *Sei* $\mathfrak{B}$ *eine boolesche Algebra und sei* A *eine Teilmenge von* B *mit* $0 \in A$. *Dann lässt sich eine reellwertige Funktion* f *auf* A *genau dann zu einer Maßfunktion auf* $\mathfrak{B}$

ausdehnen, wenn für alle Paare von n-Tupeln $(a_1, \ldots, a_n)\,, (b_1, \ldots, b_n)$ *die Implikation erfüllt ist:*

$$\text{(TH)} \qquad \sigma_i(a) \leq \sigma_i(b) \ \ (1 \leq i \leq n) \implies \sum f(a_i) \leq \sum f(b_i)$$

BEWEIS. Gilt die Bedingung (TH), so folgt nach 9.5.11

$$\begin{aligned} \prod a_i \leq \prod b_i &\implies \sigma_i(a) \leq \sigma(b) \\ &\implies \sum f(a_i) \leq \sum f(b_i)\,, \end{aligned}$$

also Bedingung (PS), und gilt (PS), so hat f eine solche Ausdehnung, und es folgt nach (9.35)

$$\begin{aligned} \sigma_i(a) \leq \sigma_i(b) &\implies \prod \sigma_i(a) \leq \prod \sigma_i(b) \\ &\implies \prod a_i \leq \prod (b_i) \\ &\implies \sum f(a_i) \leq \sum f(b_i)\,, \ \ (i \in I) \end{aligned}$$

also die Abschätzung (TH). □

Kapitel 10

Allgemeine Bricks

10.1 GMV-Algebren

Zur Erinnerung: Im vorauf gegangenen Kapitel wurde der kommutative Brick charakterisiert als Halbgruppe mit Komplementen, die den Bedingungen genügt:

$$\begin{array}{lrcl}
\text{(CS1)} & a \circ (b \circ c) & = & b \circ (a \circ c) \\
\text{(CS2)} & a \circ 0 & = & 0 \\
\text{(CS3)} & a \circ 0' & = & a \\
\text{(CS4)} & a \circ (a \circ b')' & = & b \circ (b \circ a')'.
\end{array}$$

Dies regt als Übertragung auf den nicht kommutativen Fall an zu der

10. 1. 1 Definition. Eine Algebra $\mathfrak{A} = (A, \oplus, ^-, ^\circ, 1, 0)$ vom Typ $(2, 1, 1, 0, 0)$ heißt eine *GMV-Algebra* [1]) wenn sie bezüglich $y \odot x := (x^- \oplus y^-)^\circ$ – den Bedingungen genügt:

$$\begin{array}{lrcl}
\text{(MV1)} & x \oplus (y \oplus z) & = & (x \oplus y) \oplus z \\
\text{(MV2)} & x \oplus 1 & = & x \; = \; 1 \oplus x \\
\text{(MV3)} & x \oplus 0 & = & 0 \; = \; 0 \oplus x \\
\text{(MV4)} & 0^\circ & = & 1 \; = \; 0^-
\end{array}$$

[1]) Generalized Multi Valued Algebra

(MV5) $$(x^- \oplus y^-)^\circ = (x^\circ \oplus y^\circ)^-$$

(MV6) $$\begin{aligned} x \oplus x^\circ \odot y &= y \oplus y^\circ \odot x \\ &= x \odot y^- \oplus y \\ &= y \odot x^- \oplus x \end{aligned}$$

(MV7) $$x \odot (x^- \oplus y) = (x \oplus y^\circ) \odot y$$

(MV8) $$(x^-)^\circ = x = (x^\circ)^- .$$

10. 1. 2 Proposition. *Jeder Brick $\mathfrak{B}$ bildet eine GMV-Algebra $\mathfrak{G}(B)$ bezüglich*

$$x^- := 0 : x, \quad x^\circ := x * 0, \quad x \oplus y := ax .$$

BEWEIS. Die Gleichungen (MV1) bis (MV4) und auch (MV8) sind evident.

(MV5) $$\begin{aligned} (0:x)(0:y) * 0 &= (0:y) * ((0:x) * 0) \\ &= ((0:y) * 0) : (x * 0)) \\ &= (0 : (y * 0)) : (x * 0)) \\ &= 0 : (x * 0)(y * 0) . \end{aligned}$$

(MV6) $$\begin{aligned} x \oplus x^\circ \odot y &= x \oplus (x * 0) \odot y \\ &= x \oplus ((0:y) \oplus x) * 0) \\ &= x \cdot ((0:y) \cdot x) * 0) \\ &= x \cdot (x * ((0:y) * 0) \\ &= x \cdot (x * y) \\ &= y \cdot (y * x) \\ &= y \oplus y^\circ \odot x \\ &= (x : y) \cdot y \\ &= ((0:x) * (0:y)) \cdot y \\ &= ((0 : (0:y)) \cdot ((0:x) * 0) \cdot y \\ &= x \odot y^- \oplus y \\ &= y \odot x^- \oplus x . \end{aligned}$$

(MV7) $$\begin{aligned} x \odot (x^- \oplus y) &= (((0:y) : (0:x)) \cdot (0:x))\ ^\circ \\ &= ((0:y) \cdot ((0:y) * (0:x)))\ ^\circ \\ &= (x \oplus y^\circ) \odot y . \end{aligned}$$

Damit sind wir am Ziel □

Umgekehrt gilt

10. 1. 3 Proposition. *Jede GMV-Algebra $\mathfrak{G}$ bildet einen Brick $\mathfrak{B}(G)$ bezüglich der Operationen: $a * b := a^\circ \odot b$ and $b : a := b \odot c^-$.*

BEWEIS. (BR1) ,(BR2), und (BR0) folgen unmittelbar, und es folgen

(BR3)
$$\begin{aligned} a * (b : c) &= a^\circ \odot (b \odot c^-) \\ &= (a^\circ \odot b) \odot c^- \\ &= (a * b) : c \end{aligned}$$

sowie

(10.14)
$$\begin{aligned} a \odot (b \odot c) &= a \odot (c^- \oplus b^-)^\circ \\ &= ((c^- \oplus b^-)^{\circ -} \oplus a^-)^\circ \\ &= ((c^- \oplus b^-) \oplus a^-)^\circ \\ &= (c^- \oplus (b^- \oplus a^-))^\circ \\ &= (b^- \oplus a^-)^\circ \odot c \\ &= (a \odot b) \odot c \end{aligned}$$

und damit

(BR4)
$$\begin{aligned} a : (b * a) &= a \odot (b * a)^- \\ &= a \odot (b^\circ \odot a)^- \\ &= a \odot (a^- \oplus b) \\ &= (a \oplus b^\circ) \odot b \\ &= (b \odot a^-)^\circ \odot b \\ &= (b : a) * b\,. \end{aligned}$$
□

Schließlich sei die Galoisverbindung herausgestellt.:

(GAL) $$\mathfrak{B}(\mathfrak{G}(B)) = \mathfrak{B} \text{ und } \mathfrak{G}(\mathfrak{B}(G)) = \mathfrak{G}\,.$$

10.2 Die Relative Kürzungseigenschaft

10. 2. 1 Definition. Unter einer schwachen Kegelalgebra verstehen wir eine Algebra $\mathfrak{C} := (C, *, :)$ des Typs $(2, 2)$, die den Gesetzen genügt:

(R2*) $$(a * a) * b = b$$

$$\text{(R2}^{:}\text{)} \qquad b = b : (a : a)$$

$$\text{(R3)} \qquad a * (b : c) = (a * b) : c$$

$$\text{(R4)} \qquad a : (b * a) = (b : a) * b\,.$$

Aus (R2*),(R2$^{:}$) und (R4) folgt zunächst $a * a = b * b$ and $a : a = b : b$ und damit weiter

$$\text{(10.21)} \qquad b * a = e \iff a : b = e,$$

wegen

$a * b = e \Longrightarrow b : a = (b : (a * b)) : a = ((a : b) * a) : a = (a : b) * (a : a) = e\,.$

Es liefert aber $b * a = e \;\&\; a : b = e$ *via* $a \geq b :\Longleftrightarrow a * b = e$ eine *inf-abgschlossene* Partialordnung mit Minimum e. Denn, man beachte

$$a * e = a * (e : (a * e)) = (a * e) : (a * e) = e.$$

Somit können schwache Kegelalgebren betrachtet werden als eine Typ-$(2, 0)$ Verallgemeinerung der kommutativen BCK-Algebra, die definiert ist vermöge

$$\text{(BCK1)} \qquad e * x = x$$

$$\text{(BCK2)} \qquad x * e = 0$$

$$\text{(BCK3)} \qquad a * (b * c) = b * (a * c)$$

$$\text{(BCK4)} \qquad (a * b) * b = (b * a) * a\,.$$

Man kann heutzutage geradezu von einer BCK-Industrie sprechen. Deshalb beziehen wir und auf [67] anstatt auf Originalpapiere [2)]. Dort wird u.a. eine relative Kürzungsbedingung (RCP) formuliert, und es wird eine Theorie der kommutativen BCK-Algebren entwickelt, die dieser Bedingung genügen. In dem korrespondieren Kontext werden dann mehrere äquivalente Bedinungen vorgestellt, jedoch: die zentral-fundamentale Bedingung dieser Lecture Note, die auch in Traczyk's Beitrag [153] eine wesentliche Rolle spielt, nämlich

$$\text{(W)} \qquad (a * b) * (a * c) = (b * a) * (b * c)\,,$$

[2)] allerdings nicht ohne zu erwähnen, dass die Theorie der BCK-Algebren initiiert wurde von Kiyoshi Iséki.

bleibt unerwähnt. Hinzu kommen die Studien von W. RUMP rund um die Yang-Baxter-Identität – um nur drei seiner Artikel zu nennen, vgl. [139], [140], und [141]. Dies als Vorbemerkung zu den nachfolgenden Ausführungen:

10. 2. 2 Proposition. *Sei $\mathfrak{B}$ eine schwache Kegelalgebra. Dann sind paarweise äquivalent:*

(RCP) $$a \leq b, c \;\&\; a * b = a * c \Longrightarrow b = c$$

(NOR) $$(a * b) \wedge (b * a) = 1$$

(RCO) $$(a * b) * (b * a) = b * a$$

(D I S) $$a * (b \wedge c) = a * b \wedge a * c$$

(RES) $$(a * b) * (a * c) = (b * a) * (b * c)\,.$$

BEWEIS. : (RCP) $\Longrightarrow$ (NOR). Wegen (RCP) ist im Falle $a \leq d \;\&\; a*d = b$ das Element b eindeutig bestimmt. Daher können wir im Falle $a * d = b$ als alternative Notation einführen: $a \circ b = d$ – ohne eine Produkt Definition oder Ähnliches im Hinterkopf. In diesem Sinne erhalten wir in jedem Falle

$$\begin{array}{rcl} a \leq c, d & \& & a \circ b = d \\ & \Rightarrow & \\ a & = & (d : a) * d = b * d \\ & \Rightarrow & \\ a & \leq & d : (c * b) \\ & \Rightarrow & \\ a * (d : (c * b)) & = & (a * d) : (c * b) \\ & = & b : (c * b) \\ & = & b \wedge c\,, \end{array}$$

was bedeutet, dass mit der Existenz von $a \circ b$ auch die Existenz von $a \circ (b \wedge c)$ gesichert ist, was mittels (RCP), siehe unten, zu der Kette führt:

(10.32) $$\begin{array}{rcl} a * (a \circ b \wedge a \circ c) & \leq & a * a \circ b \wedge a * a \circ c \\ & = & b \wedge c \\ & = & a * a \circ (b \wedge c) \\ & \leq & a * (a \circ b \wedge a \circ c) \end{array}$$

$$
\begin{array}{rcl}
a * a \circ (b \wedge c) & \overset{\Rightarrow}{=} & a * (a \circ b \wedge a \circ c) \\
& \overset{(\mathrm{RCP})}{\Longrightarrow} & \\
a \circ (b \wedge c) & = & a \circ b \wedge a \circ c\,.
\end{array}
$$

Insbesondere hat sich damit ergeben

(10.33) $$a \leq b, c \Longrightarrow a * (b \wedge c) = a * b \wedge a * c\,,$$

also die Bedingung

(NOR) $$a * b \wedge b * a = (a \wedge b) * (a \wedge b) = 1\,.$$

(NOR) $\Longleftrightarrow$ (RCO), man beachte $(a*b)*(b*a) = ((a*b) \wedge (b*a)) * (b*a)$ and $x \wedge y = x : (y * x)$.

(NOR) $\Longrightarrow$ (DIS), da $b \wedge c = c : (b * c)$ zu der Herleitung führt:

$$
\begin{array}{rl}
& (a * (b \wedge c)) * (a * b \wedge a * c) \\
\leq & ((a * (b \wedge c)) * (a * b)) \wedge ((a * (b \wedge c)) * (a * c)) \\
= & ((a * (b : (c * b))) * (a * b)) \wedge ((a * (c : (b * c))) * (a * c)) \\
= & (((a * b) : (c * b)) * (a * b)) \wedge (((a * c) : (b * c)) * (a * c)) \\
\leq & (c * b) \wedge (b * c) = 1
\end{array}
$$

und damit zu

(10.35) $$a * (b \wedge c) \geq a * b \wedge a * c \ \ (\geq a * (b \wedge c))\,,$$

also zu der Bedingung (DIS).

(DIS) $\Longrightarrow$ (RES). Sei zunächst $\mathfrak{C}$ durch 1 beschränkt. Dann folgt:

$$
\begin{array}{rcl}
(a * b) * (a * c) & = & ((a * 1) : (b * 1)) * ((a * 1) : (c * 1)) \\
& = & (((a * 1) : (b * 1)) * (a * 1)) : (c * 1) \\
& =: & f(a, b, c) \\
& = & f(b, a, c) \\
& = & (b * a) * (b * c)\,.
\end{array}
$$

Beachte hiernach, dass jedes Intervall $[e, c]$ von jedem allgemeinen $\mathfrak{C}$ eine beschränkte schwache Kegelalgebra mit Maximum c bildet. Dann ergibt sich der allgemeine Fall vermöge:

$$\begin{aligned}
(a*b)*(a*c) &= ((a*b)\wedge(a*c))*(a*c) \\
&\overset{(DIS)}{=} (a*(b\wedge c))*(a*c) \\
&= ((a\wedge c)*(b\wedge c))*((a\wedge c)*c) \\
&=: g(a,b,c) = g(b,a,c) \\
&= (b*a)*(b*c)\,.
\end{aligned} \tag{10.36}$$

(RES) $\Longrightarrow$ (RCP). Sei $a \le b, c$ und sei $a*b = a*c$. Dann folgt

$$b*c = (b*a)*(b*c) = (a*b)*(a*c) = (a*b)*(a*b) = 1\,,$$

also $b \ge c$, und – dual – $c \ge b$. $\square$

10.3 Vom Brick zum Kegel – auf neuen Wegen

10. 3. 1 Proposition. *Jeder Brick $\mathfrak{B}$ bildet eine normale komplementäre Halbgruppe $\mathfrak{H} := \mathfrak{H}(B)$ unter*

$$ab := 0 : ((b*(a*0))\,, \tag{10.37}$$

weshalb darüber hinaus jeder Brick einen Verband bildet unter

$$a\cdot(a*b) = a\vee b = (b:a)\cdot a \tag{10.38}$$

$$a:(b*a) = a\wedge b = (b:a)*b\,. \tag{10.39}$$

Darüber hinaus erfüllt $\mathfrak{H}(B)$ die Gleichungen (3.97) *bis* (3.107) .

BEWEIS. Zunächst erhalten wir (A3), also

$$ab*c = 1 = b*(a*c)$$

via

$$\begin{aligned}
ab*c &= (0:(b*(a*0)))*(0:(c*0)) \\
&= (b*(a*0)):(c*0) \\
&= b*((a*0):(c*0)) \\
&= b*(a*c)
\end{aligned} \tag{10.40}$$

und damit

(10.41) $$(a:b)b*a = b*((a:b)*a) = 1\,.$$

Folglich gilt

$$ab*(((0:b):a))*0) = b*(((0:b):a)a*0) \overset{(10.41)}{\leq} b*((0:b)*0) = 1\,.$$

Hieraus resultieren dann aus Gründen der Dualität zunächst (10.37) und damit weiter (A1), (A2) und ihre rechts/links dualen Versionen.

Der Rest darf dem Leser überlassen bleiben. □

Als nächstes studieren wir den Term $a*ab$ und erhalten als ein erstes Ergebnis

(10.42) $$\begin{aligned} a*ab &= ((0:(a*0))*(0:(b*(a*0)) \\ &= ((0:(a*0))*0):(b*(a*0)) \\ &= (a*0):(b*(a*0)) \\ &= (a*0)\wedge b\,. \end{aligned}$$

Insbesondere erhalten wir damit

(10.43) $$b \leq a*0 \Longrightarrow a*ab = b\,.$$

Wir sind interessiert an einer Verallgemeinerung. Aus diesem Grunde beweisen wir als nächstes

(10.44) $$x \leq ay \;\&\; y \leq a*0 \;\Longrightarrow\; x*ay = (x*a)((a*x)*y)\,.$$

Vermöge (10.40) und (10.43) erhalten wir vorab

(10.45) $$\begin{aligned} x*ay &= (a\wedge x)(a*x)*(a\wedge x)\cdot(x*a)y \\ &= (a*x)*(x*a)y\,. \end{aligned}$$

mit $a*x \perp x*a$. Folglich genügt es

$$a\,\big|\,b\cdot c \;\&\; a\perp b \;\&\; c \leq b*0 \Longrightarrow a*b\cdot c = b\cdot(a*c)$$

nachzuweisen. Im Falle von $a\,\big|\,bc \;\&\; a\perp b$ und $c \leq b*0$ erhalten wir zunächst $a*c \leq ab*0$ und damit weiter

$$\begin{aligned} as \geq bc &\overset{(3.107)}{\Longrightarrow} s = b(b*s) \;\&\; c = a(a*c) \\ &\Longrightarrow ab((a*c)\wedge(b*s)) = ab(a*c)\,, \end{aligned}$$

also $a * c \leq b * s$ und damit $b(a * c) \leq s$, was den Beweis von (10.44) abschließt. Hiernach erhalten wir endlich

$$\begin{array}{rcl} y & \leq & a * 0 \\ & \Longrightarrow & \\ x * ay & = & ((x \wedge ay)) * a)((a * (x \wedge ay) * y) \\ & = & (x * a)((a * x \wedge y) * y) \\ & = & (x * a)((a * x) * y) \end{array} \tag{10.46}$$

und selbstverständlich die duale Version, wegen

$$b \leq a * 0 \Longrightarrow 0 : b \geq 0 : (a * 0) = a \quad (\Longrightarrow \forall c \ \ c * a \leq 0 : b\,). \tag{10.47}$$

Nun können wir zeigen

10. 3. 2 Lemma.

$$xy = uv \ \&\ y \leq x * 0\ ,\ \ v \leq u * 0 \Longrightarrow (u * x)(y : v) = (x * u)(v : y)$$

BEWEIS. $xy = uv \Longrightarrow (x \wedge u)(u * x) \cdot y = (x \wedge u)(x * u) \cdot u\,,$

und es gilt

$$(u \wedge x) * 0 = ((u \wedge x) * x)(x * 0) = ((u \wedge x) * u)(u * 0)$$

also

$$((u \wedge x) * x) \cdot y \leq (u \wedge x) * 0 \ \&\ ((u \wedge x) * u) \cdot u \leq (u \wedge x) * 0\,.$$

Daher erhalten wir zunächst

$$xy = uv \Longrightarrow (u * x) \cdot y = (x * u) \cdot v \tag{10.48}$$

und hiernach analog – mittels (10.47) –

$$xy = uv \Longrightarrow (u * x) \cdot (y : v) = (x * u) \cdot (v : y)\,. \tag{10.49}$$

Damit sind wir am Ziel. □

10. 3. 3 Proposition. *In jedem Brick sind die nachfolgenden Bedingungen* (LE 1) *und* (LE 2) *äquivalent*

(LE1) $\qquad a * c = b : d \ \ \&\ \ c * a = d : b\,.$

(LE2) $\qquad ab = cd \ \ \&\ \ (a * 0) * b = (c * 0) * d\,.$

Insbesondere definieren diese Bedingungen mittels (LE2) *eine Äquivalenzrelation* $\equiv$ *auf der Menge aller Paare* $a\,.\,b$ *via*

$$\begin{array}{lccc} \text{(E)} & a\,.\,b & \equiv & c\,.\,d \\ & & :\Longleftrightarrow & \\ \text{(G)} & a*c=b:d & \& & c*a=d:b\,. \end{array}$$

BEWEIS. Bedingung (LE1) impliziert:

$$\begin{array}{rcl} c*a=d:b & \& & a*c=b:d \\ & \Longrightarrow & \\ ab & = & cd \\ & & \\ & \& & \\ (a*0)*b & = & ((a*0)*(a*c))*((a*0)*b) \\ & = & ((a*c)*(a*0))*((a*c)*b) \\ & = & ((a*c)*(a*0))*((b:d)*b) \\ & = & ((c*a)*(c*0))*((d:b)*d) \\ & = & ((c*0)*(c*a))*((c*0)*d) \\ & = & (c*0)*d\,, \end{array}$$

das ist Bedingung (LE2).

Sei nun (LE2) erfüllt. Dann erhalten wir nach Voraussetzung

$$a(b:((a*0)*b))=c(d:((c*0)*d) \tag{10.52}$$

$$(b:((a*0)*b)):(d:((c*0)*d)=b:d \tag{10.53}$$

was mittels (10.49) zu

$$(c*a)\cdot(b:d)=(a*c)\cdot(d:b)$$

führt, also zu Bedingung (L1). $\square$

10. 3. 4 Korollar. *Aufgrund der Rechts/Links-Dualität schließt das vorauf gegangene Lemma die Äquivalenz ein:*

$$(a*0)*b=(c*0)*d \Longleftrightarrow a:(0:b)=c:(0:d) \tag{10.54}$$

10.4 Zur Einbettung von Semiclans

y Wie oben gezeigt, erfüllt jeder Brick die Bedingungen

$$(a * b) * (a * c) = (b * a) * (b * c) \tag{10.55}$$

$$(c : a) : (b : a) = (c : b) : (a : b)\,. \tag{10.56}$$

Dies ermöglicht eine Abkürzung der Einbettungsprozedur des Kegel-Clan-Theorems 6.3.3 für diesen Sonderfall. Zur Erinnerung:
Sei $\mathfrak{C} := (C, \wedge, \cdot)$ ein Halbverband mit partieller Multiplikation. Dann hatten wir $\mathfrak{C}$ einen Semiclan genannt, wenn die nachfolgenden Regeln galten:

$$a \leq b \Longrightarrow \exists x, y : \quad b = ax \;\&\; b = ya \tag{C1}$$

$$\begin{aligned} ax, ay \in C \;\&\; ax = ay &\Longrightarrow x = y \\ xa, ya \in C \;\&\; xa = ya &\Longrightarrow x = y \end{aligned} \tag{C2}$$

$$\begin{aligned} ax, ay \in C &\Longrightarrow ax \wedge ay = a(x \wedge y) \\ xa, ya \in C &\Longrightarrow xa \wedge ya = (x \wedge y)a \end{aligned} \tag{C3}$$

$$ab \in C \;\&\; (ab)c \in C \iff bc \in C \;\&\; a(bc) = a(bc) \tag{C4}$$

$$(a \wedge b)c = c \;\&\; a \vee b \in C \Longrightarrow ab = a \vee b = ba\,. \tag{C5}$$

Wir nennen nun $\mathfrak{C}$ positiv, wenn zusätzlich $a \leq xa, ax \in C$ erfüllt ist. Des weiteren nennen wir $\mathfrak{C}$ beschränkt, falls C ein Topelement 0 enthält.
Das Ziel dieses Abschnitts ist die Einbettung des positiven beschränkten Semiclans, kurz *pb-Semiclans,* in einen Verbandsgruppenkegel, betrachtet als positiver Semiclan, auf dem Wege einer direkten Konstruktion.

10. 4. 1 Proposition. *Jeder pb-Semiclan lässt sich auffassen als Brick, jeder Brick last sich auffassen als pb-Semiclan.*

BEWEIS. Sei $\mathfrak{C}$ ein *pb*-Semiclan. Wir definieren

$$a * b := x \;:\Longleftrightarrow\; (a \wedge b) \cdot x = b \tag{10.62}$$

$$b : a := y \;:\Longleftrightarrow\; y \cdot (a \wedge b) = b\,. \tag{10.63}$$

Dies führt zu

$$ax \in C \;\&\; ax \geq b \Longrightarrow (a \wedge b)x \geq b \Longrightarrow x \geq a * b \tag{10.64}$$

$$(10.65) \qquad b \geq c \Longrightarrow a * c = (a \wedge c) * c = (a \wedge b \wedge c) * c$$

und damit zu

$$(10.66) \qquad a * (b : c) \;=\; (a \wedge b) * (b : (b \wedge c))$$

$$(10.67) \qquad (a * b) : c \;=\; ((a \wedge b) * b) : (b \wedge c)\,.$$

Zu verifizieren bleibt das Axiom

$$(\mathrm{BR3}) \qquad a * (b : c) \;=\; (a * b) : c\,.$$

Sei zu diesem Zweck $a, c \leq b$. Dann ist $a(a * b)$ definiert und damit auch

$$a((a * b) : c)((a * b) \wedge c)\,.$$

Folglich gilt

$$\begin{array}{rcl} a((a * b) : c)((a * b) \wedge c) & = & a(a * b) = b \\ & \geq & (b : c)((a * b) \wedge c) \\ & \Rightarrow & \\ a((a * b) : c) & \overset{(10.64)}{\geq} & b : c \\ & \Rightarrow & \\ (a * b) : c & \overset{(10.64)}{\geq} & a * (b : c)\,, \end{array}$$

so dass sich aus Gründen der Dualität

$$(a * b) : c \;=\; a * (b : c)$$

ergibt, das ist Axiom (B3).

Sei nun $\mathfrak{B}$ ein Brick. Dann liefert die Definition $ab := 0 : (b * (a * 0))$ eine Multiplikation bezüglich der $(B, *, :, \cdot)$ eine komplementäre Halbgruppe bildet, vgl. 10.3.1. Folglich bildet $\mathfrak{B}$ einen a *pb*-Semiclan unter $\circ$, definiert mittels

$$a \circ b := ab \;:\Longleftrightarrow\; b \leq a * 0 \;\;(\;\&\; a \leq 0 : b)\,,$$

man beachte, dass $(ab)c$ genau im Falle $a * ab = b \;\&\; ab * abc = c$ erklärt ist , dass darüber hinaus $(a * ab)(ab * (ab)c) = a * a(bc)$ erfüllt ist und dass der Rest sich dualitätsbedingt ergibt. □

FAZIT: Bricks lassen sich als *pb*-Semiclans auffassen und und *pb*-Semiclans als Bricks.

SEI VON NUN AN $\mathfrak{C}$ ein Brick, betrachtet als *pb*-Semiclan. Wir werden auf der Menge der Paare $a.b$ eine Operation derart erklären, dass $C \times C$

sich als Clan-Ausdehnung von $\mathfrak{C}$ erweist. Der Rest ergibt sich dann auf ausgetretenen Bahnen.
Der Leser erinnere sich zunächst an 10.3.3, also an

$$\begin{array}{rcl} a\,.\,b \equiv c\,.\,d & :\Longleftrightarrow & a * c = b : d \quad \& \quad c * a = d : b\,. \\ & \Longleftrightarrow & ab = cd \quad \& \quad (a*0)*b = (c*0)*d\,. \end{array}$$

Insbesondere daran, das $\equiv$ eine Äquivalenzrelation definiert. Wir bezeichnen die $\equiv$-Klassen mittels $[\,a\,.\,b\,]$, ..., $[\,x\,.\,y\,]$ und erhalten:

$$[\,a\,.\,b\,] \;=\; [\,ab\,.\,(a*0)*b\,] \tag{10.69}$$

$$[\,a\,.\,b\,] \;=\; [\,a:(0:b)\,.\,ab\,] \tag{10.70}$$

sowie ihre dualen Versionen auf Grund von

$$ab * a = \quad 1 \quad = ((a*0)*b) : b \tag{10.71}$$

$$a * ab \overset{(10.42)}{=} b : ((a*0)*b)\,. \tag{10.72}$$

Damit enthält jede Klasse $[\,x\,.\,y\,]$ ein eindeutig bestimmtes Paar $X.Y$ mit $X = uv, Y = (u*0)*v$ für alle $u.v \equiv x.y$. Im Rest dieses Abschnitts werden wir stillschweigend

$$[A\,.\,B] := [\,ab\,.\,(a*0)*b\,]$$

annehmen. Das bedeutet insbesondere

$$[\,a\,.\,b\,] = [\,c\,.\,d\,] \Longleftrightarrow A = C \;\;\&\;\; B = D\,.$$

Natürlich gilt auch dual

$$[\,\overline{A}\,.\,B\,] := [\,a:(0:b)\,.\,ab\,] = [\,a\,.\,b\,]\,. \tag{10.73}$$

Folglich erhalten wir

$$[A\,.\,B] = [\,AB\,.\,B\,] = [\,\overline{A}\,.\,\overline{A}B\,] = [\,\overline{A}\,.\,B\,]\,. \tag{10.74}$$

10. 4. 2 Definition. Wir setzen

$$\begin{array}{c} [\,a\,.\,b\,] \circ [\,c\,.\,d\,] \quad := \quad [\,A\overline{C}\,.\,BD\,] \\ \text{gdw.} \\ A*0 \geq \overline{C} \quad \& \quad B \leq 0:D \end{array}$$

$$\text{und} \qquad [\,a\,.\,b\,] \mathrel{\overline{\leq}} [\,c\,.\,d\,] \;:\Longleftrightarrow\; A \leq C \;\&\; B \leq D\,.$$

$\circ$ und $\overline{\le}$ sind nach Konstruktion wohl definiert. Wir werden nun zeigen, das $([C \times C], \circ, \overline{\le})$ eine *pb*-Semiclan-Erweiterung von $\mathfrak{C}$ bezüglich $\circ$ und $\overline{\le}$ bildet.

Zur Assoziativität

Wir beginnen mit dem Nachweis von Axiom (C4) im Sonderfall

$$([\,a\,.\,b\,] \circ [\,e\,.\,c\,]) \circ [\,e\,.\,d\,]\,.$$

Als ERSTES zeigen wir:

$[\,a\,.\,b\,]\circ[\,c\,.\,d\,]$ ist definiert gdw. $([\,a\,.\,b\,]\circ[\,e\,.\,c\,])\circ[\,e\,.\,d\,]$ definiert ist.

Zu diesem Zweck haben wir zu verifizieren, dass die nachfolgenden Bedingungen (1) & (2) in Kombination mit (A)

(1) $c : (0 : d) \le b * (a * 0)$

(2) $(a * 0) * b \le (0 : d) : c$

äquivalent sind zu den Bedingungen nachfolgenden Bedingungen (a) & (b), in Kombination mit (B)

(a) $(a * 0) * b \le 0 : c$

(b) $(ab * 0) * ((a * 0) * b)c \le 0 : d\,.$

(A)$\Longrightarrow$(B). (a) resultiert unmittelbar aus (2), und mittels (1) und (2) erhalten wir

$$\begin{aligned}
(ab * 0) * ((a * 0) * b)c &\overset{(10.46)}{=} ((a * 0) * b)((ab * 0) * c)\\
&\le ((0 : d) : c)((c : (0 : d)) * c)\\
&= ((0 : d) : c) \cdot ((0 : d) : c) * (0 : d))\\
&= (0 : d) : c \vee 0 : d\\
&= 0 : d\,.
\end{aligned}$$

Als nächstes beweisen wir (b)$\Longrightarrow$(A), was *a fortiori* (B)$\Longrightarrow$(A) erzwingt.
(b)$\Longrightarrow$(A). Bedingung (1) folgt aus Bedingung (b) vermöge

$$\begin{aligned}
c : (0 : d) &\le c : ((a * 0) * b)((ab * 0) * c)\\
&= (c : ((b * (a * 0)) * c)) : ((a * 0) * b)\\
&\le b * (a * 0)\,,
\end{aligned}$$

und Bedingung (2) resultiert aus Bedingung (b) vermöge

$$\begin{array}{rrcl} & (ab*0)*((a*0)*b)c & \leq & 0:d \\ \Longrightarrow & ((ab*0)*((a*0)*b)c):c & \leq & (0:d):c \\ \Longrightarrow & (ab*0)*(((a*0)*b)c:c) & \leq & (0:d):c \\ \Longrightarrow & ((b*(a*0))*((a*0)*b) & \leq & (0:d):c \\ \Longrightarrow & (a*0)*b & \leq & (0:d):c\,. \end{array}$$

HIERNACH verifizieren wie die Gleichheit unter der Bedingung, dass Bedingung (A) (äquivalent (B)) erfüllt ist, d.h. wie zeigen

$$L_1 * L_2 = R_1 : R_2 \quad \text{und} \quad L_2 * L_1 = R_2 : R_1$$

für den Fall unserer obigen Ausgangslage. Zu diesem Zweck betrachte man

$$\begin{array}{lrcll} (10.75) & ([\,A\,.\,B\,]\circ[\,e\,.\,c\,])\circ[\,e\,.\,d\,] & = & [\,Ac\,.\,((A*0)*Bc)d\,] & =: [\,L_0\,.\,R_1\,] \\ (10.76) & [\,A\,.\,B\,]\circ[\,c\,.\,d\,] & = & [\,A(c:(0:d))\,.\,Bcd\,] & =: [\,L_2\,.\,R_2\,]\,. \end{array}$$

Zunächst folgt fast unmittelbar

$$\underline{L_1 * L_2} = \ 1 \ = \underline{R_1 : R_2}\,,$$

und es ergibt sich weiter

$$\begin{array}{rcl} \underline{L_2 * L_1} & = & A(c:(0:d))*Ac \\ & \overset{(10.42)}{=} & (c:(0:d))*(A*0\wedge c) \\ & \overset{(3.98)}{=} & (c:(0:d))*((B:((0:d):c))*(A*0\wedge c)) \\ & & (\text{recall} \quad B\perp A*0) \\ & = & ((B:((0:d):c))(c:(0:d))*(A*0\wedge c) \\ & \overset{(10.42)}{=} & (Bc:(0:d))*(A*0\wedge c) \\ & \overset{(3.106)}{=} & (Bc:(0:d))*(A*0\wedge Bc) \\ & = & ((Bc:(0:d))*(Bc:((A*0)*Bc)) \\ & = & (((Bc:(0:d))*Bc):((A*0)*Bc)) \\ & = & (Bc\wedge(0:d)):((A*0)*Bc) \\ & \overset{(10.46)}{=} & (Bcd:d):((A*0)*Bc) \\ & = & Bcd:((A*1)*Bc)d = \underline{R_2 : R_1}\,, \end{array}$$

also

$$([\,a\,.\,b\,] \circ [\,e\,.\,c\,]) \circ [\,e\,.\,d\,] = ([\,a\,.\,b\,] \circ ([\,e\,.\,c\,]) \circ [\,e\,.\,d\,]) \,. \tag{10.77}$$

Dies impliziert dann – fast unmittelbar:

$$\begin{aligned} ([\,a\,.\,e\,] \circ [\,u\,.\,v\,]) \circ [\,e\,.\,d\,] &= [\,au\,.\,vd\,] \\ &= [\,a\,.\,e\,] \circ (([\,u\,.\,v\,] \circ [\,e\,.\,d\,]) \,. \end{aligned} \tag{10.78}$$

Hieraus folgt dann die allgemeine Assoziativität geradeaus mittels (10.77) und (10.78) , auf Grund der Rechts-/Links-Dualität.

SCHLIESSLICH betonen wir

$$a * 0 \geq b \Longrightarrow [\,a\,.\,e\,] \circ [\,b\,.\,e\,] = [\,ab\,.\,e\,] \,,$$

das ist die Einbettungseigenschaft bezüglich der partiellen Operation $\circ$.

Zu den Kürzungsregeln

$$\text{(LCR)} \qquad [\,a\,.\,b\,] \circ [\,x\,.\,y\,] = [\,a\,.\,b\,] \circ [\,u\,.\,v\,] \;\Longrightarrow\; [\,x\,.\,y\,] = [\,u\,.\,v\,]$$

$$\text{(RCR)} \qquad [\,x\,.\,y\,] \circ [\,a\,.\,b\,] = [\,u\,.\,v\,] \circ [\,a\,.\,b\,] \;\Longrightarrow\; [\,x\,.\,y\,] = [\,u\,.\,v\,] \,.$$

BEWEIS. Nach Definition und auf Grund der Rechts-/Links-Dualität können wir uns darauf beschränken die Implikation (LCR) zu verifizieren und hier auf Grund der Assoziativität auf den Sonderfall $b = 1$, also auf:

$$\begin{array}{rcl} [\,a\,.\,1\,] \circ [\,x\,.\,y\,] &=& [\,a\,.\,1\,] \circ [\,u\,.\,v\,] \\ &\Rightarrow& \\ [\,ax\,.\,y\,] &=& [\,au\,.\,v\,] \\ &\Rightarrow& \\ \multicolumn{3}{c}{ax * au = x * (a * au) = y : v} \\ &\Rightarrow& \\ x * u &=& y : v \quad (\text{wegen } u \leq a * 0) \\ &\Rightarrow& \\ [\,x\,.\,y\,] &=& [\,u\,.\,v\,] \end{array}$$

die letzte Zeile aus Gründen der Dualität. □

Ordnungsprobleme

Die verbleibenden Axiome (C1), (C3), (C5) betreffen Ordnungsprobleme.

Als erstes erhalten wir, dass $C \times C/\equiv$ bezüglich $\overline{\leq}$ einen Verband mit $[\,1\,.\,1\,]$ als Minimum und $[\,0\,.\,0\,]$ als Maximum bildet.
Als nächstes erhalten wir die Divisoreneigenschaft, d.h.

$$\begin{array}{rcl} [\,A\,.\,B\,] & \overline{\leq} & [\,C\,.\,D\,] \\ & \Longrightarrow & \\ [\,C\,.\,D\,] & = & [\,A\,.\,B\,]\circ[\,X\,.\,Y\,] \\ & = & [\,U\,.\,V\,]\circ[\,A\,.\,B\,] \\ & & (\exists\,[\,U\,.\,V\,],[\,X\,.\,Y\,])\,. \end{array} \tag{10.81}$$

BEWEIS. Auch hier dürfen wir uns *per definitionem* und auf Grund der Dualität auf eine Seite beschränken, z.B. auf die Links-Teilereigenschaft. Dann folgt unter Annahme von $D = BY$ mit $B * 0 \geq Y$ und $E := 1$

$$\begin{array}{rcl} [\,A\,.\,D\,] & = & [\,A\,.\,BY\,] \\ & = & [\,A\,.\,E\,]\circ([\,B\,.\,E\,]\circ[\,E\,.\,Y\,]) \\ & = & ([\,A\,.\,E\,]\circ[\,E\,.\,B\,])\circ[\,E\,.\,Y\,] \\ & = & [\,A\,.\,B\,]\circ\underline{[\,E\,.\,Y\,]\,.} \end{array}$$

Folglich sind wir am Ziel, sobald wir das Problem für $B = D$ gelöst haben. Betrachten wir also den Fall $[\,AX\,.\,B\,]$ mit $X \leq A * 0$. Hier erhalten wir:

$$\begin{array}{rcl} [\,AX\,.\,D\,] & = & [\,AX\,.\,B\,] \\ & = & [\,A\,.\,E\,]\circ[\,X\,.\,B\,] \\ & = & [\,A\,.\,E\,]\circ[\,XB\,.\,(X*0)*B\,] \\ & = & [\,A\,.\,XB\,]\circ[\,E\,.\,(X*0)*B\,] \\ & = & [\,A\,.\,B(B*XB)\,]\circ[\,E\,.\,(X*0)*B\,] \\ & = & [\,A\,.\,B\,]\circ\underline{([\,E\,.\,B*XB\,]\circ E\,.\,(X*0)*B\,]}\,. \end{array}$$

□

SCHLIESSLICH erhalten wir durch Kombination der Verbandseigenschaft mit der Kürzungseigenschaft Axiom (C3), während Axiom (C5) nach Definition fast evident ist, man beachte $a \wedge b = 0 \Longleftrightarrow a * b = b$.

DAMIT IST

nach abzählbarer Wiederholung entlang wohlbekannter Linien

DIE EINBETTUNG ABGESCHLOSSEN.

Ein Hinweis: Die obige Methode wirkt schon in nach oben gerichteten Se-

miclans, da unter dieser Bedingung jeder Schritt unterhalb einer geeigneten oberen Schranke realisiert werden kann.
Folglich bedeutet die Erweiterung einen Semiclans zu einem sup-abgeschlossenen Semiclan und anschließende Anwendung der obigen Methoden eine alternative Einbettung für Semiclans.
Jedoch erfordert die Konstruktion einer solchen Erweiterung einige Anstrengung, man vergleiche [24], wo eine eindeutig bestimmte Ausdehnung dieses Typs in einem allgemeineren Kontext konstruiert wird.

10.5 Zur Einbettung kommutativer Bricks

In diesem Abschnitt betrachten wir kommutative Bricks, um eine Abkürzung des allgemeinen Einbettungsbeweises vorzustellen, die vom didaktischen Standpunkt aus von Wert sein könnte.

10. 5. 1 Proposition. *Erfülle* $(G*, 0)$ *die Bedingungen*

$$a * (b * c) = b * (a * c) \tag{10.82}$$
$$a * (b * b) = c * c \tag{10.83}$$
$$(a * 0) * 0 = a\,. \tag{10.84}$$

Dann sind die Gleichungen

$$(a * b) * (a * c) = (b * a) * (b * c) \tag{10.85}$$
$$(a * b) * b = (b * a) * a \tag{10.86}$$

unter Voraussetzung von (10.82) *bis* (10.84) *äquivalent zueinander.*

BEWEIS. Nach (10.84) ist jedes a vom Typ $x * 0$ und nach (10.82) bis (10.85) folgt

$$((a * 0) * (b * 0)) * (b * 0) = (b * a) * (b * 0) = ((b * 0) * (a * 0)) * (a * 0)\,,$$

d.h. Gleichung (10.86).
Auf der anderen Seite ziehen (10.82), (10.83), (10.84), (10.86)

$$\begin{aligned} (a * b) * (a * c) &= ((b * 0) * (a * 0)) * ((c * 0) * (a * 0)) \\ &= (c * 0) * (((b * 0) * (a * 0)) * (a * 0)) \\ &= (b * a) * (b * c) \end{aligned}$$

nach sich, das ist Gleichung (10.85). □

Sei nun $\mathfrak{B} = (B, *, 0)$ ein kommutativer Brick, definiert mittels (10.82) bis (10.85). Im Einbettungssatz haben wir $B \times B$ bezüglich

$$\text{(M)} \qquad a\,.\,b \star c\,.\,d \;:=\; b * (a * c)\;.\;((a * c) * b) * (((c * a) * b) * d)$$

und

$$\text{(C)} \qquad a\,.\,b \equiv c\,.\,d \;:\Longleftrightarrow\; a\,.\,b \star c\,.\,d = 1\,.\,1 = c\,.\,d \star a\,.\,b$$

betrachtet.

Da (10.85) sich von $(B, *)$ nach $(B \times B, \star)$ fortpflanzt, folgt leicht, dass $\equiv$ eine Kongruenzrelation ist. Des weiteren erhalten wir geradeaus

$$\begin{aligned}
&(10.89) & a\,.\,b \star 1\,.\,1 &= 1\,.\,1\\
&(10.90) & a\,.\,b &\equiv b\,.\,a\\
&(10.91) & a\,.\,b \star c\,.\,d &= b\,.\,1 \star (a\,.\,1 \star c\,.\,d)\,.
\end{aligned}$$

Das liefert – ohne Probleme – dass (C) eine Kongruenzrelation ist, so dass uns nur zu zeigen bleibt, dass die $\equiv$-Klassen $[\,x\,.\,y\,]$ den Bedingungen genügen

$$\text{(S)} \qquad ([\,a\,.\,b\,] \star ([\,c\,.\,d\,]) \star [\,u\,.\,v\,] \;=\; ([\,c\,.\,d\,] \star ([\,a\,.\,b\,]) \star [\,u\,.\,v\,]$$

$$\text{(T)} \qquad ([\,a\,.\,b\,] \star [\,0\,.\,0\,]) \star [\,0\,.\,0\,] \;=\; [\,a\,.\,b\,]\,.$$

Hier folgt zunächst (S) durch wiederholte Anwendung von (10.91). Und weiter erhalten wir

$$(10.94) \qquad a\,.\,b \star c\,.\,d = c * a\,.\,b \star a * c\,.\,d \equiv c * a\,.\,d * b \star a * c\,.\,b * d\,,$$

was zu

$$(10.95) \qquad a\,.\,b \equiv c\,.\,d \Longrightarrow (d * b) * (a * c) = 0 = (a * c) * (d * b)$$

führt und folglich auf Grund von Dualität und Symmetrie zu

$$(10.96) \qquad a\,.\,c \equiv c\,.\,d \Longleftrightarrow a * c = d * b \;\&\; c * a = b * d\,.$$

Das zieht dann weiter nach sich

$$
\begin{aligned}
(10.97) \qquad & ([\,a\,.\,b\,] \star [\,0\,.\,0\,]) \star [\,0\,.\,0\,] \\
= \;& [\,b * (a * 0)\,.\,((a * 0) * b) * 0\,] \star [\,0\,.\,0\,] \\
= \;& [\,(((a * 0) * b) * 0) * ((b * (a * 0)) * 0) \\
. \;& (((b * (a * 0)) * 0) * ((a * 0) * b) * 0)) * 0\,] \\
= \;& [\,((a * 0) * b)\,.\,((b * (a * 0)) * 0)\,] =: [\,L\,.\,R\,] \\
= \;& [\,ab\,.\,(a * 0) * b\,] \\
= \;& [\,a\,.\,b\,]
\end{aligned}
$$

Die vorauf gegangene Herleitung beruht auf dem vorhergehenden Abschnitt. Deshalb bieten wir zusätzlich noch als einen direkten Beweis von $[\,L\,.\,R\,] = [\,a\,.\,b\,]$ die beiden nachfolgenden Gleichungen an:

$$(10.98) \quad a*((a*0)*b) = (a*0)*(a*b) = 1 = ((b*(a*0))*0)*((b*0)*0)$$

$$(10.99) \quad ((a*0)*b)*((a*0)*0) = (b*(a*0))*(b*0) = b*((b*(a*0))*0)\,.$$

10.6 Abschließende Bemerkungen

In Sonderfällen wirken – was nicht überrascht – schon höchst vertraute Einbettungs-Methoden. Unter diesen seien nur zwei hervorgehoben, nämlich der endliche Fall $Ł_n$ und der indexsemiclan!divisibler divisible kommutative Fall.

10. 6. 1 Beispiel. *Betrachte* $Ł_g := \{0, 1, ..., g\}$ *bezüglich* $\oplus$, *definiert vermöge* $a \oplus b := a + b$ *gdw.* $a + b \leq g$.

Hier können wir uns zum einen an Peano orientieren, während wir auf der anderen Seite auch über die g-al-Darsellung zusammen mit der g-al-Addition zum Ziel gelangen.
In jedem dieser beiden Fälle ist der korrespondierende Verbandsgruppenkegel isomorph zu $(\mathbf{N}^0, +)$, insbesondere ist damit das Ergebnis unabhängig von der gewählten Basis g.
In anderen Worten: Die erzeugte Verbandsgruppe ist in jedem Falle isomorph zu der additiven Gruppe $\mathfrak{Z}$.

10. 6. 2 Beispiel. *Betrachten wir nun das reelle Einheitsintervall bezüglich der partiellen Operation* $\oplus$, *definiert vermöge* $a \oplus b := a + b$ gdw. $a + b \leq 1$ *– uns bezeichnen wir diese Algebra mit* $\mathfrak{E}$.

Dann folgt $\mathfrak{E}_{\frac{1}{2}} := ([0,1/2], \oplus_{\frac{1}{2}})$ mit $a \oplus_{\frac{1}{2}} b := a + b$ gdw. $a + b \leq 1/2$ isomorph ist zu $\mathfrak{E}$. Das bedeutet, dass $\mathfrak{E}$ die erste Erweiterung zu $\mathfrak{E}_{\frac{1}{2}}$ ist.
Erneut in anderen Worten: der Brick $\mathfrak{E}_{\frac{1}{2}}$ ist isomorph zu $\mathfrak{E}$, und man kann $\mathfrak{E}$ als Erweiterung von $\mathfrak{E}_{\frac{1}{2}}$ betrachten, womit der erste und grundlegende Einbettungsschritt getan ist.
Es bleibe an dieser Stelle dem Leser überlassen, weitere geeignete Intervalle zu finden.

10. 6. 3 Beispiel. *Sei hiernach $\mathfrak{C}$ eine divisibler kommutativer pb-Semiclan, also ein pb-Semiclan, dessen Elemente a eine Zerlegung $a = \frac{a}{2} \oplus \frac{a}{2}$ zulassen.*
Dann ist $\frac{a}{2}$ eindeutig bestimmt, da $x \oplus x = a \Longrightarrow x \oplus x = xx$ und $2a \wedge 2b = 2(a \wedge b)$ im Falle von $2a = 2b \leq 0$ zu $a * b = 1 = b * a$ und somit zu $a = b$ führt, man beachte die Kürzungsregeln (RCR) und (LCR) .
Folglich können wir operieren wie im vorauf gegangenen Beispiel.

Obacht! Jede Kegel-Algebra lässt sich wegen

$$ab \leq c \in B \Longrightarrow ab = ab \wedge c = (c : ab) * c = ((c : b) : a) * c \in B$$

sogar als Ordnungsideal in einen Verbandsgruppenkegel einbetten. Das kann sich sehr viel anders verhalten, haben wir es lediglich mit einem RR-Gruppoid zu tun. Hierzu betrachten wir eine Menge $\{1, p \neq q, 0\}$ mit primen p, q bezüglich $*$, definiert vermöge $x*y = 1 :\Longleftrightarrow y \,\big|\, x$, und $x*y = y$ im anderen Fall. Dies liefert uns ein *RR*-Gruppoid, was zu einer links-kürzbaren, rechts-komplementären Halbgruppe $(S, \cdot, \star)$ führt mit $p \cdot q < 0$ wegen $0 \star pq = (0 \star p)((p \star 0) \star q) = (0 * p)((p * 0) * q) = 1$ und $pq \notin \{0, p, q, 1\}$, wegen $pq \star 0 = q \star (p \star 0) = q * (p * 0) = 0 \rightsquigarrow pq \neq 0$, $pq = p \Longrightarrow q = 1$, $pq = q \Longrightarrow 1 = q \star pq = (q \star p)((p \star q) \star q) = (q * p)((p * q) * q) = p$ sowie $pq = 1 \Longrightarrow p = 1 = q$.

Kapitel 11

Teilbarkeits-Semiloops

11.1 Einführung

Wir führen den Leser an dieser Stelle breit ein, um ihm eine Basis für das abschließende Kapitel – zum Darstellungsproblem – zu bieten.
Unter einem *Gruppoid* verstehen wir eine *Algebra* $(G,\cdot) =: \mathfrak{G}$ des *Typs* (2).
Unter einem *binären System* verstehen wir ein Gruppoid, das schwächer ist als die *Gruppe.* Spezielle binäre Systeme sind also u. a. *Halbgruppen, Quasigruppen* und *Loops* . Die Bezeichnung binäres System geht zurück auf R. H. Bruck, vgl. [46].
Ein binäres System $\mathfrak{G}$ heißt *partial* bzw. *verbands-* geordnet, wenn G partial bzw. verbandsgeordnet ist und zudem der Bedingung genügt:

$$(0) \qquad a \leq b \Longrightarrow xa \leq xb \ \&\ ax \leq bx\ .$$

Ist $(G,\cdot,\leq)$ verbandsgeordnet, so nennen wir $(G,\cdot,\leq)$ kurz ein *Verbandsgruppoid* .
Als *Verbandshalbgruppe* bezeichnen wir demzufolge jedes assoziative Verbandsgruppoid. Analog sprechen wir von einer *Verbandsquasigruppe*, wenn alle Gleichungen $ax = b$ und $ya = b$ eindeutige Lösungen a/b im ersten und $b\backslash a$ im zweiten Fall besitzen. Demzufolge verstehen wir unter einer *Vrbands-Loop* eine Verbandsquasigruppe mit 1. Existiert in einer Verbandsloop $\mathfrak{L}$ zu jedem x ein x^{-1} mit $x^{-1}(xa) = a$ und $a = (ax)x^{-1}$, so sagt man, $\mathfrak{L}$ habe die *Inverseneigenschaft.* Ist dies der Fall, so gilt zudem $(x^{-1})^{-1} = x$ und $(xy)^{-1} = y^{-1}x^{-1}$, wie der Leser leicht bestätigt.
Es gibt keinen Mangel an Verbandsquasigruppen. Um dies einzusehen, betrachten wir $(R^n,\leq)$ bezüglich $a \circ b := a + nb$ $(n \in \mathbf{N})$ mit fixem n.
Weiterhin gibt es einen Überfluss an Verbandsloops, da wir ausgehend von

einer Verbandsquasigruppe $(Q, \circ, \wedge, \vee)$ eine Verbandsloop erhalten, wenn wir für ein vorgegebenes x, y definieren: $a \cdot b := (a/x) \circ (y \backslash b)$. In diesem Falle fungiert $x \circ y$ als 1 als Eins. Und schließlich sollte betont werden, dass die freie Loop nicht nur eine *Verbandsordnung,* sondern sogar eine *lineare Ordnung* zulässt, [89], [90].

Verbandsgeordnete binäre Systeme sind *kongruenz-distributiv* in jedem Falle und *kongruenz-vertauschbar* in vielen Fällen. Demzufolge ist die Theorie der *verbandsgeordneten* binären Systeme reich vom rein algebraischen Standpunkt aus gesehen. Auf der anderen Seite aber gibt es noch nicht viele Ergebnisse über *Verbandsgruppoide* basierend auf ornungstheoretischen oder kombinierten Aspekten, obwohl bereits G. Birkhoff in [10] und ebenso L. Fuchs in [79] Probleme dieser Art formulieren. Dennoch, zumindest eine fruchtbare Theorie der Verbandsloops scheint möglich, was sich schon in [10] andeutet und geradezu suggeriert wird durch Ergebnisse von Evans und Hartman, [71], die als erste einen Durchbruch schafften, nach mehreren Beiträgen verschiedener Autoren wie Zelinsky [162], [163], Kaplansky sowie Ingraham & Birkhoff (s. [10]) und Aczél [2].

Die zentrale Struktur dieses Kapitels ist die des *Teilbarkeitssemiloop,* kurz, die *d-semiloop,* definiert als *sup-halbverbandsgeordnetes Kürzungsgruppoid mit* 1, derart dass gilt

$$ax \leq b \Longrightarrow \exists u : au = b \;\&\; ya \leq b \Longrightarrow \exists v : va = b\,.$$

Somit ist die d-semiloop eine gemeinsame Verallgemeinerung der Verbands-Loop und des *Verbandsloop-Kegels.*

Jede *Verbandsgruppe* ist, wie wir oben sahen, *Quotientenerweiterung* ihres *Kegels* in solcher Weise, dass die Struktur des Ganzen völlig bestimmt wird durch die Struktur des Kegels. Dies ist ganz anders im Falle einer Verbandsloop, wo nicht einmal eine *lineare* oder eine *vollständige* Ordnung des *positiven* Kegels Einfluss auf den *negativen* Kegel nehmen. Um dies einzusehen betrachte der Leser die reelle Achse bezüglich

$$a \circ b := \begin{cases} a + b & \text{falls eine Komponente negativ ist} \\ a - ab + b & \text{im anderen Fall}\,. \end{cases}$$

Von daher scheint die Situation hoffnungslos. Dennoch gilt ein Ergebnis, das einiges Licht wirft für den Fall, dass man den Kegel isoliert betrachtet, denn wir werden zeigen:

> *Verbandsloop-Kegel* sind identisch mit den positiven d-semiloops, und jeder Verbandsloop-Kegel ist sogar Kegel einer *Verbandsloop mit Inverseneigenschaft.*

Dies vertieft ein Theorem von J. v. Neumann und beantwortet zugleich eine von ihm gestellte Frage, (s. [10]), vor allem aber vermittelt dieses Resultat Hoffnung auf eine Möglichkeit, allgemeine Verbandsloop-Probleme erfolgreich auf dem Wege über *inverse Verbandsloops* angehen zu können.
Ist ein geordnetes binäres System gegeben, stellt sich als erstes *Ordnungsproblem* die Frage, was die *absteigende Kettenbedingung* für *abgeschlossene Intervalle* vom rein algebraischen Standpunkt aus bedeutet. So ist denn diese Frage wiederholt für die verschiedensten algebraischen Systeme behandelt worden, insbesondere für *Halbgruppen* von Arnold [3], Clifford [52], [53], Lorenzen [119] und anderen, (s. [80]), und für Verbandsgruppen von Birkhoff und Ward, siehe etwa [10]. Doch für Verbandsloops blieb die Frage offen bis Evans [70] zeigte, dass Verbandsloops, die dieser Bedingung genügen, übereinstimmen mit den *abelschen Verbandsgruppen* mit *eindeutiger Primelementzerlegung.* Das liefert als Korollar, dass jede Verbandsquasigruppe mit D. C. C. das *Isotop* einer *freien abelschen Gruppe* ist. Siehe hierzu auch Testov.
Dies regt an zu einer ähnlichen Untersuchung von d-semiloops, und es ist in keiner Weise überraschend, dass ein Analogon zu Evans' Theorem gültig bleibt. Aber es sind – in den Augen des Verfassers – weniger die Resultate als die Methoden, die diesen Abschnitt rechtfertigen.
Zwei natürliche Verallgemeinerungen der Kettenbedingung bzw. der Primelementzerlegungseigenschaft bieten sich an, zum einen die *Vollständigkeit* (für abgeschlossene Intervalle) und zum anderen die *Repräsentierbarkeit*, d.h. die Eigenschaft, eine subdirekte Zerlegung in *linear geordnete Faktoren* zu besitzen.
Soweit Vollständigkeit betrachtet wird, werden wir beweisen, dass *potenzassoziative d-semiloops* sogar assoziativ und kommutativ sind, womit Iwasawas Theorem [100] über die Kommutativität vollständiger Verbandsgruppen auf d-semiloops übertragen wird. Weiter werden wir in einem vierten Abschnitt zeigen, dass Vollständigkeit, lediglich kombiniert mit *Monassoziativität* eine zu schwache Forderung darstellt, um Assoziativität oder Kommutativität zu erzwingen.
Als ein weiteres Problem im Kontext der Vollständigkeit greifen wir die Fra-

ge nach d-semiloops auf, die eine *vollständige Erweiterung* zulassen. Dies ist im Blick auf verbandsgruppenähnliche Strukturen wiederholt zum Gegenstand vom Untersuchungen gemacht worden. Hier waren dem Anschein nach wohl ARNOLD [3] und VAN DER WAERDEN [155] die ersten, die ein *Einbettungsproblem* im allgemeinen behandelt haben, vor anderen, wie LORENZEN [119], CLIFFORD [52], [53], und später EVERETT & ULAM [72], die als erste einen nicht kommutativen Fall behandelten. Doch eine Analyse nicht assoziativer Verhältnisse gab niemand vor 1972, als P. A. HARTMAN [89], [90] das Problem der vollständigen Einbettung für partial geordnete Quasigruppen und Loops erledigte. Natürlich gibt es noch weitere Resultate, man konsultiere etwa [10] und [32], vor allem selbstverständlich RICHARD DEDEKINDS Initialbeitrag (s. [60]). Somit bedeutet die Charakterisierung von d-semiloops mit vollständiger Erweiterung einen höchst natürlichen weiteren Schritt im Blick auf eine lang anhaltende Entwicklung. Schließlich wenden wir uns *repräsentierbaren* d-semiloops zu und werden dabei einen Schlüssel vorstellen, der im letzten Kapitel ganz allgemein das Problem der Repräsentierbarkeit erschließen wird.

EIN HINWEIS: Es werden sich duale Sachverhalte verschiedenster Art einstellen, z. B. rechts- links Dualitäten oder $\geq/\leq$ Dualitäten. Folglich wird es Aussagen geben, die zwangsläufig zusammen mit der zu ihnen dualen Aussage gelten. Deshalb sollte der Leser einen solchen Sachverhalt realisieren, wo immer er sich einstellt. Dennoch wird er von Zeit zu Zeit ausdrücklich aufgefordert werden, dieser Tatsache Rechnung zu tragen.

11.2 d-Semiloops

11. 2. 1 Definition. Eine Algebra Algebra $\mathfrak{G} := (G, \cdot, \wedge, 1)$ vom Typ (2,2,0) heiße eine *Teilbarkeits-Semiloop,* wenn sie den Gesetzen genügt:

(DSL 1) $\quad (G, \cdot)$ ist ein *Kürzungsgruppoid.*

(DSL 2) $$1 \cdot a = a = a \cdot 1$$

(DSL 3) $\quad (G, \wedge)$ ist ein *Halbverband.*

(DSL 4) $$x(a \wedge b) \cdot y = xa \cdot y \wedge xb \cdot y$$

(DSL 5) $$\begin{aligned} ax \leq b &\implies \exists u : au = b \\ ya \leq b &\implies \exists v : va = b\,. \end{aligned}$$

Ist $\mathfrak{G}$ eine Teilbarkeits-Semiloop, so nennen wir $\mathfrak{G}$ auch kurz eine *d-semiloop* – in Abkürzung von *divisibility semiloop.*

Man beachte, dass (DSL 4) aufgrund von (DSL 2) Rechts- und *Links-Distributivität* fordert und man beachte ferner, dass der *negative Kegel* einer jeden d-semiloop auch aufgefasst werden kann als positive d-semiloop bezüglich $\vee$, wegen der Implikation $a, b \leq 1 \Longrightarrow ab \leq b$.
Klassische Beispiele der d-semiloop sind die *Verbandsloop* und *ihr Kegel.* Demzufolge ist die d-semiloop eine gemeinsame Verallgemeinerung dieser beiden Strukturen. Sei fortan eine d-semiloop $\mathfrak{G}$ fest gewählt. Dann gelten:

(11.7)
$$\begin{array}{rcl} a & \leq & b \\ & \Longrightarrow & \\ ax \leq bx & \& & ya \leq yb \\ & \Longrightarrow & \\ a & \leq & b\,. \end{array}$$

DENN: Offenbar können wir uns auf die linksseitigen Fälle beschränken. Diese folgen aber vermöge $a \leq b \Longrightarrow ya \wedge yb = y(a \wedge b) = ya$ für die Links-Rechts-Richtung und vermöge $ya = ya \wedge yb \Longrightarrow ya = y(a \wedge b) \Longrightarrow a = a \wedge b$ für die Rückrichtung. □

(11.8)
$$\begin{array}{rcl} b \geq 1 & \& & a''(a \wedge c) = a \\ & \Longrightarrow & \\ a \wedge bc & = & (a'' \wedge b)(a \wedge c)\,. \end{array}$$

DENN: $b \geq 1 \Longrightarrow a \wedge bc = a''(a \wedge c) \wedge ba \wedge bc = (a'' \wedge b)(a \wedge c)$. □

Aus (11.8) resultiert fast unmittelbar für geeignete $x_b \leq b$, $x_c \leq c$

(11.9)
$$\begin{array}{rcl} x \leq bc & \& & b \geq 1 \\ & \Longrightarrow & \\ x & = & x_b \cdot x_c \end{array}$$

(11.10)
$$\begin{array}{rcl} (a \wedge b)a' & = & a \\ & \Longrightarrow & \\ ba' & = & \sup\,(a, b) := a \vee b\,. \end{array}$$

BEWEIS. Sei $(a \wedge b)a' = a$. Dann folgt $a' \geq 1$ und damit $ba' \geq a$ & $ba' \geq b$. Auf der anderen Seite erfüllt jedes c mit $c \geq a, b$ für ein geeignetes x die Implikation: $c = bx$ & $a = (a \wedge b)(a' \wedge x) \Longrightarrow a' = x \wedge a' \Longrightarrow a' \leq x \Longrightarrow ba' \leq bx = c$.

Ganz ähnlich zeigt man, dass $(a \vee b)a' = a$ & $(a \vee b)b' = b$ zu $ab' = a \wedge b$ führt. Dies wird gewährleistet durch (DSL 5). $\square$

$$x(a \vee b) \cdot y \;=\; xa \cdot y \vee xb \cdot y \tag{11.11}$$

DENN: Sei $xa \vee xb = (xa)c$. Dann existiert nach (DSL 5) ein Element u mit $xu = xa \vee xb$, woraus $u \geq a \vee b$ resultiert und demzufolge $x(a \vee b) = xa \vee xb$. Der Rest ergibt sich dual. $\square$

$$\begin{array}{rcl} (a \wedge b)a' = a & \& & (a \wedge b)b' = b \\ & \Longrightarrow & \\ (a \wedge b)a' \cdot b & = & ab' \\ & = & a \vee b \\ & = & (a \wedge b)(a' \vee b')\,. \end{array} \tag{11.12}$$

$$b \wedge c = 1 \;\mathsf{V}\; b \vee c = 1 \;\Longrightarrow\; ab.c = ac.b\,. \tag{11.13}$$

DENN: Es gilt $b \wedge c = 1 \Longrightarrow ab \wedge ac = a$ und $b \vee c = 1 \Longrightarrow ab \vee ac = a$, weshalb wir in diesem Falle dual schließen können – man pole um! $\square$

$$a \wedge b = 1 \;\Longrightarrow\; ab = a \vee b = ba\,. \tag{11.14}$$

$$\begin{array}{rcl} ab & = & cd \\ & \Longrightarrow & \\ ab = (a \wedge b)(b \vee d) & = & (a \vee c)(b \wedge d)\,. \end{array} \tag{11.15}$$

DENN:

$$\begin{array}{rcl} ab & = & cd \\ & \Longrightarrow & \\ ab \geq (a \wedge c)b \vee (a \wedge c)d & = & (a \wedge c)(b \vee d) \\ & \& & \\ ab \leq a(b \vee d) \wedge c(b \vee d) & = & (a \wedge c)(b \vee d). \end{array}$$ $\square$

$$a = (1 \wedge a)(1 \vee a) \;=\; (1 \vee a)(1 \wedge a)\,. \tag{11.16}$$

11. 2. 2 Definition. Unter dem *positiven Anteil von a* verstehen wir das Element $1 \vee a =: a^+$, unter seinem *negativen* Anteil das Element $1 \wedge a =: a^-$. Weiter bezeichnen wir mit a^* das Element x mit $a^- x = 1$, und wir definieren dual das Element $a^{\cdot}$, das also $a^{\cdot} a^- = 1$ erfüllt.

Schließlich verstehen wir unter dem *Kegel* die Menge aller a^+, also die Menge aller a mit $a \geq 1$.

Im Blick auf (11.2.2) erhalten wir fast unmittelbar nach (11.16):

(11.17)
$$\begin{aligned} a \leq b &\iff 1 \wedge a \leq 1 \wedge b \ \&\ 1 \vee a \leq 1 \vee b \\ &\iff a^* \geq b^* \ \&\ a^+ \leq b^+ . \end{aligned}$$

und damit

11. 2. 3 Proposition. *In einer d-semiloop charakterisiert der Kegel die Ordnung.*

Wie wir als nächstes sehen werden, interagieren die oben ausgezeichneten Elemente über diverse „Koppelungen", die jetzt vorgestellt werden sollen.

(11.18)
$$ab = ab^+ \cdot b^- \ = \ ab^- \cdot b^+$$

DENN: Man schreibe $ab = a1 \cdot b = ab \cdot 1$ und beachte (11.15) □

(11.19)
$$a^+ \wedge a^* \ = \ 1 \ ,$$

DENN: (11.18) liefert $a^+ = aa^*$ & $aa^* \wedge a^* = (a \wedge 1)a^* = 1$. □

(11.20)
$$c \leq 1 \ \&\ b \wedge c^* = 1 \implies a \cdot bc = ab \cdot c = ac \cdot b \ .$$

DENN: Es gilt $b \wedge c^* = 1 \Longrightarrow 1 \wedge cb = (1 \wedge c)(c^* \wedge b) = 1 \wedge c$ nach dem Rechts-Dual zu (11.8). Folglich dürfen wir bei negativem c ausgehen von $c = (cb)^-$ und damit von $cb = c(1 \vee cb)$, also $b = (cb)^+$, was dann nach (11.18) zu $a \cdot bc = ab \cdot c = ac \cdot b$, also unserer Behauptung führt. □

Als nächstes haben wir

(11.21)
$$\begin{aligned} u \wedge a^* = 1 &\implies a^- u \wedge 1 = a^- \\ &\implies 1 \vee a^- u = u \\ &\implies u \wedge a^* = 1 , \end{aligned}$$

und hieraus folgt fast unmittelbar:

(11.22)
$$\begin{array}{ccc} y \leq 1 \leq x & \& & x \wedge y^* = 1 \ \&\ xy = a \\ & \Longrightarrow & \\ x = a^+ & \& & y = a^- \ . \end{array}$$

Als nächstes erhalten wir

$$\begin{aligned} &(ab)^+ &=& \ (1 \vee a^+b^-)(1 \vee a^-b^+) \\ \& \quad &(ab)^- &=& \ (1 \wedge a^+b^-)(1 \wedge a^-b^+)\,. \end{aligned} \tag{11.23}$$

BEWEIS. Unter Berücksichtigung von (11.20) folgt zunächst

$$\begin{aligned} ab &= a^+a^- \cdot b^+b^- \\ &= (a^+ \cdot a^-b^+)b^- \\ &= (a^+(1 \vee a^-b^+)) \\ &\cdot\ ((1 \wedge a^-b^+)b^-) \\ &= ((1 \wedge a^-b^+) \cdot a^+b^-) \\ &\cdot\ (1 \vee a^-b^+) \end{aligned}$$

und damit weiter

$$ab = ((1 \wedge a^-b^+) \cdot (1 \wedge a^+b^-)) \cdot ((1 \vee a^+b^-) \cdot (1 \vee a^-b^+)\,. \tag{11.24}$$

Es gilt nun

$$(1 \vee a^+b^-) \wedge (1 \wedge a^-b^+)^* = 1 = (1 \vee a^+b^-)) \wedge (1 \wedge a^+b^-)^*\,, \tag{11.25}$$

und es genügt nach (11.22) zu zeigen, dass

$$1 \vee a^+b^- \ \perp\ (\,((1 \wedge a^-b^+) \cdot (1 \wedge a^+b^-)\,)^*$$

erfüllt ist. Dies folgt aber nach (11.21) vermöge

$$\begin{aligned} u \wedge a^+ = \quad 1 \quad &= u \wedge b^* \\ &\Longrightarrow \\ 1 \vee b^-u = \quad u \quad &= 1 \vee a^-u \\ &\Longrightarrow \\ b^- \vee b^- \cdot a^-u \quad &= \quad b^-u \\ &\Longrightarrow \\ 1 \vee b^- \vee b^-a^- \cdot u \quad &= \quad 1 \vee b^-u = u \\ &\Longrightarrow \\ u \wedge (a^-b^-)^* \quad &= \quad 1 \end{aligned}$$

Damit sind wir am Ziel. □

Schließlich erhalten wir

$$a \wedge b^{:} = 1 \Longleftrightarrow a \wedge b^* = 1\,. \tag{11.26}$$

DENN: $a \wedge b^{\cdot} = 1 \Longrightarrow ab^- \wedge 1 = b^- \Longrightarrow a(b^- b^*) \wedge b^* = 1 \Longrightarrow a \wedge b^* = 1$. $\Box$

Hiernach führen wir zwei Zusatz-Operationen ein.

11. 2. 4 Definition. x heiße *Rechtskomplement von* a *in* b, symbolisiert mittels $a * b$, wenn $(a \wedge b)x = b$ erfüllt ist.. Dual definieren wir das *Linkskomplement* $b : a$ *von* a *in* b.

Wegen $(a \wedge b)(a * b \wedge b * a) = a \wedge b$ resultiert fast definitionsgemäß

$$a * b \wedge b * a = 1 , \tag{11.27}$$

und es resultieren weiter:

$$\begin{array}{rrcl} & a \wedge b & = & a/(b * a) = (b : a)\backslash b \\ \& & a \vee b & = & a(a * b) = (a : b)b \end{array} \tag{11.28}$$

$$\begin{array}{rcl} a \leq b & \Longrightarrow & x * a \leq x * b \\ & \& & a * x \geq b * x . \end{array} \tag{11.29}$$

Darüber hinaus gelten

$$a * (b \vee c) = a * b \vee a * c \tag{11.30}$$

DENN: $a(a * b \vee a * c) = a(a * b) \vee a(a * c) = a \vee b \vee a \vee c = a \vee (b \vee c)$. $\Box$

$$(a \wedge b) * c = a * c \vee b * c \tag{11.31}$$

DENN: $(a \wedge b) * c \geq a * c \vee b * c \;\&\; (a \wedge b)(a * c \vee b * c) \geq (a \wedge b) \vee c$. $\Box$

$$a * (b \wedge c) = a * b \wedge a * c \tag{11.32}$$

DENN:

$$\begin{array}{rcl} a * (b \wedge c) & \leq & a * b \wedge a * c \\ & \& & \\ (a \wedge b \wedge c)(a * b \wedge a * c) & \leq & (a \wedge b)(a * b) \wedge (a \wedge c)(a * c) \\ & = & b \wedge c \\ & \rightsquigarrow & \\ a * b \wedge a * c & \leq & a * (b \wedge c) \end{array}$$

$\Box$

(11.33) $$(a \vee b) * c = a * c \wedge b * c$$

DENN:
$$\begin{array}{rcl} (a \vee b) * c & \leq & a * c \wedge b * c \\ & \& & \\ (a \vee b)(a * c \wedge b * c) & \leq & a(a * c) \vee b(b * c) \\ & = & a \vee b \vee c \\ & \rightsquigarrow & \\ a * c \wedge b * c & \leq & (a \vee b) * c\,. \end{array}$$
□

Der Leser sollte beachten, dass (11.30) bis (11.33) gültig bleiben, wenn wir $*$ ersetzen durch $\backslash$ und : durch /, vorausgesetzt die eingehenden Operationsergebnisse existieren.
Anwendung von Lemma (11.32) liefert uns hiernach:

11. 2. 5 Proposition. $(G, \wedge, \vee)$ *ist distributiv.*

BEWEIS. Es ist $a \vee (b \wedge c) = a(a * (b \wedge c)) = a(a * b) \wedge a(a * c) = (a \vee b) \wedge (a \vee c)$ erfüllt, (auch gilt bei Anwendung von (11.33) alternativ: $a \wedge (b \vee c) = a/((b \vee c) * a) = a/(b * a) \vee a/(c * a) = (a \wedge b) \vee (a \wedge c)$). □

Hiernach ergeben sich fast *per definitionem*

(11.34)
$$\begin{array}{rrcl} & (a \wedge b)^+ & = & a^+ \wedge b^+ \\ \& & (a \wedge b)^- & = & a^- \wedge b^- \\ \& & (a \vee b)^+ & = & a^+ \vee b^+ \\ \& & (a \vee b)^- & = & a^- \vee b^- \end{array}$$

Schließlich sei zur Ergänzung[1)] erwähnt:

11. 2. 6 Lemma. *Ist $\mathfrak{L}$ eine <u>kommutative</u> d-semiloop, so gelten die Gleichungen:*

(11.35) $$(a \wedge b)(a \vee b) = ab$$

(11.36) $$(a \wedge b)^2 = a^2 \wedge b^2$$

(11.37) $$(a \vee b)^2 = a^2 \vee b^2$$

[1)] Hinweis: Das Lemma 11.2.6 wurde in [35] nicht formuliert

DENN: (11.35) ergibt sich *via* :

$$\begin{aligned} (a \wedge b)(a \vee b) &= (a \wedge b)a \vee (a \wedge b)b \\ &\leq ab \\ &\leq a(a \vee b) \wedge b(a \vee b) \\ &= (a \wedge b)(a \vee b) \end{aligned}$$

(11.36) ergibt sich *via* :

$$\begin{aligned} ab \wedge (a^2 \wedge b^2) &= (ab \wedge a^2)ab \wedge b^2 \\ &= a(b \wedge a) \wedge b(b \wedge a) \\ &= (a \vee b)(a \wedge b) \\ &= ab \\ &\rightsquigarrow \\ (a \wedge b)^2 &= a^2 \wedge ab \wedge b^2 \\ &= a^2 \wedge b^2 \,. \end{aligned}$$

Und (11.37) ergibt sich dual zu (11.36). $\square$

Im Rest dieses Paragraphen betrachten wir spezielle Sachverhalte mit Blick auf spätere Paragraphen.

11. 2. 7 Definition. Wir sagen *a bedecke* b, wenn $a > b$ erfüllt ist und kein Element von G *streng zwischen* a und b liegt. Bedeckt p das Element 1, so heißt p ein *Atom.*

11. 2. 8 Lemma. *Jedes Atom ist* prim, *d. h. jedes Atom erfüllt die Implikation* $p \leq a^+b^+ \Longrightarrow p \leq a^+ \vee p \leq b^+$.

DENN: $p \leq a^+b^+ \;\&\; p \not\leq b^+ \Longrightarrow p \leq (p \wedge a^+)(p \wedge b^+) = p \wedge a^+$. $\square$

11. 2. 9 Lemma. *Jedes Atom* p *erfüllt* $ap \cdot p^n = a \cdot pp^n$ *, wenn man als Standardklammerung die Klammerung von links vereinbart.*

DENN: $ap \cdot p^n = a \cdot qp^n \;\&\; p \neq q$ impliziert $ap \cdot p^n = aq \cdot p^n$, wegen (11.13), man beachte $ap.p^n$ bedeckt ap^n, weshalb q ein Atom ist. $\square$

11. 2. 10 Korollar. *Die natürlichen* Potenzen *eines jeden Atoms* p *bilden eine Unterhalbgruppe.*

DENN: Dies folgt nach 11.2.9 *via* Induktion. □

11. 2. 11 Lemma. *Jedes Atom erfüllt* $px = 1 \Longleftrightarrow xp = 1$.

DENN: Wir führen den Beweis für $\Longrightarrow$: Zunächst gilt 1 bedeckt x, und wir haben darüber hinaus $x \leq 1 \leq p$ & $x \leq xp \leq p$. Folglich können wir schließen:

$$\begin{array}{ll} & 1 \wedge xp = 1 \quad \Longrightarrow \quad xp = 1 \text{ wegen } xp < p \\ \bigvee & 1 \wedge xp = x \quad \Longrightarrow \quad 1 \vee xp = p \Longrightarrow xp = px = 1\,. \end{array}$$

Damit sind wir am Ziel. □

Endlich wenden wir uns Regeln zu, die vor allem im Abschnitt über *vollständige d-semiloops* von Bedeutung sein werden.

11. 2. 12 Lemma. *Existieren die Rechts-Inversen* a^r *und* b^r, *so existieren auch die Rechts-Inversen zu* $a \wedge b$ *und* $a \vee b$, *und es gelten die Formeln*

$$(a \wedge b)^r = a^r \vee b^r \quad \textit{und} \quad (a \vee b)^r = a^r \wedge b^r\,.$$

DENN: $aa^r = 1 = bb^r \Longrightarrow (a \wedge b)(a^r \vee b^r) = 1 = (a \vee b)(a^r \wedge b^r)$. □

Weiter benötigen wir einige Implikationen für *orthogonale Paare,* d. h. Paare a, b mit $a \wedge b = 1$, i. Z. $a \perp b$. Hier erhalten wir

11. 2. 13 Lemma. *Ist* $\mathfrak{G}$ positiv, *d. h., erfüllen alle* a *die Bedingung* $a \geq 1$, *so gilt:*

$$\begin{array}{rcl} a \perp b & \Longrightarrow & a * bc = b(a * c) \\ & \& & cb : a = (c : a)b \end{array}$$

DENN:

$$\begin{array}{rcll} a \perp b & \Longrightarrow & (a \wedge bc)(b(a * c)) & \\ & = & (a \wedge c)(b(a * c)) & (11.8) \\ & = & b \cdot (a \wedge c)(a * c) & \\ & = & bc\,. & (11.13) \end{array}$$

Der Rest folgt dual. □

11. 2. 14 Lemma. *Ist* $\mathfrak{G}$ *positiv, so gilt die Implikation*

$$\begin{array}{rcl} a \perp c & \Longrightarrow & ab * c = b * c = ba * c \\ & \& & c : ab = c : b = c : ba\,. \end{array}$$

DENN: $a \perp c$ impliziert nach (11.8) $(ab \wedge c)x = c \Longrightarrow (b \wedge c)x = c$.

Der Rest folgt dual. □

11. 2. 15 Lemma. *Ist $\mathfrak{G}$ positiv, so gilt die Implikation*

$$a \perp b \implies xa * xb = b \quad \& \quad bx : ax = b\,.$$

DENN: $a \perp b$ impliziert $(xa \wedge xb)y = xb \Longrightarrow x(a \wedge b) \cdot y = xb \Longrightarrow y = b$. Der Rest folgt dual. □

11. 2. 16 Lemma. *Ist $\mathfrak{G}$ positiv und assoziativ, also eine kürzbare komplementäre Halbgruppe, so gelten die schon oben bewiesenen Regeln:*

(i) $$ab * c = b * (a * c)$$

(ii) $$a * (b : c) = (a * b) : c$$

(iii) $$a * bc = (a * b)((b * a) * c)\,.$$

Wir kommen nun zu (bedingt) vollständigen d-semiloops. Analog zum endlichen Fall erhalten wir hier:

11. 2. 17 Lemma. *Ist $\mathfrak{G}$ vollständig, so erfüllt $\mathfrak{G}$:*

$$\begin{array}{llrcl}
 & (i) & x(\bigvee a_i)y = \bigvee(xa_iy) & \& & x(\bigwedge a_i)y = \bigwedge(xa_iy), \\
\textit{und dual} & (ii) & x\backslash(\bigvee a_i) = \bigvee(x\backslash a_i) & \& & x\backslash(\bigwedge a_i) = \bigwedge(x\backslash a_i) \\
\textit{sowie} & (iii) & (\bigvee a_i)\backslash x = \bigwedge(a_i\backslash x) & \& & (\bigwedge a_i)\backslash x = \bigvee(a_i\backslash x) \\
\textit{und dual} & (iv) & a \wedge \bigvee b_i = \bigvee(a \wedge b_i) & \& & a \vee \bigwedge b_i = \bigwedge(a \vee b_i).
\end{array}$$

BEWEIS. Der Beweis darf dem Leser überlassen bleiben, da er analog verläuft wie für endliche Suprema bzw. Infima. □

Schließlich sei bemerkt:

11. 2. 18 Lemma. *$\mathfrak{G}$ ist schon dann vollständig, wenn der* Positivbereich *von $\mathfrak{G}$ vollständig ist. Genauer : $s \leq a_i \Longrightarrow \bigwedge(1 \vee a_i) \cdot bigwedge(1 \wedge a_i) = \bigwedge a_i$.*

DENN: Dies folgt aus der Äquivalenz

$$x \leq a_i \implies 1 \vee x \leq 1 \vee a_i \quad \& \quad (1 \wedge x)^* \geq (1 \wedge a_i)^*\,,$$

man betrachte *nach unten beschränkte* Mengen $\{a_i \,\big|\, (i \in I)\}$. □

11.3 Der Verbandsloop-Kegel

Die Struktur einer Verbandsgruppe ist bis auf Isomorphie vollständig festgelegt durch ihren Kegel. So stellt sich die Frage, ob das Gleiche gilt für Verbandsloops. Die Antwort ist nach 11.2.12 evidenterweise positiv für den zugrunde liegenden Verband. Aber es wurde schon in der Einleitung gezeigt, dass nicht isomorphe Verbandsloops sehr wohl isomorphe Kegel haben können. Daher reduziert sich die Frage auf das Problem, ob es möglich ist, jene d-semiloops zu charakterisieren, die eine Verbandsloop-Erweiterung zulassen. Zu diesem Zweck wählen wir in diesem Abschnitt $\mathfrak{C}$ durchgehend als eine positive d-semiloop.

11. 3. 1 Definition. Mit L sei die Menge aller *orthogonalen positiven Paare* $[\,a\,|\,b\,]$ bezeichnet. Weiter bezeichne $\mathfrak{L}$ die Struktur $(L, \circ, \wedge)$, deren Operationen definiert seien vermöge:

$$\begin{aligned} [\,a\,|\,b\,]\circ[\,c\,|\,d\,] &:= [\,(a:d)(b*c)\,|\,(d:a)(c*b)\,] \\ \text{und}\quad [\,a\,|\,b\,]\cap[\,c\,|\,d\,] &:= [\,a\wedge c\,|\,b\vee d\,]\,. \end{aligned}$$

Offenbar ist $\circ$ rechts-links-dual erklärt. Das bedeutet: Ein Satz und sein Beweis bleiben richtig, wenn wir $[x\,|\,y]$ durch $[y\,|\,x]$ sowie $a*b$ durch $b:a$ und $c:d$ durch $d*c$ ersetzen. Weiterhin ist $\circ$ nach (11.8) eine Funktion, also auch eine Operation. Hiernach erhalten wir sukzessive:

(11.41) $$a\perp b\ \&\ c\perp d\ \Longrightarrow\ (a\wedge c)\perp(b\vee d)\,,$$

DENN: $(a\wedge c)\wedge(b\vee d)=(a\wedge c\wedge b)\vee(a\wedge c\wedge d)\,.$ □

Nach (11.41) ist $(L,\wedge)$ also ein Halbverband.

(11.42) $$\begin{aligned} [\,a\,|\,b\,]\le[\,c\,|\,d\,]\ \Longrightarrow\ & [\,a\,|\,b\,]\circ[\,x\,|\,y\,]\le[\,c\,|\,d\,]\circ[\,x\,|\,y\,] \\ \& \ \ & [\,x\,|\,y\,]\circ[\,a\,|\,b\,]\le[\,x\,|\,y\,]\circ[\,a\,|\,b\,]. \end{aligned}$$

DENN: Dies folgt unmittelbar aus (11.29). □

(11.43) $$\begin{aligned} [\,a\,|\,b\,]\circ[\,c\,|\,d\,] &= \Big([\,a\,|\,b\,]\circ[\,c\,|\,1\,]\Big)\circ[\,1\,|\,d\,] \\ &= [\,a\,|\,1\,]\circ\Big([\,1\,|\,b\,]\circ[\,c\,|\,d\,]\Big)\,. \end{aligned}$$

DENN: Dies folgt aus Dualitätsgründen vermöge

$$\begin{aligned}
& [\,(a:d)(b*c)\,\big|\,(d:a)(c*b)\,] \\
=\ & [\,a(b*c):d\,\big|\,(d:a)(c*b)\,] && (11.2.13) \\
=\ & [\,a(b*c):d\,\big|\,(d:a(b*c))(c*b)\,] && (11.2.14) \\
=\ & [\,a(b*c)\,\big|\,c*b\,]\circ[\,1\,\big|\,d\,] \\
=\ & \Big(\,[\,(a\,\big|\,b\,]\circ[\,c\,\big|\,1)\,]\Big)\circ[\,1\,\big|\,d\,]\,.
\end{aligned}$$

□

(11.44)
$$\begin{aligned}
[\,(a\,\big|\,b\,] &= \Big(\,[\,a\,\big|\,b\,]\circ[1\,\big|\,x\,]\Big)\circ[\,x\,\big|\,1\,] \\
&= [\,1\,\big|\,x\,]\circ\Big(\,[\,x\,\big|\,1\,]\circ[\,a\,\big|\,b\,]\Big)\,.
\end{aligned}$$

DENN: Dies folgt aus Dualitätsgründen vermöge

$$\begin{aligned}
& [\,(a:x)\,\big|\,(x:a)b\,]\circ[\,x\,\big|\,1\,] \\
=\ & [\,(a:x)((x:a)b*x)\,\big|\,x*(x:a)b\,] \\
=\ & (\,[\,(a:x)((x:a)b*(x:a)(a\wedge x)) \\
& \big|\,(x:a)(a\wedge x)*(x:a)b\,] \\
=\ & [\,(a:x)(x\wedge a)\,\big|\,b\,] \\
=\ & [\,a\,\big|\,b\,]\,. && (11.2.15)
\end{aligned}$$

□

(11.45)
$$\begin{aligned}
[\,a\,\big|\,b\,] &= (\,[\,a\,\big|\,b\,]\circ[\,x\,\big|\,1\,]\,)\circ(1\,\big|\,x) \\
&= [\,x\,\big|\,1\,]\circ(\,[\,1\,\big|\,x\,]\circ[\,a\,\big|\,b\,]\,)\,.
\end{aligned}$$

DENN: Dies folgt aus Dualitätsgründen *via*

$$\begin{aligned}
& [\,a(b*x)\,\big|\,(x*b)\,]\circ[\,1\,\big|\,x\,] \\
=\ & [\,a(b*x):x\,\big|\,(x:a(b*x))(x*b)\,] \\
=\ & [\,a(b*x):(b\wedge x)(b*x) \\
& \big|\,((x:(b*x)):a)(x*b)\,] \\
=\ & [\,a\,\big|\,(x\wedge b)(x*b)\,] && (11.2.15) \\
=\ & [\,a\,\big|\,b\,]\,.
\end{aligned}$$

□

(11.46)
$$\begin{aligned}
[\,a\,\big|\,b\,] &= (\,[\,a\,\big|\,b\,]\circ[\,x\,\big|\,y\,]\,)\circ[\,y\,\big|\,x\,] \\
&= [\,x\,\big|\,y\,]\circ(\,[\,y\,\big|\,x\,]\circ[\,a\,\big|\,b\,]\,.
\end{aligned}$$

DENN: Dies folgt aus Dualitätsgründen *via*

$$\begin{aligned}
& \Big([\,a\,|\,b\,] \circ [\,x\,|\,y\,] \Big) \circ [\,y\,|\,x\,] \\
= \ & \Big((\,(\,[\,a\,|\,b\,] \circ [\,x\,|\,1\,]\,) \circ [\,1\,|\,y\,]\,) \circ [\,y\,|\,1\,] \Big) \circ [\,1\,|\,x\,] \\
= \ & \Big([\,a\,|\,b\,] \circ [\,x\,|\,1\,] \Big) \circ [\,1\,|\,x\,] \\
= \ & [\,a\,|\,b\,]\,.
\end{aligned}$$

□

11. 3. 2 Lemma. *Das System der Forderungsgleichungen*

$$\text{(G)} \qquad \begin{aligned} [\,c\,|\,d\,] &\doteq [\,a\,|\,b\,] \circ [\,x\,|\,y\,] \\ [\,c\,|\,d\,] &\doteq [\,u\,|\,v\,] \circ [\,a\,|\,b\,] \end{aligned}$$

hat eindeutig bestimmte Lösungen.

DENN: Nach (11.46) ist

$$[\,x\,|\,y\,] = [\,b\,|\,a\,] \circ [\,c\,|\,d\,]$$

im ersten und

$$[\,u\,|\,v\,] = [\,c\,|\,d\,] \circ [\,b\,|\,a\,]$$

im zweiten Fall die einzige Lösung. □

$$\text{(11.48)} \qquad \begin{aligned} [\,a\,|\,b\,] &= [\,1\,|\,1\,] \circ [\,a\,|\,b\,] \\ &= [\,a\,|\,b\,] \circ [\,1\,|\,1\,]\,. \end{aligned}$$

DENN: $[\,a:1\,|\,1*b\,] \;=\; [\,a\,|\,b\,] = [\,1*a\,|\,b:1\,]\,.$ □

$$\text{(11.49)} \qquad \begin{aligned} [\,ab\,|\,1\,] &= [\,a\,|\,1\,] \circ [\,b\,|\,1\,] \\ &\ \ \& \\ [\,a \wedge b\,|\,1\,] &= [\,a\,|\,1\,] \cap [\,b\,|\,1\,]\,. \end{aligned}$$

DENN: dies ist offenbar. □

Damit haben wir bislang bewiesen:

11. 3. 3 Proposition. *Ein partial geordnetes Gruppoid ist Verbandsloop-Kegel genau dann, wenn es eine positive d-semiloop ist.*

11. 3. 4 Definition. Als *invers* bezeichnet man Loops mit der *Inverseneigenschaft,* englisch: *inverse property,* das sind Loops mit

$$\forall\, a\ \exists\, a^{-1}\ : a^{-1}(ab) = b = (ba)a^{-1}\,.$$

Inverse Loops erfüllen offenbar $aa^{-1} = 1 = a^{-1}a$ und weiterhin können wir schließen $(xy)^{-1} = y^{-1}x^{-1}$, wegen $(xy)y^{-1} = x \Longrightarrow y^{-1} = (xy)^{-1}x \Longrightarrow y^{-1}x^{-1} = (xy)^{-1}$.
Im allgemeinen sind Loops bei weitem nicht invers. Es lässt sich aber verblüffenderweise zeigen:

11. 3. 5 Proposition. *Zu jedem Verbandsloop-Kegel existiert nicht nur eine allgemeine sondern sogar eine inverse Verbandsloop-Erweiterung.*

DENN: Mit $[x \,|\, y]^{-1} := [y \,|\, x]$ folgt die Behauptung aus (11.46). □

Wir betrachten nun die Ausdehnung $\mathfrak{L}$ des Kegels $\mathfrak{C}$. Wir werden zeigen, dass $\mathfrak{L}$ bis auf Isomorphie eindeutig bestimmt ist, sofern wir inverse Verbandsloops betrachten. Weiterhin wollen wir auf das Kongruenz- und Ordnungsverhalten der Ausdehnung eingehen.

11. 3. 6 Proposition. *$\mathfrak{L}$ ist im wesentlichen die einzig mögliche inverse Ausdehnung von $\mathfrak{C}$.*

BEWEIS. Sei $\mathfrak{J}$ eine inverse Verbandsloop-Erweiterung von $\mathfrak{C}$. Dann erhalten wir nach den Regeln der Verbandsloop-Arithmetik:

$$\begin{array}{rrcll} & 1 \vee a^{-1}b & = & a * b & (a(1 \vee a^{-1}b) = a \vee b) \\ & 1 \vee ba^{-1} & = & b : a & \text{(via Dualität)} \\ & 1 \wedge a^{-1}b & = & (1 \vee b^{-1}a)^{-1} = (b * a)^{-1} & \\ \text{und} & 1 \wedge ba^{-1} & = & (a : b)^{-1} & \text{(via Dualität)} \end{array}$$

Weiter sind die beiden Erweiterungen nach 11.2.3 als Ordnungsstrukturen isomorph, sofern sie algebraisch isomorph sind. Deshalb können wir uns auf die multiplikativen Aspekte beschränken. Als erstes halten wir fest:

$$\begin{aligned} ab^{-1} &= (1 \vee ab^{-1})(1 \wedge ab^{-1}) \\ &= (a : b)(b : a)^{-1} \,. \end{aligned} \tag{11.50}$$

In Worten: jedes Element aus G besitzt eine Darstellung $x \cdot y^{-1}$ mit orthogonalen Elementen x, y . Das liefert aber im Falle $\alpha = ab^{-1}$ und $\gamma = cd^{-1}$

mit $a \perp b$ und $c \perp d$:

$$\begin{aligned}
ab^{-1} \cdot cd^{-1} &= (ab^{-1} \cdot c) \cdot d^{-1} \\
&= (a \cdot (b^{-1}c)) \cdot d^{-1} \\
&= (a((1 \vee b^{-1}c) \cdot (1 \wedge b^{-1}c)) \cdot d^{-1} \\
&= a(1 \vee b^{-1}c) \cdot (1 \wedge b^{-1}c)d^{-1} \\
&= a(b * c) \cdot (c * b)^{-1}d^{-1} \\
&= (c * b)^{-1} \cdot (a(b * c) \cdot d^{-1}) \\
&= (c * b)^{-1} \cdot (ad^{-1} \cdot (b * c)) \\
&= (c * b)^{-1} \cdot ((a : d)(d : a)^{-1} \cdot (b * c)) \\
&= (a : d)(b * c) \cdot (c * b)^{-1}(d : a)^{-1} \\
&= (a : d)(b * c) \cdot ((d : a)(c * b))^{-1} .
\end{aligned}$$

Somit sichert die Funktion $[a \mid b] \longmapsto ab^{-1}$ einen Isomorphismus von $\mathfrak{L}$ und $\mathfrak{I}$, wenn der Kegel $\mathfrak{C}$ isomorph ist zum Kegel von $\mathfrak{I}$. □

Hiernach wenden wir uns den elementaren algebraischen Eigenschaften zu.

11. 3. 7 Lemma. *Ist $\mathfrak{C}$ kommutativ, so ist auch $\mathfrak{L}$ kommutativ.*

DENN: Ist $\mathfrak{C}$ kommutativ, so gilt $x : y = y * x$, und dies liefert:

$$\begin{aligned}
[\, a \mid b\,] \circ [\, c \mid d\,] &= [\,((a : d)(b * c) \mid (d : a)(c * b)\,] \\
&= [\,(b * c)(d * a) \mid (c * b)(a * d)\,] \\
&= [\, c \mid d\,] \circ [\, a \mid b\,] .
\end{aligned}$$

□

Eine Loop $\mathfrak{L}$ heißt *monassoziativ*, wenn jedes $a \in L$ eine Unterhalbgruppe von $(L, \cdot)$ erzeugt. Eine Loop heißt *potenz-assoziativ*, wenn jedes $a \in L$ eine Untergruppe von $(L, \cdot, \backslash, /)$ erzeugt.

11. 3. 8 Lemma. *Ist $\mathfrak{C}$ monassoziativ, so ist $\mathfrak{L}$ potenz-assoziativ.*

DENN: Nach (11.8) erhalten wir $[\, a \mid b\,]^n = [\, a^n \mid b^n\,]$ $(n \in \mathbf{N})$ und aufgrund der Inverseneigenschaft $[\, a \mid b\,]^{-n} = ([\, a \mid b\,]^{-1})^n$. □

Analog, aber nicht ganz so unmittelbar, folgt:

11. 3. 9 Lemma. *Ist $\mathfrak{C}$ assoziativ, so ist $\mathfrak{L}$ ebenfalls assoziativ.*

BEWEIS. Wir zeigen

$$\begin{aligned}
\big([\,a\,|\,1\,]\circ[\,c\,|\,d\,]\big)\circ[\,1\,|\,v\,] &= [\,a\,|\,1\,]\circ\big([\,c\,|\,d\,]\circ[\,1\,|\,v\,]\big)\\
\big([\,1\,|\,b\,]\circ[\,c\,|\,d\,]\big)\circ[\,1\,|\,v\,] &= [\,1\,|\,b\,]\circ\big([\,c\,|\,d\,]\circ[\,1\,|\,v\,]\big)\\
\big([(1\,|\,b\,]\circ[\,c\,|\,d\,]\big)\circ[\,u\,|\,1\,] &= [\,1\,|\,b\,]\circ\big([\,c\,|\,d\,]\circ[\,u\,|\,1\,]\big)\ .
\end{aligned}$$

Zeile 3 ist das Duale zu Zeile 1, denn setzen wir $a \cdot b := ba$, so erhalten wir eine duale d-semiloop mit $[a\,|\,b] \cdot [c\,|\,d] = [c\,|\,d] \circ [a\,|\,b]$. Daher folgt Zeile 3 aus der Zeile 1 für die duale Struktur. Folglich bleiben zu verifizieren

$$\begin{aligned}
& [(a:d)c:v\,|\,(v:(a:d)c)(d:a)]\\
= \quad & [(a:(v:c)d)(c:v)\,|\,(v:c)d:a]\\
\text{und} \quad & [(b*c):v\,|\,(v:(b*c))d(c*b)]\\
= \quad & [(b*(c:v)\,|\,(v:c)d((c:v)*b)]\,.
\end{aligned}$$

Es resultiert aber die Zeile 1 aus 11.2.16 und die linken Komponenten der zweiten Zeile sind gleich nach 11.2.16. Bleibt zu zeigen:

$$\begin{aligned}
(v:(b*c))d(c*b) \ &* \ (v:c)d((c:v)*b) = 1\\
(v:(b*c))d(c*b) \ &: \ (v:c)d((c:v)*b) = 1\,.
\end{aligned}$$

Nun ist aber die zweite Gleichung rechts-links-dual zur ersten. Somit genügt es, den ersten Fall zu sichern. Wir erhalten:

$$\begin{aligned}
& (v:(b*c))d(c*b)*(v:c)d((c:v)*b)\\
= \ & d(c*b)*(((v:c)*(v:(b*c)))*d((c:v)*b))\\
= \ & d(c*b)*(((c:v)*(c:(b*c)))*d((c:v)*b)) && (11.2.16, ii)\\
= \ & d(c*b)*d(((c:v)*(c:(b*c)))*((c:v)*b)) && (11.2.13)\\
= \ & (c*b)*(((c\wedge b)*(c:v))*((c\wedge b)*b)) && (11.28, 11.2.16)\\
= \ & (c*b)*(((c\wedge b)*(c:v))*(c*b)) = 1\,.
\end{aligned}$$

Schließlich folgt:

$$\begin{aligned}
& \Big([\,a\,|\,b\,]\circ[\,c\,|\,d\,]\Big)\circ[\,u\,|\,v\,]\\
= \ & \Big(([\,a\,|\,1\,]\circ([\,1\,|\,b\,]\circ[\,c\,|\,d\,]))\circ[\,u\,|\,1\,]\Big)\circ[\,1\,|\,v\,]\\
= \ & \Big([\,a\,|\,1\,]\circ(([\,1\,|\,b\,]\circ[\,c\,|\,d\,]))\circ[\,u\,|\,1\,])\Big)\circ[\,1\,|\,v\,]\\
= \ & [\,a\,|\,1\,]\circ\Big((([\,1\,|\,b\,]\circ[\,c\,|\,d\,]))\circ[\,u\,|\,1\,]))\circ[\,1\,|\,v\,]\Big)\\
= \ & [\,a\,|\,1\,]\circ\Big(([\,1\,|\,b\,]\circ([\,c\,|\,d\,]\circ[\,u\,|\,1\,]))\circ[\,1\,|\,v\,]\Big)\\
= \ & [\,a\,|\,1\,]\circ\Big([\,1\,|\,b\,]\circ(([\,c\,|\,d)\circ[\,u\,|\,1\,])\circ[\,1\,|\,v\,])\Big)\\
= \ & [\,a\,|\,b\,]\circ\Big([\,c\,|\,d\,]\circ[\,u\,|\,v\,]\Big)\,.
\end{aligned}$$

Damit sind wir am Ziel. □

Wir geben noch zwei ordnungstheoretische Ergebnisse:

11. 3. 10 Lemma. *Ist $\mathfrak{C}$ linear geordnet, so ist auch $\mathfrak{L}$ linear geordnet.*

DENN: Es gelten $a \leq b \Longrightarrow [\,a \,|\, b\,] = [\,1 \,|\, b\,]$ und $a \geq b \Longrightarrow [\,a \,|\, b\,] = [\,a \,|\, 1\,]$. Und weiter haben wir $[\,a \,|\, 1\,] \geq [\,1 \,|\, b\,]$ für alle $a, b \in C$. □

11. 3. 11 Lemma. *Ist $\mathfrak{C}$ vollständig, so ist auch $\mathfrak{L}$ vollständig.*

DENN: Man beachte 11.2.18 □

Schließlich betrachten wir Kongruenzen.

11. 3. 12 Proposition. *Die Kongruenzen von $(C, \cdot, *, :)$ setzen sich eindeutig fort nach $\mathfrak{L}$.*

BEWEIS. Sei $\equiv$ eine Kongruenz auf $(C, \cdot, *, :)$. Wir definieren als Ausdehnung $[\,a \,|\, b\,] \equiv [\,c \,|\, d\,] :\Longleftrightarrow a \equiv c \;\&\; b \equiv d$. Dies liefert eine Kongruenz auf $\mathfrak{L}$ wie der Leser leicht bestätigt.
Auf der anderen Seite erhalten wir für jede Ausdehnung ρ von $\equiv$ von $(C, \cdot, *, :)$ nach $\mathfrak{L}$ die Implikation $[\,a \,|\, b\,] \;\rho\; [\,c \,|\, d\,] \Longleftrightarrow ad \equiv bc$, woraus $a \equiv c \;\&\; b \equiv d$ resultiert, man beachte (11.8). □

11.4 Die Kettenbedingung

Offenbar erfüllt eine d-semiloop die absteigende Kettenbedingung für jedes beliebige $[a, b)$, wenn es die aufsteigende Kettenbedingung für jedes beliebige $(c, d]$ erfüllt. Wir können deshalb kurz von Modellen mit Kettenbedingung – C.C. – als Kürzel für chain condition – sprechen.
Sei in diesem Abschnitt $\mathfrak{G}$ eine d-semiloop mit C.C. Dann ist jedes positive Element a ein Produkt von Atomen, da andernfalls unter den nicht zerlegbaren ein minimales existieren würde, mit Widerspruch. Weiter existiert zu jedem $a > 1$ und beliebigem Atom p ein maximales $p(a) \in \mathbf{N}$ unter den $m \in \mathbf{N}$ mit $p^m \leq a$. Schließlich erfüllt jedes Paar verschiedener Atome p, q die Beziehung $p^m \perp q^n$ $(\forall m, n \in \mathbf{N})$, wegen (11.8), und daher auch $p^m \cdot q^n = p^m \vee q^n$. Dies liefert für jedes positive $a \in G$ eine eindeutig bestimmte Primfaktorzerlegung, siehe auch [70].
Ziel dieses Paragraphen ist der Nachweis, dass C.C. Assoziativität und Kommutativität impliziert. Dies ist fast offenbar für C^+, also dual auch für C^-, doch fordert die allgemeine Aussage noch eine Kalkulation.

11. 4. 1 Lemma. *Sei $\overline{q}$ das Rechts-Inverse zu q und seien p, q zwei Atome. Dann kommutiert p^m mit jedem $\overline{q}^n$.*

DENN: Es genügt $p\overline{p} = 1 \Longrightarrow p^m \cdot \overline{p}^m = 1$ zu verifizieren, man beachte (11.20) und 11.2.11. Dies folgt aber durch Induktion, denn 11.2.9 impliziert $p^m p \cdot \overline{p\overline{p}}^m = p^m(p\overline{p} \cdot \overline{p}^m)$. □

11. 4. 2 Lemma. *Erfülle $\mathfrak{G}$ die Kettenbedingung. Dann ist $\mathfrak{G}$ assoziativ und kommutativ.*

BEWEIS. Nach 11.4.1 erhalten wir mittels Distributivität $a^+ \cdot b^- = b^- \cdot a^+$, also $a^+ \cdot b = a^+b^+ \cdot b^- = b^- \cdot b^+a^+ = b \cdot a^+$ und dual $a \cdot b^- = b^- \cdot a$. Somit gelangen wir zu

$$a \cdot b = a^- \cdot a^+b = ba^+ \cdot a^- = b \cdot a\,.$$

Weiterhin haben wir $ab^- \cdot c^- = a \cdot b^-c^-$. Folglich gilt

$$\begin{aligned} ab \cdot c &= (a^+b^+ \cdot a^-b^- \cdot c^-)c^+ \\ &= c^+(a^+b^+ \cdot a^-b^-c^-) \\ &= c^+a^+b^+ \cdot a^-b^-c^- = a \cdot bc\,, \end{aligned}$$

das Letzte wegen der Assoziativität in $\mathfrak{G}^+$. □

Zusammenfassend erhalten wir damit:

11. 4. 3 Proposition. *Eine d-semiloop erfüllt die Kettenbedingung für abgeschlossene Intervalle $[\,a\,,\,b\,]$ genau dann, wenn sie sich als direkte Summe von Kopien der Algebren $(\mathbf{Z}, +, \min)$ und $(\mathbf{N}^0, +, \min)$ auffassen lässt.*

11.5 Vollständige d-semiloops

Wir werden beweisen, dass potenz-assoziative (bedingt) vollständige d-semiloops sogar assoziativ und kommutativ sind. Dies wurde für loops auf der reellen Achse zuerst von ACZÉL [2] gezeigt und für linear geordnete loops im allgemeinen von HARTMAN [90].

11. 5. 1 Definition. $\mathfrak{G}$ heißt *potenz-assoziativ*, wenn jedes a eine Unterhalbgruppe und jedes Paar a^-, a^* eine Untergruppe von $(G, \cdot)$ erzeugt.

11. 5. 2 Definition. In Ausdehnung der Relation $\perp$ werden wir von nun an unter $u \perp x$ die Beziehung $u^+u^* \wedge x^+x^* = 1$ verstehen. Weiter soll *die Polare* $U^\perp$ die Menge aller x bezeichnen, die in diesem Sinne $u \perp x$ für alle $u \in U$ erfüllen.

Man zeigt leicht *via* (11.23) und Lemma 11.2.12, dass $U^\perp$ einen multiplikativ abgeschlossenen Unterverband von $\mathfrak{G}$ bildet.

11. 5. 3 Lemma. *Sei* $\mathfrak{C} := (C^+, \cdot, \wedge, \vee)$ *und sei* $\mathfrak{C}_1 \times \mathfrak{C}_2$ *eine direkte Zerlegung von* $\mathfrak{C}$. *Dann ist* $\mathfrak{C}_1^\perp \times \mathfrak{C}_2^\perp$ *eine direkte Zerlegung von* $\mathfrak{G}$.

BEWEIS. Wir bezeichnen $C_1^\perp$ mit G_2 und $C_2^\perp$ mit G_1. Dann ist jedes Element ein Produkt vom Typ a_1a_2, wobei die Indizes für die Komponenten G_1, G_2 stehen. Um dies einzusehen, betrachten wir a^-. Es gibt eine Zerlegung $a^* = a_1^*a_2^*$ und wir haben $a^-a_1^* \leq 1$ und $a^-a_2^* \leq 1$, also auch Elemente $a_1^{*\ell}$ und $a_2^{*\ell}$ mit $(a_1^{*\ell} \cdot a_2^{*\ell}) \cdot (a_1^* \cdot a_2^*) = 1$. Folglich ist $a_1^{*\ell}a_2^{*\ell}$ gleich a^-, und es gehören nach Definition $a_1^{*\ell}$ bzw. $a_2^{*\ell}$ zu G_1 bzw. G_2. Dies liefert dann weiter

$$\begin{aligned} a^+a^- = a_1^+a_2^+ \cdot a_1^{*\ell}a_2^{*\ell} &= a_1^+(a_2^+ \cdot a_1^{*\ell}a_2^{*\ell}) \\ &= a_1^+(a_1^{*\ell} \cdot a_2^+a_2^{*\ell}) = a_1^+a_1^{*\ell} \cdot a_2^+a_2^{*\ell} \end{aligned}$$

aufgrund von (11.20), (11.26), (11.8). Des weiteren erhalten wir bei Anwendung von (11.20), (11.8)

$$\begin{aligned} a_1a_2 = b_1b_2 &\Longrightarrow a_1^+a_2^+ \cdot a_1^-a_2^- = b_1^+b_2^+ \cdot b_1^-b_2^- \\ &\Longrightarrow a_1^+a_2^+ = b_1^+b_2^+ \& a_1^-a_2^- = b_1^-b_2^- \\ &\Longrightarrow a_1^+ = b_1^+ \ldots a_2^- = b_2^-\,, \end{aligned}$$

wegen $a_1^-a_2^- \cdot a_1^*a_2^* = 1$. Somit gilt $a_1^+a_2^+ \perp (a_1^-a_2^-)^*$.

Folglich können wir G als kartesisches Produkt von G_1 und G_2 betrachten. Wir zeigen nun, dass die Operationen $\cdot$ und $\wedge$ punktweise festgelegt sind. Zu diesem Zweck sei zunächst an $a_1a_2 = a_1^+a_2^+ \cdot a_1^-a_2^-$ erinnert, was unter Hinweis auf (11.20) schon oben erwähnt wurde. Dies impliziert dann geradeaus

$$\begin{aligned} a.b_1b_2 &= (a \cdot b_1^+b_2^+) \cdot b_1^-b_2^- \\ &= (a \cdot b_2^+b_1^+) \cdot b_2^-b_1^- \\ &= (ab_1^+ \cdot b_2^+)b_1^- \cdot b_2^- \quad (11.13) \\ &= (ab_1^+ \cdot b_1^-)b_2^+ \cdot b_2^- \\ &= ab_1 \cdot b_2 \\ &= ab_2 \cdot b_1\,, \end{aligned}$$

und damit:

$$a_1a_2 \cdot b_1b_2 = (a_1a_2 \cdot b_1)b_2 \;=\; (a_1b_1 \cdot a_2)b_2 = a_1b_1 \cdot a_2b_2 \,.$$

Man beachte als nächstes

$$a_1^+a_2^+ = a_1^+ \vee a_2^+ \quad \text{und} \quad a_1^-a_2^- = a_1^- \wedge a_2^- \qquad (11.14)$$

und erinnere sich an $(a \wedge b)^+ = a^+ \wedge b^+$ und $(a \wedge b)^- = a^- \wedge b^-$. Dann folgt:

$$\begin{aligned} a_1a_2 \wedge b_1b_2 &= (a_1^+a_2^+ \wedge b_1^+b_2^+) \cdot (a_1^-a_2^- \wedge b_1^-b_2^-) \\ &= (a_1^+ \wedge b_1^+)(a_2^+ \wedge b_2^+) \cdot (a_1^- \wedge b_1^-)(a_2^- \wedge b_2^-) \\ &= (a_1^+ \wedge b_1^+)(a_1^- \wedge b_1^-) \cdot (a_2^+ \wedge b_2^+)(a_2^- \wedge b_2^-) \\ &= (a_1 \wedge b_1) \cdot (a_2 \wedge b_2) \,. \end{aligned}$$

Damit sind wir am Ziel □

11. 5. 4 Lemma. *Sei $\mathfrak{G}$ vollständig und gelte $a \not\leq b$ & $b \not\leq a$. Dann gibt es eine direkte Zerlegung $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2$ mit $\overline{a}_1 \leq \overline{b}_1$ & $\overline{a}_2 \leq \overline{b}_2$.*

BEWEIS. Nach Lemma 11.5.2 genügt es, die Behauptung für positive d-semiloops zu verifizieren. In diesem Falle definieren wir $C_1 := (a * b)^{\perp}$ und $C_2 := C_1^{\perp}$. Dann sind C_1 und C_2 1-disjunkt und jedes c hat eine Zerlegung c_1c_2 mit $c_1 \perp c_2$ und $c_1 = \sup(x)$ $(x \leq c \;\&\; x \in C_1)$ [2)], man beachte: $y \in C_1 \Longrightarrow c_1 \cdot (c_2 \wedge y) = c_1 \cdot 1 \Longrightarrow c_2 \wedge y = 1$. Weiterhin ist diese Zerlegung eindeutig und die Operationen dürfen stellenweise ausgeführt werden – wegen $a \wedge b = 1 \Longrightarrow a \cdot b = a \vee b$. □

Nun sind wir in der Lage zu zeigen:

11. 5. 5 Proposition. *Eine potenz-assoziative vollständige d-semiloop $\mathfrak{L}$ ist assoziativ und kommutativ. Hingegen muss eine monassoziative d-semiloop $\mathfrak{G}$ weder assoziativ noch kommutativ sein, selbst dann nicht, wenn $\mathfrak{G}$ linear geordnet ist.*

BEWEIS. Wir werden die Behauptung beweisen, indem wir eine Serie von Modellen konstruieren und auf diesem Wege die Situation immer weiter einengen, bis endlich $ab \cdot c \neq a \cdot bc$ zu einem Widerspruch führt.
Nach Lemma 11.5.3 können wir ausgehen von einem Modell $\mathfrak{G}_1$ mit $ab \cdot c < a \cdot bc$ für ein Tripel a, b, c. Weiterhin dürfen wir nach demselben Lemma

[2)] Diese Idee scheint zurückzugehen auf Riesz [137]. Siehe auch Birkhoff [10].

annehmen, dass a, b and c *streng positiv* oder *streng negativ* sind und dass $\{a, b, c\}$ linear geordnet ist.

Wir betrachten $1 < t \leq d := ab \cdot c * a \cdot bc$ und ein $x > 1$. Es gibt ein $n \in \mathbf{N}$ derart, dass $t^n \leq x \,\&\, t^{n+1} \not\leq x$ erfüllt ist, da andernfalls $\mathrm{Sup}(t^n) := \Omega$ existieren und $\Omega \cdot t = \Omega$ erfüllen würde, mit Widerspruch. Folglich würde in jedem Fall ein Modell $\overline{\mathfrak{G}}_1$ existieren mit $\overline{t}^n \leq \overline{x} < \overline{t}^{n+1}$, das $\overline{a}\overline{b} \cdot \overline{c} < \overline{a} \cdot \overline{b}\overline{c}$ erfüllt, wegen $\overline{1} < \overline{x} * \overline{t}^{n+1} \leq \overline{a}\overline{b} \cdot \overline{c} * \overline{a} \cdot \overline{b}\overline{c}$.

Also dürfen wir ausgehen von einem Modell $\mathfrak{G}_2$, das ein Tripel u, v, w enthält mit $uv \cdot w < u \cdot vw$ und $1 < s \leq uv \cdot w * u \cdot vw$, derart dass $\{s^n \,|\, n \in \mathbf{Z} \cup \{u, v, w\}$ linear geordnet ist, denn man wende die obige Einschachtelungsmethode sukzessive an auf $a \vee a^*$, $b \vee b^*$, $c \vee c^*$. Keins dieser Elemente ist gleich 1 und ist beispielsweise a streng negativ, so ist $\overline{r} := \overline{t} \wedge \overline{a}^*$ wegen der Potenzassoziativität nach (DSL 5) invertierbar, weshalb wir unser Verfahren fortsetzen können mit diesem $\overline{r}$, das $\overline{1} < \overline{r} \leq \overline{d}$ erfüllt.

Damit haben wir in $\mathfrak{G}_2$ etwa $1 < s \leq uv \cdot w * u \cdot vw < s^3$. Somit genügt es, für ein geeignetes Tripel x, y, z die Beziehung $1 < g^4 \leq xy \cdot z * x \cdot yz$ in irgendeinem Modell $\mathfrak{H}$ nachzuweisen.

Zu diesem Zweck gehen wir o. B. d. A. aus von $s^n < u \vee u^* =: \tilde{u} < s^{n+1}$. Dies führt zu $1 < u * s^{n+1} =: f < s$ und weiter zu $f(f * s) = s$, weshalb sich mindestens einer der drei Fälle $1 < f^2 \leq s$ oder $1 < (f \wedge (f * s))^2 \leq s$ oder $f^2 \not\leq s \,\&\, f \perp f * s$ einstellt.

Offenbar gibt es in den beiden ersten Fällen dann auch ein f_1 in G_2, das der Abschätzung $1 < f_1^2 \leq s$ in $\mathfrak{G}_2$ genügt. Wir zeigen nun, dass auch der dritte Fall ein Modell des gewünschten Typs sichert, was sich wie folgt ergibt:

$f \perp f * s$ impliziert $s \not\leq f^2$, da $f(f * s) \leq ff$ zu $1 < f * s < f$ führen würde. Also haben wir $f^2 \not\leq s \not\leq f^2$ und damit eine direkte Zerlegung $\mathfrak{G}_2 = \overline{\mathfrak{G}}_2 \times \overline{\overline{\mathfrak{G}}}_2$ mit $\overline{f}^2 \geq \overline{s}$ in $\overline{\mathfrak{G}}_2$ und $\overline{\overline{f}}^2 \leq \overline{\overline{s}}$ in $\overline{\overline{\mathfrak{G}}}_2$.

Wir nehmen nun an, es sei $\overline{\overline{f}}$ gleich $\overline{\overline{1}}$. Dann ist $\overline{f}$ verschieden von $\overline{1}$ und deshalb $\overline{\mathfrak{G}}_2$ ein Modell mit $\overline{f} * \overline{s} = \overline{f} * \overline{s} \wedge \overline{f}^2 = \overline{1}$, woraus $\overline{f} = \overline{s}$ und damit $\overline{\tilde{u}} = \overline{s}^n$ resultiert.

Somit gelangen wir bei Fortsetzung der Methode mit $\overline{v}$ oder $\overline{w}$ in der Rolle von u (s. o.) in jedem Fall zu einem direkten Faktor $\mathfrak{G}'$ von $\mathfrak{G}$ mit $1' < f'^2 \leq s' \leq u'v' \cdot w' * u' \cdot v'w'$.

Daher erhalten wir, ausgehend von der neuen Situation mit f' in der Rolle

von s tatsächlich am Ende ein Modell $\mathfrak{H}$ mit einem Tripel x, y, z, das der Abschätzung $1 < g^4 \leq xy \cdot z * x \cdot yz$ genügt, ein Widerspruch!
Somit ist $\mathfrak{G}$ assoziativ, und man verifiziert analog, dass $\mathfrak{G}$ auch kommutativ ist.
Wir zeigen nun, dass linear geordnete vollständige Loops existieren, die weder assoziativ noch kommutativ sind. Zu diesem Zweck betrachten wir die reelle Achse.

(i) Wir definieren $a \circ b := a + b$ außer wenn $a \leq 0 \leq b$ erfüllt ist. In diesem Falle setzen wir $a \circ b := a + b/2$, wenn $a + b/2 \leq 0$ erfüllt ist, und $a \circ b := 2a + b$ sonst.
Dies liefert eine monassoziative linear geordnete Loop, die weder assoziativ noch kommutativ ist, denn man beachte:

$$((-1) \circ 2) \circ (-1) = -1 \;\neq\; -1/2 = (-1) \circ (2 \circ (-1)) \,.$$

(ii) Wir definieren $a \circ b := a + b$, außer im Falle $a, b \leq 0$, in dem wir $a \circ b := a - ab + b$ festsetzen, vgl. [90].
Dies liefert eine linear geordnete vollständige kommutative monassoziative Loop, die aber nicht assoziativ ist, denn man beachte:

$$(1 \circ (-1)) \circ (-1) = -1 \;\neq\; -2 = 1 \circ ((-1) \circ (-1)) \,. \qquad \square$$

11.6 Vervollständigung

Das Ziel dieses Abschnittes ist eine Charakterisierung derjenigen d-semiloops, die eine Vervollständigung zulassen.
Hierzu betrachten wir nach unten abgeschlossene Teilmengen A. Sie müssen offensichtlich den nachfolgenden Gesetzen genügen:

(i) $\quad x, y \,\big|_\ell\, A \;\&\; x\backslash A \downarrow y\backslash A \implies x = y$

(ii) $\quad x, y \,\big|_r\, A \;\&\; A/x \downarrow A/y \implies x = y$

(iii) $\quad A \,\big|_\ell\, x, y \;\&\; A\backslash x \uparrow A\backslash y \implies x = y$

(iv) $\quad A \,\big|_r\, x, y \;\&\; x/A \uparrow y/A \implies x = y$

worin $\Big|_\ell$ und $\Big|_r$ für *teilt links* bzw. *teilt rechts* steht und $\downarrow$ bzw. $\uparrow$ für *koinitial* bzw. *kofinal*.

Um ein Beispiel zu geben: Es folgt etwa (i) vermöge

$$a\backslash A \downarrow y\backslash A \Longrightarrow x\backslash \bigwedge A = \bigwedge(x\backslash A) = \bigwedge(y\backslash A) = y\backslash \bigwedge A\,.$$

Es ist also eine Charakterisierung gewonnen, sobald wir zeigen können, dass (i) bis (iv) eine solche Erweiterung garantieren.
Im weiteren bezeichne (A) die Menge aller oberen Schranken von A und dual $[A]$ die Menge aller unteren Schranken von A.
Weiterhin stehe p für ein *Multiplikations-Polynom* in einer *Variablen,* d. h. für ein Polynom des Typs $\ldots a_4((a_2(xa_1))a_3)$, man beachte, dass $\mathfrak{G}$ eine 1 besitzt. Demzufolge wird $p(A)$ dann die Menge aller $p(a)$ $(a \in A)$ bezeichnen.
Als eine Folgerung aus (DSL 5) notieren wir, dass $p^{-1}(v)$ genau dann existiert, wenn es ein a gibt mit $v \geq p(a)$. Man beachte, dass sich die einzelnen Komponenten sukzessive von v abspalten lassen.

11. 6. 1 Definition. Eine Teilmenge A von G heiße ein *u-Ideal*, wenn A alle Elemente c enthält, die der Bedingung $v \geq p(A) \Longrightarrow v \geq p(c)$ genügen.
Es ist leicht zu zeigen, dass u-Ideale *Verbandsideale* sind, und der Leser bestätigt ebenfalls leicht, dass G ein u-Ideal ist und dass der Durchschnitt aller u-Ideale, die $A \neq \emptyset$ enthalten, wieder ein u-Ideal ist. Hieraus folgt, dass es jeweils ein engstes $A \neq \emptyset$ umfassendes u-Ideal $\overline{A}$ gibt, und dass darüber hinaus die Definition $\overline{A} \cdot \overline{B} = \overline{AB}$ eine eindeutig bestimmte Multiplikation liefert wegen

$$\overline{A} = \overline{C} \;\&\; \overline{B} = \overline{D} \;\Longrightarrow\; v \geq p(AB) \Leftrightarrow v \geq p(CD)\,.$$

Alternativ werden wir das Ideal $\overline{A}$ im weiteren auch durch $\mathcal{A}$ symbolisieren.
Sei nun X die Menge der Elemente x, für die $\mathcal{A}x \subseteq \mathcal{B}$ nicht leer ist. Dann ist $X =: \mathcal{A} * \mathcal{B}$ ein u-Ideal, was aus der Implikation

$$\begin{array}{rcl} v \geq p(X) & \Rightarrow & v \geq p(c) \\ & \Longrightarrow & \\ w \geq q(\mathcal{B}) \Rightarrow w & \geq & q(AX) \Rightarrow w \geq q(Ac) \\ & \Longrightarrow & \\ Ac & \subseteq & B \end{array}$$

resultiert, die ihrerseits impliziert:

$$\overline{A} \;=:\; \mathcal{A} = [(A)]\,. \tag{11.55}$$

DENN: Offenbar ist $\mathcal{A}$ enthalten in $[(A)]$. Weiterhin erfüllt jedes $c \in [(A)]$ die Implikation:

$$v \geq p(A) \Longrightarrow p^{-1}(v) \geq A \implies p^{-1}(v) \geq c \Longrightarrow v \geq p(c)\,.$$

Deshalb ist auch jedes c aus $[(A)]$ in $\mathcal{A}$ enthalten. □

11. 6. 2 Lemma. a $:= \overline{a}$ *ist gleich der Menge aller* x *unterhalb von* a. *Daher ist* $\mathfrak{G}$ *im Blick auf* $\cdot$ *und* $\supseteq$ *eingebettet in die Struktur der u-Ideale.*

BEWEIS. Geradeaus. □

Sei von nun an bis zum Ende dieses Abschnitts $\mathfrak{G}$ stets eine d-semiloop, die den Bedingungen (i) bis (iv) genügt. Dann folgt:

(11.56) $$\mathcal{A} \cdot \mathcal{X} \subseteq b \implies \mathcal{A} \cdot (\mathcal{A} * b) = b\,.$$

BEWEIS. Zunächst existiert aufgrund unserer Voraussetzung $\mathcal{A} * b$. Sei hiermit nun $\mathcal{A} \cdot (\mathcal{A} * b) \leq c \leq b$. Dann existiert ein v mit $A \cdot v \leq c \leq b$, weshalb auch ein u mit $\mathcal{A} \leq u \;\&\; us = b$ existiert. Für ein jedes solche u erhalten wir aber

$$us = b \Longrightarrow \mathcal{A}s \leq b \Longrightarrow \mathcal{A}s \leq c \Longrightarrow \mathcal{A} \leq c/s = u_c \Big|_{\ell} b\,.$$

Somit finden wir zu jedem $u \geq A$ ein $u_c \geq A$ mit $us = b \Longrightarrow u_c s = c$. Das aber bedeutet, dass die Menge U aller u mit $\mathcal{A} \leq u \;\&\; u \Big|_{\ell} b$ die Beziehung $U \backslash b \uparrow U \backslash c$ erfüllt, woraus dann $c = b$ aufgrund von (iii) resultiert. □

(11.57) $$\mathcal{A} \subseteq \mathcal{B} \implies \mathcal{A} \cdot (\mathcal{A} * \mathcal{B}) = \mathcal{B}\,.$$

BEWEIS. Wir betrachten ein beliebiges $b \in \mathcal{B}$. Dann erfüllt das u-Ideal $\mathcal{A}_b$, das erzeugt wird von allen $a \wedge b \;\; (a \in A)$, die Gleichung

(11.58) $$\mathcal{A}_b \cdot \mathcal{X}_b = b \;\text{ mit }\; \mathcal{X}_b = \mathcal{A}_b * b\,.$$

Wir studieren nun das u-Ideal $\mathcal{X}$, das erzeugt wird von allen $\mathcal{X}_b$. Dann gilt offenbar $\mathcal{A} \cdot \mathcal{X} \supseteq \mathcal{B}$ und wir können darüber hinaus für jedes Paar $a, x \;\; (a \in A, x \in X_b)$ schließen:

$$\begin{aligned} (a \wedge b)x \leq b &\implies x \leq a * b \\ &\implies ax \leq a(a * b) = a \vee b \in \mathcal{B}\,, \end{aligned}$$

weshalb auch $\mathcal{A} \cdot \mathcal{X} \subseteq \mathcal{B}$ erfüllt ist. $\square$

$$\text{(11.59)} \qquad \mathrm{a} \cdot \mathcal{X} \subseteq \mathcal{B} \implies \exists \mathcal{Z} : \mathrm{a} \cdot \mathcal{Z} = \mathcal{B}\,.$$

BEWEIS. Nach (11.57) existiert ein u-Ideal $\mathcal{Y}$ mit $(\mathrm{a} \cdot \mathcal{X}) \cdot \mathcal{Y} = \mathcal{B}$, und es existiert wegen $ax \vee ay = (ax)(1 \vee y) \in \mathcal{B}$ zu jedem Paar x, y $(x \in \mathcal{X}, y \in \mathcal{Y})$ ein Element z mit $(ax)y \leq az = b \in \mathcal{B}$. Daher erfüllt das von diesen z erzeugte u-Ideal $\mathcal{Z}$ die Gleichheit $\mathrm{a} \cdot \mathcal{Z} = \mathcal{B}$. $\square$

$$\text{(11.60)} \qquad s \geq A \;\&\; \mathcal{A} \cdot \mathcal{X} \;=\; \mathcal{A} \cdot \mathcal{Y} \Longrightarrow \mathcal{X} = \mathcal{Y}\,.$$

BEWEIS. Sei $v \geq \mathcal{X}$. Dann folgt $\mathcal{A} \cdot v \geq \mathcal{A} \cdot y$ $(\forall y \in \mathcal{Y})$ und damit

$$\mathcal{A} \cdot \overline{(v \vee y)} \;=\; \mathcal{A} \cdot \mathrm{v} =: \mathcal{B}\,. \quad (11.55)$$

Das aber erzwingt $(\mathcal{B})/v = (\mathcal{B})/(y \vee v)$, so dass wir nach (ii) $v = y \vee v$ erhalten. Es folgt $v \geq \mathcal{Y}$ und damit $\mathcal{X} \supseteq \mathcal{Y}$, also aus Gründen der Dualität sogar $\mathcal{X} = \mathcal{Y}$. $\square$

$$\text{(11.61)} \qquad \mathrm{a} \cdot \bigwedge \mathcal{X}_i \;=\; \bigwedge (\mathrm{a} \cdot \mathcal{X}_i)\,.$$

BEWEIS. Zunächst existiert aufgrund der Implikation (11.59) ein u-Ideal $\mathcal{Z}$, mit $\mathrm{a} \cdot \mathcal{Z} = \bigwedge(a \cdot \mathcal{X}_i)$ $(i \in I)$. Weiter gilt nach (11.55) die Gleichung $\overline{\{a \vee b \,|\, a \in \mathcal{A}, b \in \mathcal{B}\}} = \overline{\{\mathcal{A}, \mathcal{B}\}}$. Folglich gilt für alle nach oben beschränkten u-Ideale $\mathcal{A}$ die Implikation: $\mathcal{A} \cdot \mathcal{X} \subseteq \mathcal{A} \cdot \mathcal{Y} \Longrightarrow \mathcal{X} \subseteq \mathcal{Y}$. Somit ist $\mathcal{Z}$ enthalten in jedem $\mathcal{X}_i$. Das liefert unsere Behauptung. $\square$

Wir erinnern erneut an unsere Praxis, mit einer Aussage stets auch die zu ihr duale Aussage als bewiesen zu erachten, was logisch natürlich keiner Begründung bedarf.
Bislang waren wir mit u-Idealen befasst. Dual zum u-Ideal entsteht das v-Ideal formal dadurch, dass wir (in 11.6.1) $\leq$ umpolen zu $\geq$. Die Beweise jedoch, die wir bislang gegeben haben, übertragen sich nicht ohne weiteres in jedem Falle, da die von uns betrachtete Struktur nicht $\geq / \leq$-dual ist. Dennoch wird der Leser leicht verifizieren, dass der Weg bis hin zu inklusive 11.6.1 geradeaus dualisiert werden kann. Auf diese Weise gewinnen wir mit $\underline{X}$ als Symbol für das von X erzeugte v-Ideal dann ein Produkt $\underline{A} \circ \underline{B} = \underline{AB}$ und einen *Rechts-Quotienten* $\underline{A} * \underline{B} := \{x \,|\, Ax \subseteq \underline{B}\}$ (bzw. einen *Links-Quotienten* $\underline{B} : \underline{A} := \{x \,|\, xA \subseteq \underline{B}\}$).

Wir kehren zurück zur u-Idealerweiterung von $\mathfrak{G}$. Wir wollen zeigen, dass (DSL 5) erfüllt ist. Zu diesem Zweck notieren wir *Haupt-u-Ideale* a auch mit a und u-Ideale im allgemeinen mit kleinen griechischen Buchstaben. Weiterhin werden wir die Menge $\{v \,|\, v \in G \;\&\; v \geq \alpha\}$ mit (α) bezeichnen und dual die Menge $[\alpha]$ erklären.
Auf diese Weise betrachten wir also eine nach oben stetige Schnitterweiterung Σ von $\mathfrak{G}$ mit:

$$\begin{array}{rcl} x\alpha \leq \beta \Longrightarrow \beta = x\kappa & \& & \alpha x \leq \beta \Longrightarrow \beta = \lambda x \\ & \& & \\ a \bigwedge \beta_i & = & \bigwedge (a\beta_i)\,. \end{array}$$

11. 6. 3 Lemma. *Es gibt keine anderen nach unten beschränkten v-Ideale von $\mathfrak{G}$ als die Teilmengen (α) von Σ, was insbesondere $\underline{A} = ([A])$ bedeutet.*

BEWEIS. Sei A nach unten beschränkt und sei $\bigwedge A =: \alpha$. Dann gilt $\underline{A} \subseteq (\alpha)$, da Σ eine Schnitterweiterung ist, und es resultiert $(\alpha) \subseteq \underline{A}$ aus $t \leq p(A) \Longrightarrow t \leq p(\alpha) \overset{(11.61)}{\Longrightarrow} t \leq p(c) \;\; (c \geq \alpha)$. □

$$\underline{A} \supseteq \underline{B} \;\Longrightarrow\; \underline{A}\Big|_{\ell}\underline{B} \;\&\; \underline{A}\Big|_{r}\underline{B}\,. \tag{11.62}$$

BEWEIS. Man betrachte ein festes $b \in B$. Dann ist $\underline{A}$ gleich $\underline{a \wedge b}$. Sei nun X_b die Menge aller x mit $Ax \geq b$ und sei $b \leq c \leq AX_b$. Wir bezeichnen $\mathrm{Inf}(A)$ mit α. Dann folgt $Ax \geq b \Longrightarrow \alpha x \geq b \Longrightarrow \alpha x \geq c$. Im Blick auf unsere vorhergehende Bemerkung gibt es aber Elemente β, γ derart, dass $\alpha\beta = b \;\&\; \alpha\gamma = c$ erfüllt ist, was $x \geq \beta \Longrightarrow \alpha x \geq b \Longrightarrow \alpha x \geq c \Longrightarrow x \geq \gamma$ liefert. Dies führt dann weiter zu $\beta = \gamma$, woraus sich $b = c$ ergibt. Daher erfüllt jedwedes d mit $d \leq AX_b$ die Gleichheit $d \vee b = b$. Folglich erfüllt das von allen X_b erzeugte Ideal $\underline{X}$ die Gleichheit $\underline{A} \circ \underline{X} = \underline{B}$. □

Bis hierher haben wir gezeigt, dass die v-Ideale eine nach unten stetige Erweiterung zu $\mathfrak{G}$ gewährleisten in Bezug auf $\leq \,:=\, \supseteq$. Wir werden nun zeigen, dass Σ und die v-Idealerweiterung isomorph sind. Damit verifizieren wir implizit zusätzlich die Existenz einer vollständigen Erweiterung die zudem Axiom (DSL 5) erfüllt, was aufgrund der Stetigkeit nach unten aus $\mathcal{A} \cdot \mathcal{B} \subseteq \mathcal{C} \Longrightarrow \mathcal{A} \cdot \mathcal{B} \subseteq c \;\; (c \geq \mathcal{C})$ (s. 11.56) resultiert.

$$\bigwedge(\alpha) \circ \bigwedge(\beta) \;=\; \bigwedge(\alpha\beta)\,. \tag{11.63}$$

BEWEIS. Man definiere $\alpha \circ \beta = \gamma$, falls $(\alpha) \circ (\beta) = (\gamma)$. Dann sind $\alpha \circ d$ und αd gleich aufgrund von (11.61). Sei nun $\alpha\beta \leq c$ und $s \leq ab$ für alle $a \in (\alpha), b \in (\beta)$ und $c = \alpha \circ \gamma$. Dann folgt für alle $c_i \geq \gamma$ die Abschätzung $\alpha \circ c_i = \alpha c_i \geq \alpha\beta \Longrightarrow c_i \geq \beta$, weshalb wir nach Voraussetzung $s \leq \alpha \circ c_i$ und damit weiter $s \leq \alpha \circ \gamma = c$ erhalten.
Damit sind wir am Ziel. □

11. 6. 4 Proposition. *$\mathfrak{G}$ besitzt eine Schnitterweiterung, die ihrerseits isomorph ist zu der Struktur der nach unten beschränkten v-Ideale bezüglich $\leq\, := \,\supseteq$, und ebenso zu der Struktur der nach oben beschränkten u-Ideale bezüglich $\leq\, := \,\subseteq$.*

BEWEIS. Nach (11.63) liefert $[(A)] \longmapsto (A)$ einen Homomorphismus, und es ist diese Abbildun *per definitionem* bijektiv. □

Zusammenfassend halten wir fest:

11. 6. 5 Theorem. *Eine d-semiloop besitzt eine vollständige Schnitterweiterung genau dann, wenn sie die Bedingungen (i) bis (iv) erfüllt.*

Sei hiernach $\mathfrak{G}$ erklärt wie oben und Σ die i. w. eindeutig bestimmte Schnitterweiterung. Dann können wir zusätzlich zeigen:

11. 6. 6 Korollar. *Ist $\mathfrak{G}$ potenz-assoziativ, so ist auch Σ potenz-assoziativ.*

BEWEIS. Ist c gleich einem Produkt, gebildet aus Faktoren $a_i \leq \alpha$ $(1 \leq i \leq n)$, das unterhalb eines Produktes aus lauter α's liegt, so gilt $a_1 \vee \ldots \vee a_n \leq \alpha$ und damit $(a_1 \vee \ldots \vee a_n)^n \leq \pi$ für jedes weitere Produkt π aus lauter α's. □

11. 6. 7 Korollar. *Ist $\mathfrak{G}$ eine Verbandsloop, so ist auch Σ eine Verbandsloop. Ist $\mathfrak{G}$ zudem invers, so ist auch Σ invers.*

BEWEIS. Zunächst haben wir $\alpha \leq a \;\&\; b \leq \beta \Longrightarrow \alpha(a\backslash b) \leq \beta$.
Sei nun zusätzlich $\mathfrak{G}$ invers und $\alpha = \bigvee a_i \;\; (i \in I, a_i \in G)$. Dann folgt:

$$(ba_i)a_i^{-1} = b \;\Longrightarrow\; \bigvee ba_i \bigwedge a_i^{-1} = (b\alpha)\alpha^{-1} = b\;,$$

also auch die allgemeine Inversität aufgrund der Stetigkeit nach oben. □

11. 6. 8 Korollar. *Eine Verbandsgruppe besitzt eine vollständige Erweiterung genau dann, wenn sie archimedisch ist.*

BEWEIS. Offenbar ist die aufgestellte Bedingung notwendig. Auf der anderen Seite gilt:
Ist $\mathfrak{G}$ eine Verbandsgruppe, so sind die Bedingungen (i) bis (iv) schon erfüllt, wenn $Ax \downarrow A \Longrightarrow x = 1$ und sein Dual erfüllt sind. Das aber ist eine Konsequenz der Archimedizität wegen

$$\begin{aligned} Ax \downarrow A \geq s \quad &\Longrightarrow \quad Ax^{-n} \downarrow A \downarrow Ax^n \\ &\Longrightarrow \quad x^{-n} \leq s^{-1}a \geq x^n (a \in A, n \in \mathbf{N}) \\ &\Longrightarrow \quad (x^*)^n \leq s^{-1}a \ \&\ (x^+)^n \leq s^{-1}a \ , \end{aligned}$$

man beachte (11.8). Daher ist Σ eine vollständige Verbandsgruppe, da die Assoziativität aus $\underline{A} \circ \underline{B} = AB$ resultiert. □

11.7 Kongruenzen

Im weiteren interessieren wir uns für kürzbare Kongruenzen eines unterliegenden d-semiloops $\mathfrak{G}$. Der Leser erinnere sich in diesem Zusammenhang an das Theorem über direkte Zerlegungen. Das Hauptanliegen wird sein zu klären, unter welchen Bedingungen $\mathfrak{G}$ repräsentierbar ist.

11. 7. 1 Lemma. *Sei U der positive Anteil der 1-Klasse einer kürzbaren Kongruenz $\equiv$ (man beachte, dass kürzbare Kongruenzen zugleich Kongruenzen im Blick auf $*$ und $:$ sind). Dann ist U eine multiplikativ abgeschlossene konvexe Teilmenge mit:*

(ii) $$ab \cdot U \ = \ a \cdot bU$$

(iii) $$U \cdot ab \ = \ Ua \cdot b \, .$$

DENN: $u \in U$ impliziert:

(i) $$a \equiv au = va \ \Longrightarrow \ v \equiv 1$$

(ii) $$ab \equiv ab \cdot u = a \cdot bv \ \Longrightarrow \ bv \equiv b1 \Longrightarrow v \equiv 1$$

(iii) $$ab \equiv a \cdot bu = ab \cdot v \ \Longrightarrow \ \ldots \Longrightarrow v \equiv 1\, ,$$

weshalb (i) bis (iii) erfüllt sind. Der Rest ist dann evident. □

11. 7. 2 Definition. Als *Kern* bezeichnen wir im folgenden jede multiplikativ abgeschlossene konvexe positive Teilmenge aus G die zum einen 1 enthält und zum anderen die Bedingungen (i) bis (iii) erfüllt.

11. 7. 3 Lemma. *Ist U ein Kern, so definiert*

$$x \equiv y\,(U) \;:\Longleftrightarrow x \leq yu \;\&\; y \leq xv \;\; (\exists\, u, v \in U)$$

eine kürzbare Kongruenz derart, dass der positive Anteil der 1*-Klasse zusammenfällt mit U .*

BEWEIS. Geradeaus *per definitionem*. □

Damit gilt als ein erstes Resultat:

11. 7. 4 Proposition. *In jeder d-semiloop $\mathfrak{G}$ werden die kürzbaren Kongruenzen $\equiv$ repräsentiert durch die Kerne U via*

$$\text{(C)} \qquad a \equiv b\,(U) \iff a \leq bu \;\&\; b \leq au\,.$$

DENN: Es gilt $a \equiv b \Longrightarrow a \leq b(a * b \vee b * a) \;\&\; b \leq a(a * b \vee b * a)$ mit $(a * b, b * a \equiv 1)$. □

In [71] geben Evans & Hartman eine Charakterisierung der repräsentierbaren Verbandsloops. Diese Charakterisierung greift auch bei d-semiloops. Zu diesem Zweck betrachten wir zwei orthogonale Elemente a, b. Offenbar erfüllen sie die Äquivalenz

$$\begin{array}{rrcl} & a \wedge (bx \cdot y)/xy & = & 1 \\ \iff & a \cdot xy \wedge bx \cdot y & = & xy \\ \iff & ((a \cdot xy)/y)/x \wedge b & = & 1 \quad \text{(DSL 5)}\,. \end{array}$$

Damit liefert die erste Zeile, dass im Falle $u \perp v$ auch u und $(vx \cdot y)/xy$ orthogonal sind. Und die Gültigkeit der dritten Zeile bedeutet: Sind u, v orthogonal so sind auch u und $((v \cdot xy)/y)/x$ orthogonal.
Das aber bedeutet, dass wir aus jeder dieser Zeilen im Falle $u \wedge v = 1$ und $U = (u^{\perp})^{+}$ herleiten können:

$$\begin{array}{rrcl} & (Ux \cdot y)/xy \subseteq U & \leadsto & Ux \cdot y \subseteq U \cdot xy \\ \& & (((U \cdot xy)/y)/x \subseteq U & \leadsto & U \cdot xy \subseteq Ux \cdot y\,. \end{array}$$

Entsprechend resultiert aus $u \wedge v = 1 \Longrightarrow u \wedge (xv)/x = 1$ die Gleichheit $Ux = xU$.
Hiernach kommen wir zu der angekündigten Charakterisierung.

11. 7. 5 Proposition. *Eine d-semiloop $\mathfrak{G}$ ist genau dann repräsentierbar, wenn sie die Bedingungen erfüllt:*

$$(i) \qquad (a * b) \cdot xy \wedge (b * a)x \cdot y \;=\; xy$$

$$(ii) \qquad xy \cdot (a * b) \wedge x \cdot y(b * a) \;=\; xy$$

$$(iii) \qquad x \cdot (a * b) \wedge (b * a) \cdot x \;=\; x\,.$$

BEWEIS. Wie der Leser leicht sieht, sind die aufgestellten Bedingungen notwendig. Sie sind aber auch hinreichend.
DENN: Offenbar sind a und b orthogonal, wenn $a * b = b$ & $b * a = a$ erfüllt ist. Daher fordern die aufgestellten Bedingungen, dass der positive Anteil eines jeden $U^{\perp}$ einen Kern bildet. Sei nun U maximal in der Menge der Kerne M, die c nicht enthalten. Dann ist $\mathfrak{G}/U =: \overline{\mathfrak{G}}$ linear geordnet, da $\overline{\mathfrak{G}}$ andernfalls ein Paar $\overline{p}, \overline{q}$ mit $\overline{p} * \overline{q} \neq \overline{1} \neq \overline{q} * \overline{p}$ enthalten würde. Dann aber wären $\overline{U}_1 := ((\overline{p} * \overline{q})^{\perp})^{+}$ und $\overline{U}_2 := (U_1^{\perp})^{+}$ zwei Kerne mit $\overline{U}_1 \cap \overline{U}_2 = \{\overline{1}\}$, obwohl $\overline{U}_1$ und $\overline{U}_2$ sich nach Konstruktion von $\{\overline{1}\}$ unterscheiden, ihre Urbilder also beide c enthalten müssten, ein Widerspruch zu $\overline{c} \neq \overline{1}$! □

11.7.5 charakterisiert repräsentierbare d-semiloops auf klassische Weise, und es ist augenscheinlich, dass diese Methode sich außerordentlich stützt auf die Relation der Orthogonalität. Diesen Sachverhalt überwindet

11. 7. 6 Proposition. *Eine d-semiloop $\mathfrak{G}$ ist genau dann repräsentierbar, wenn jedes Paar von Multiplikationspolynomen der Bedingung genügt:*

$$(0) \qquad p(a) \wedge q(b) \;\leq\; p(b) \vee q(a)\,.$$

BEWEIS. Offenbar ist die Bedingung (0) notwendig. Sei hiernach (0) erfüllt. Setzen wir dann für positive Elemente, also Elemente vom Typ c^{+}, zur Abkürzung

$$(c^{+}x \cdot y)/xy \;:=\; c^{+}\,\theta\,,$$

so können wir für orthogonale Elemente a, b schließen:

$$\begin{array}{rcl} a \wedge b\,\theta & \leq & b \vee a\,\theta \\ & \Longrightarrow & \\ a \wedge b\,\theta & = & (a \wedge b\,\theta) \wedge (b \vee a\,\theta) \\ & = & (a \wedge b\,\theta \wedge b) \vee (a \wedge b\,\theta \wedge a\,\theta) \\ & = & (1 \wedge b\,\theta) \vee (a \wedge 1) \\ & = & 1 \wedge (a \vee b\,\theta)\,, \end{array}$$

weshalb (i) erfüllt ist, und es folgen ganz analog die Bedingungen (ii) und (iii). □

Kapitel 12

Repräsentierbarkeit

Eine fundamentale Methode der Verortung algebraischer Strukturen ist die Koordinatisierung. Sie greift bei abstrakten geordneten Strukturen vor allem dann, wenn es genug „Ketten” als Faktoren – einer subdirekten Zerlegung – gibt. Sind diese Ketten sogar *innere direkte Faktoren* so sind sie natürlich maximal und damit konvex bzw. konvex und unbeschränkt. In dieser Lecture Note bietet sich zumindest eine gemeinsame Untersuchung von Residuationsstrukturen an, etwa der normalen komplementären Halbgruppe und der Verbandsloop.
In beiden Fällen haben wir die Grundgegebenheit eines rechts-normalen Verbandsgruppoids. Wie wir schon gesehen haben, geht bei der Untersuchung von Verbandsloops mit der Assoziativität vieles verloren, doch eine enge Verwobenheit mit einer starken Verbandsstruktur vermag andererseits auch manches auszugleichen.
In diesem Kapitel befassen wir uns mit übergreifenden Sätzen, die Gültigkeit über mehrere klassische Strukturen hinweg besitzen. Sie sind ihrerseits anzusehen als Beiträge zur allgemeinen Teilbarkeitstheorie. Betrachten wir zunächst Q^+. Hier gelten die beiden Klassiker:

12. 0. 7 Proposition. $\mathfrak{Q}^+$ ist repräsentierbar, *d. h. zerfällt subdirekt in angeordnete Komponenten*

und

12. 0. 8 Proposition. *Die maximalen konvexen Ketten von* $\mathfrak{Q}^+$ *sind direkte Faktoren von* $\mathfrak{Q}$ *. Man beachte: die maximalen konvexen Ketten sind exakt die Mengen* p^n $(n \in \mathbf{Z})$ *.*

Damit sind aus dem Satz von Euklid zwei Folgerungen gewonnen, die sich allgemein algebraisch formulieren lassen.

12.1 Zur Repräsentierbarkeit

Hatten wir im letzten Abschnitt des letzten Kapitels repräsentierbare *d*-semiloops untersucht, so wenden wir uns in diesem Kapitel ganz allgemein *repräsentierbaren geordneten Strukturen* zu.

Hier gibt es natürlich eine Fülle von Ergebnissen, bezogen auf spezielle verbandsgeordnete Strukturen, das absolut historische Resultat unter ihnen das STONEsche Theorem für *boolesche Algebren*, später ausgedehnt von BIRKHOFF auf *distributive Verbände* [10]. Erwähnt seien etwa die Arbeiten von: LORENZEN [118], CLIFFORD [53], RIBENBOIM [138] über *abelsche Verbands-Gruppen;* LORENZEN [119], ŠIK [142], BANASCHEWSKI [5] über beliebige *Verbands-Gruppen;* von SWAMY [147] über abelsche *residuierte Verbands-Halbgruppen;* BOSBACH [15], [32] über *komplementäre Halbgruppen;* THÉRÈSE MERLIER [123] über *abelsche Verbands-Monoide;* FUCHS [78] über *partial geordnete Algebren;* FUCHS [81] über *positive abelsche Verbands-Monoide;* von BIRKHOFF & PIERCE [11] über *Verbands-Ringe* sowie – *last but not least* – EVANS & HARTMAN [71] über *Verbands-Loops.*

Doch eine allgemeine Lösung stand aus und auch spezielle Probleme waren ungelöst, obwohl sie mehrfach formuliert worden waren, so beispielsweise das Verbandshalbgruppenproblem [79], [81], das Verbandsgruppoid- und das Verbandsquasigruppenproblem [71], bevor in [37] das schon oben im Sonderfall vorgestellte Kriterium (0) formuliert und eingesetzt wurde.

Hinweis: In zwei anderen Lecture Notes – [30], [38] – stellt der Autor Teilbarkeits-Halbgruppen bzw. Ideal-Halbgruppen vor, in denen natürlich das hier besprochene Darstellungsproblem eine zentrale Rolle spielt. Sonderfälle mit Blick auf diese beiden Strukturen sind hier weitgehend übergangen. Sie sind eingebettet in die entsprechenden Theorien.

12.2 Ein allgemeiner Darstellungssatz

Wir starten ganz allgemein.

12. 2. 1 Definition. Sei $\mathfrak{A} := (A, \wedge, \vee, f_i)$ eine Algebra, derart dass $(A, \wedge, \vee)$ einen Verband bildet mit Operationen f_i von der *Stellenzahl* n_i. Dann heiße $\mathfrak{A}$ eine *Verbands-Algebra*, wenn jede *Operation* an jeder *Stelle* isoton ist.

Verteilt sich zudem jedes f_i *über* $\wedge$ und auch *über* $\vee$, so nennen wir $\mathfrak{A}$ eine *verbandsgeordnete Algebra.*

Verbands-Algebra ist demnach etwa das *Verbands-Gruppoid.* Allerdings, die *Verbands-Gruppe, die Verbands-Quasigruppe, die Verbands-Loop* sind natürlich nur dann erfasst, wenn man sie – lediglich – als Verbands-Gruppoid betrachtet, also die *Inversen-Operationen* ignoriert. Auf der anderen Seite erfüllen *Verbands-Quasigruppen*

$$x\backslash(a \wedge b) = x\backslash a \wedge x\backslash b \;\&\; (a \wedge b)/x = a/x \wedge b/x$$

und

$$x\backslash(a \vee b) = x\backslash a \vee x\backslash b \;\&\; (a \vee b)/x = a/x \vee b/x\,.$$

Daher können wir *Verbands-Quasigruppen*, *Verbands-Loops* und *Verbands-Gruppen* auch betrachten als *verbandsgeordnete Algebren*

$$(G\ell_x, r_x, \wedge, \vee)\;\;(x \in G)\text{ mit } \ell_x(a) := x\backslash a \text{ und } r_x(a) := a/x\,,$$

wir unterscheiden also

zwischen

Verbands-Strukturen und verbandsgeordneten Strukturen.

Sprechen wir von einer Verbandsgruppe, so wollen wir eine Gruppe mit Verband mit isotoner Multiplikation meinen, die natürlich bei Homomorphismen und direkten Produktbildungen in eine Gruppenmultiplikation übergeht, nicht aber notwendig beim Übergang zu Unterstrukturen, die ja möglicher weise nur Halbgruppen sind. Hingegen bedeute verbandsgeordnete Gruppe stets eine Struktur $(G, \ell_x, r_x, \wedge, \vee)$ im obigen Sinne. Ganz analog seien die *Verbandsquasigruppe,* der *Verbandsring* etc. erklärt. Verbandsgeordnet schließt also immer ein, dass – erforderlichenfalls – zuvor der Typ in einer solchen Weise abgewandelt wurde, dass sich alle Operationen über $\wedge$ und $\vee$ verteilen.

12. 2. 2 Definition. Sei $\mathfrak{A}$ eine verbandsgeordnete Algebra. Ein *Term* heiße *linear komponiert*, wenn er eine Variable ist oder von dem besonderen Typ

$$f(x_1, \ldots, q(x, y_1, \ldots, y_m), \ldots, x_n)$$

worin f eine fundamentale Operation und $q(x, y_1, \ldots, y_m)$ (schon) linear komponiert ist.

12.2.2 liefert eine Menge von Termen mit einer *Initialvariablen* x derart, dass im Falle der distributiven verbandsgeordneten Algebra die aufkommenden *Polynomfunktionen* $\overline{p}(x)$ des Typs

$$p(x, c_1, \ldots, c_n) \ \ (c_i \in A)$$

die Gesetze $\overline{p}(a \wedge b) = \overline{p}(a) \wedge \overline{p}(b)$ und $\overline{p}(a \vee b) = \overline{p}(a) \vee \overline{p}(b)$ erfüllen. Um zu betonen, dass der Term $\overline{p}(x)$ ohne $\wedge$ und $\vee$ aufgebaut wurde, schreiben wir auch $\tilde{p}(x)$. Hiernach stellen wir vor:

12. 2. 3 Das Darstellungslemma. *Eine verbandsgeordnete Algebra $\mathfrak{A}$ ist repräsentierbar, wenn sie distributiv ist und die Bedingung erfüllt:*

$$(\tilde{0}) \qquad \tilde{p}(a) \wedge \tilde{q}(b) \ \leq \ \tilde{p}(b) \vee \tilde{q}(a)\,.$$

Dies kann vereinheitlicht werden zu

$$(\overline{0}) \qquad \overline{p}(a) \wedge \overline{q}(b) \ \leq \ \overline{p}(b) \vee \overline{q}(a)\ .$$

BEWEIS. Offenbar ist $(\overline{0})$ notwendig und es impliziert $(\overline{0})$ *a fortiori* $(\tilde{0})$. Darüber hinaus erzwingt $(\overline{0})$ die Abschätzung

$$f(..a \wedge a..) \wedge f(..b \wedge b..) \ \leq \ f(..a \wedge b..) \vee f(..b \wedge a..)\,,$$

weshalb f sich über $\wedge$ verteilt. Analog zeigt man, dass sich auch jedes f über $\vee$ verteilt. Der Leser beachte, dass $(\overline{0})$ fast unmittelbar aus $(\tilde{0})$ folgt, wenn $\mathfrak{A}$ distributiv ist. Hinweis: man schreibe $\overline{p}$ und $\overline{q}$ als Durchschnitt von Vereinigungen von q$\sim$ - Funktionen.
Wir zeigen nun, dass Distributivität zusammen mit $(\tilde{0})$ Repräsentierbarkeit gewährleistet. Zu diesem Zweck starten wir von $r < s$ mit dem Ziel, ein linear geordnetes homomorphes $\overline{\mathfrak{A}}$ zu konstruieren, das $\overline{r} < \overline{s}$ erfüllt. Dann lassen sich je zwei Elemente $x \neq y$ trennen, wegen $x \neq y \Longleftrightarrow x \wedge y \neq x \vee y$.
Nach dem ZORNschen Lemma existiert ein maximales Verbandsideal M, unter denjenigen Idealen, die r enthalten, s hingegen nicht. Dieses erfüllt weiter die Implikation

$$(\mathrm{P}) \qquad a \wedge b \in M \implies a \in M \ \mathbf{\vee} \ b \in M\,,$$

da andernfalls wegen der Distributivität die beiden Mengen

$$U := \{u \,|\, a \wedge u \in M\} \text{ und } V := \{v \,|\, v \wedge u \in M \ \ (\forall u \in U)\}$$

Verbandsideale wären, die wegen $a, b \notin M$ beide das Element c enthalten müssten, was dann $c \wedge c = c \in U \cap V$ und damit $c \in M$ implizierte, ein Widerspruch! Wir definieren nun

$$a \equiv b \quad :\Longleftrightarrow \quad \tilde{p}(a) \in M \Leftrightarrow \tilde{p}(b) \in M \quad (\forall\, \tilde{p}) \; .$$

Dies liefert eine Kongruenz schon dann, wenn M nur irgendeine Menge ist, wie man im Gruppoidfall leicht zeigt und was sich im allgemeinen Fall analog herleitet. Weiterhin erhalten wir in $\overline{\mathfrak{A}} := \mathfrak{A}/\equiv$

$$\begin{array}{rcl} \overline{u} & \leq & \overline{v} \\ & \Longleftrightarrow & \\ \tilde{p}(v) \in M & \Rightarrow & \tilde{p}(u) \in M \end{array}$$

wegen

$$\begin{array}{rcl} \overline{u} & \leq & \overline{v} \\ & \Longrightarrow & \\ \overline{u} & = & \overline{u} \wedge \overline{v} \\ & \Longrightarrow & \\ \tilde{p}(v) \in M & \Rightarrow & \tilde{p}(u) \in M \end{array}$$

und

$$\begin{array}{rcl} \tilde{p}(v) \in M & \Rightarrow & \tilde{p}(u) \in M \\ & \Longrightarrow & \\ \tilde{p}(u \wedge v) \in M & \Rightarrow & \tilde{p}(u) \in M \vee \tilde{p}(v) \in M \\ & \Longrightarrow & \\ \tilde{p}(u \wedge v) \in M & \Rightarrow & \tilde{p}(u) \in M \\ & \Longrightarrow & \\ \overline{u} & \leq & \overline{v} \; . \end{array}$$

Somit sind $\overline{a}$ und $\overline{b}$ genau dann unvergleichbar, wenn es linear komponierte Polynomfunktionen $\tilde{p}(x), \tilde{q}(x)$ gibt, die der Bedingung

$$\begin{array}{ccc} \tilde{p}(a) \notin M & \& & \tilde{p}(b) \in M \\ \tilde{q}(a) \in M & \& & \tilde{q}(b) \notin M \end{array}$$

genügen. Doch das ist nicht möglich, wegen $(\tilde{0})$, da wir schließen könnten:

$$\begin{array}{cccl} & \tilde{p}(a) & \wedge & \tilde{q}(b) \notin M \\ \& & \tilde{p}(b) & \vee & \tilde{q}(a) \in M \; , \end{array}$$

mit Widerspruch zu $\tilde{p}(a) \wedge \tilde{q}(b) \leq \tilde{p}(b) \vee \tilde{q}(a)$.

Folglich ist $\mathfrak{A}$ linear geordnet. $\square$

Das Darstellungslemma liefert eine Serie spezieller Resultate, u. a. als allererstes:

12. 2. 4 Ein Satz von Birkhoff. *Jeder distributive Verband zerfällt subdirekt in 2-elementige Ketten, ist also ein Verband von Mengen.*

12. 2. 5 Korollar. *Ein abelsches verbandsgeordnetes Monoid $\mathfrak{M}$ ist genau dann repräsentierbar, wenn es verbandsdistributiv ist und sich die Multiplikation verteilt über Schnitt und Vereinigung.* [123].

BEWEIS. Da $\mathfrak{M}$ ein abelsches Monoid ist, können wir uns beschränken auf den Beweis von $xa \wedge yb \leq xb \vee ya$. Hier gilt aber:

$$\begin{aligned}
(xa \wedge yb) \wedge (xb \vee ya) &= (xa \wedge yb \wedge xb) \vee (xa \wedge yb \wedge ya) \\
&= (xa \wedge (y \wedge x)b) \vee ((x \wedge y)a \wedge yb) \\
&= (xa \wedge (xa \vee yb)) \wedge (x \wedge y)(a \vee b) \wedge yb \\
&= xa \wedge yb\,.
\end{aligned}$$
$\square$

Der Leser beachte, dass es schon genügt, zu je zwei Elementen über eine gemeinsame Einheit zu verfügen.

12. 2. 6 Korollar. *Sei $\mathfrak{S} := (S, \cdot, \wedge, \vee)$ eine verbandsgeordnete Halbgruppe. Dann ist $\mathfrak{S}$ genau dann repräsentierbar, wenn ihr Verband $(S, \wedge, \vee)$ distributiv ist und sich die Multiplikation über Schnitt und Vereinigung verteilt sowie $\mathfrak{S}$ zusätzlich für jedes (x, y, u, v) aus S^1 der Abschätzung genügt:*

$$\text{(S0)} \qquad xay \wedge ubv \ \leq \ xby \vee uav\,.$$

BEWEIS. Die Forderungen garantieren $\tilde{p}(a) \wedge \tilde{q}(b) \leq \tilde{p}(b) \vee \tilde{q}(a)$, wie man ganz leicht sieht. $\square$

12. 2. 7 Korollar. *Eine verbandsgeordnete Loop $(L, \cdot, \wedge, \vee)$ ist repräsentierbar genau dann, wenn $\mathfrak{L}$ den Gleichungen aus* [70] *genügt:*

$$\text{(EH)} \qquad \begin{aligned}
x \cdot (a * b) \wedge (b * a) \cdot x &= x \\
(a * b) \cdot xy \wedge (b * a)x \cdot y &= xy \\
xy \cdot (a * b) \wedge x \cdot y(a * b) &= xy\,.
\end{aligned}$$

BEWEIS. Wir sahen schon oben, dass alle zu fordernden Distributivgesetze erfüllt sind. Weiterhin sehen wir, dass die aufgestellten Bedingungen notwendig sind.

Daher bleibt nur zu zeigen, dass sie auch hinreichen. Dies haben wir schon oben unter 11.7.5 geleistet, aber wir möchten einen direkten Beweis zu (EH) $\Longrightarrow$ $(\tilde{0})$ anbieten. Zu diesem Zweck betrachten wir $\mathfrak{L}$ als verbandsgeordnete Algebra $(L, \cdot, \wedge, \vee, \ell_s, r_s)$ $(s \in L)$. Dann ist zu zeigen, dass die Bedingung

$$\tilde{p}(a) \wedge \tilde{q}(b) \ \leq\ \tilde{p}(b) \vee \tilde{q}(a)$$

erfüllt ist. Dabei dürfen wir nach den Regeln der Arithmetik $\tilde{p}$ als die identische Abbildung annehmen, und wir können weiter den allgemeinen Beweis zu

$$(a:b)u \wedge (b:a)\,\theta \ \leq\ (b:a)u \vee (a:b)\,\theta$$

transformieren, worin θ eine *innere Abbildung,* d. h. eine *via* der definierenden Operationen erzeugte Abbildung, ist. Somit dürfen wir ausgehen von $a \perp b$, $\tilde{p}(x) = x \cdot z$ und $\tilde{q}(y) = y\,\theta$, was zu

$$\begin{array}{rcll} au \wedge b\,\theta & = & x_a x_y & (x_a \leq a \ \&\ x_u \leq u) \\ & \Longrightarrow & & \\ au \wedge b\,\theta & = & (x_a \wedge x_a x_u)(x_u \vee 1) & (11.15) \\ & \leq & 1 \vee u & (a \perp b\,\theta) \\ & \leq & a\,\theta \vee bu & (a\,\theta \perp b) \end{array}$$

führt. Zur Erinnerung: Gilt $a \perp b \Longrightarrow a \perp b\,\theta$ für die erzeugenden inneren Abbildungen θ, so impliziert $a \perp b$ auch $a \perp b\,\theta$ für alle inneren Abbildungen θ). □

Aufgrund des letzten Theorems kann man also ausgehen von (EH) und zeigen, dass sich $\mathfrak{L}$ unter dieser Bedingung subdirekt zerlegen lässt in angeordnete Komponenten, indem man $(\tilde{0})$ herleitet und dann 12.2.3 anwendet. Man hat aber zu beachten, dass der oben gegebene Beweis das *inner mapping theorem* heranzieht, das besagt, dass die Gruppe der inneren Abbildungen erzeugt wird von $((\#.xy)/y)/x$, $xy\backslash(x \cdot y\,\#)$ und $(x \cdot \#)/x$, siehe etwa [46].

Weiter erhalten wir bei Anwendung von 11.5.3 (und 11.2.10) insbesondere:

12. 2. 8 Korollar. *Eine vollständige d-semiloop $(L, \cdot, \leq, 1)$ ist repräsentierbar und erfüllt zusätzlich jedes abgeschlossene Intervall die Kettenbedingung, so ist $(L, \leq, 1)$ direkte Summe von atomischen Ketten, siehe hierzu auch noch einmal 11.4.3.*

Verbandsquasigruppen sind – wie schon erwähnt – keine verbandsgeordneten Algebren im Sinne unserer Definition 12.2.1 Doch wie wir sahen, lassen sich diese Strukturen „umetikettieren” zu verbandsgeordneten Strukturen, indem man *unverträgliche* Operationen *splittet.*
Betrachten wir als Beispiel etwa eine verbandsgeordnete Halbgruppe $\mathfrak{S}$. Indem wir die Multiplikation in Operatoren m_x mit $m_x(a) := xa$ splitten, geht jede Links-Kongruenz von $\mathfrak{S}$ über in eine Kongruenz von $(S, \wedge, \vee, m_x)$ $(x \in S)$, und es lässt sich offenbar auch umgekehrt jede Kongruenz von $(S, \wedge, \vee, m_x)$ $(x \in S)$ auffassen als Links-Kongruenz von $\mathfrak{S}$. Damit erhalten wir für *volldistributive Verbandsmonoide,* d. s. distributive Verbandsmonoide, in denen sich die Multiplikation über $\wedge$ und $\vee$ verteilt:

12. 2. 9 Korollar. *Jedes volldistributive Verbandsmonoid $\mathfrak{S}$ ist ein Verbandsmonoid von Ketten-Endomorphismen* [24].

BEWEIS. Wir betrachten $\mathfrak{S}$ als verbandsgeordnete Algebra $(S, \wedge, \vee, m_x)$. Diese erfüllt $(\tilde{0})$, man kopiere den Beweis von 12.2.5. Daher „gibt es genug” linear geordnete Restklassensysteme, die sich zu einer Kette $\mathcal{C}$ von Links-Klassen von $\mathfrak{S}$ zusammenlegen lassen, auf der die Elemente aus S von links operieren. Auf diese Weise kann $\mathfrak{S}$ eingebettet werden in die Halbgruppe aller *Ordnungsendomorphismen* von $\mathcal{C}$. □

Damit ist insbesondere bewiesen:

12. 2. 10 Holland's celebrated Theorem. *Jede Verbandsgruppe ist eine Gruppe von Ketten-Automorphismen* [95]).

Wir wenden uns nun *Verbandsringen* zu. Ein Ring heißt *partial geordnet* im Blick auf $\leq$, wenn er den Bedingungen genügt:

$$(+) \qquad a \leq b \implies x + a \leq x + b$$

$$(\cdot) \qquad 0 \leq a, b \implies 0 \leq ab$$

Ein partial geordneter Ring heißt ein Verbandsring, wenn $\leq$ eine Verbandsordnung definiert. Offenbar ist die Multiplikation nicht isoton. Auf der anderen Seite ist die Multiplikation vollständig bestimmt, sobald sie auf dem positiven Kegel festgelegt ist. Folglich ist jedes homomorphe Bild schon festgelegt durch das Bild des Kegels. Daher macht es Sinn, den Verbandsring $\mathfrak{R}$ zu betrachten als $(R, +, \wedge, \vee, r_x, \ell_x)$, mit $r_x(a) := ax^+$ und $\ell_x(a) := x^+a$. Auf diese Weise wird $\mathfrak{R}$ zu einer verbandsgeordneten Algebra, doch muss diese Algebra nicht distributiv sein, da ℓ_x und r_x sich nicht verteilen müssen über $\wedge$ und $\vee$, man betrachte etwa den Ring der reellen 2×2-Matrizen bezüglich $A \leq B$ gdw. $a_{ik} \leq b_{ik}$ $(1 \leq i \leq 2, 1 \leq k \leq 2)$. Daher müssen wir nach weiteren Bedingungen schauen, wollen wir Distributivität erzwingen. Hilfe bringt hier der positive Kegel von $\mathfrak{R}$. Um deutlich zu machen, dass wir bezüglich der Residuation die Addition im Blick haben, setzen wir $a - (a \wedge b) := a \div b$.

12. 2. 11 Lemma. *Sei $\mathfrak{R} := (R, +, \wedge, \vee, \ell_x, r_x)$ ein Verbandsring. Dann ist $\mathfrak{R}$ eine distributive verbandsgeordnete Algebra im obigen Sinne genau dann, wenn $\mathfrak{R}$ die Bedingung erfüllt:*

$$\text{(L)} \qquad c^+(a \div b) \wedge c^+(b \div a) = 0\,.$$

BEWEIS. Sei (L) erfüllt und c positiv. Dann gilt:

$$\begin{array}{rcl}
ca \wedge cb & = & c((a \wedge b) + a \div b) \wedge c((a \wedge b) + b \div a) \\
& = & (c(a \wedge b) + c(a \div b)) \wedge (c(a \wedge b) + c(b \div a)) \\
& = & c(a \wedge b) + (c(a \div b) \wedge c(b \div a)) \\
& = & c(a \wedge b) \\
& \rightsquigarrow & \\
ca \vee cb & = & (ca + cb) - (ca \wedge cb) \\
& = & c(a + b) - c(a \wedge b) \\
& = & c((a + b) - (a \wedge b)) \\
& = & c(a \vee b)\,.
\end{array}$$

Damit sind wir i. w. am Ziel. □

Der letzte Satz liefert bei Anwendung von 12.2.3:

12. 2. 12 Korollar. *Ein Verbandsring ist repräsentierbar (ein Funktionenring) genau dann, wenn er die Bedingung* (L) *und* $(\tilde{0})$, *kurz* $(\mathrm{L},\tilde{0})$ *erfüllt.*

Das letzte Korollar charakterisiert den Funktionenring entlang der Linie dieses Abschnitts. Auf andere Weise haben Birkhoff & Pierce in ihrer grundlegenden Arbeit [11] und durch wiederum eine andere Bedingung hat Fuchs in [79] eine Charakterisierung geleistet und auch die Äquivalenz der aufgestellten Bedingungen nachgewiesen. Diesem Äquivalenznachweis fügen wir einen weiteren hinzu, im Blick auf Birkhoff/Pierce

$$\text{(BP)} \qquad a \perp b \Longrightarrow c^+a \perp b \;\&\; ac^+ \perp b \quad (\Longrightarrow c^+a\,d^+ \perp x^+b\,y^+)\,.$$

12. 2. 13 Hinweis. *Es gibt eine kurze direkte Herleitung der Äquivalenz* (BP) $\Longleftrightarrow$ (L,$\tilde{0}$) .

BEWEIS. Wir beschränken uns auf den assoziativen Fall, doch ist dies keineswegs wesentlich, sondern nur angenehm für die Herleitung.
Erfülle $\mathfrak{R}$ also (BP). Dann ist (L) evident. Weiterhin ist leicht zu sehen, dass die Polynome in ($\tilde{0}$) vom Typ $c_1^+ x c_2^+ + s$ sind. Folglich reduziert sich ($\tilde{0}$) nach einigen einfachen Kalkulationen auf

$$(c_1(a \div b)c_2 + u) \wedge d_1(b \div a)d_2 \;\;\leq\;\; (c_1(b \div a)c_2 + u) \vee d_1(a \div b)d_2 \,.$$

mit positiven Elementen c_1, c_2, d_1, d_2.Wegen (BP) dürfen wir aber $c_1(a \div b)c_2$ auf der linken Seite „unterdrücken", also von

$$u \wedge d_1 b^* d_2 \;\;\leq\;\; (c_1 b^* c_2 + u) \vee d_1 a^* d_2$$

mit orthogonalenElementen a^*, b^* ausgehen, denn (11.8) impliziert

$$x \perp y \;\&\; z \geq 0 \Longrightarrow x \wedge (y + z) = x + z.$$

Somit ist wegen $u \wedge d_1 b^* d_2 \leq u + c_1 b^* c_2 + u$ auch ($\tilde{0}$) erfüllt.
Gelte hiernach in $\mathfrak{R}$ die Bedingung (L, $\tilde{0}$). Dann folgt (BP) vermöge:

$$\begin{array}{rcl}
a & \perp & b \\
 & \Longrightarrow & \\
c^+ a \wedge b & \leq & c^+ b \vee a \\
 & \Rightarrow & \\
c^+ a \wedge b & = & (c^+ a \wedge b \wedge c^+ b) \vee (c^+ a \wedge b \wedge a) \\
 & = & (c^+(a \wedge b) \wedge b) \vee (c^+ a \wedge 0) \\
 & = & 0\,.
\end{array}$$

□

Nach den Regeln der Arithmetik kann jede komplementäre Halbgruppe im Blick auf die Operatoren c_x^* und $c_x^{:}$ mit $c_x^*(a) = x * a$ und $c_x^{:}(a) = a : x$ betrachtet werden als eine distributive $\vee$-halbverbandsgeordnete Algebra $(S, \cdot, c_x^*, c_x^{:}, \vee)$. Allerdings: wir haben zu zeigen, dass die Kongruenzen von $(S, \cdot, c_x^*, c_x^{:})$ übereinstimmen mit den Kongruenzen von $(S, \cdot, *, :)$. Dies gelingt über die Formel $a * (b : c) = (a * b) : c$. Denn, ist $\equiv_c$ eine Kongruenz von $(S, \cdot, c_x^*, c_x^{\cdot})$, so erhalten wir

$$\begin{array}{rcl} a \equiv_c b & \Longrightarrow & a * b \equiv_c a * a = 1 \ \& \ 1 = b * b \equiv_c b * a \\ (& \Longleftrightarrow & b : a \equiv_c a : a = 1 \ \& \ 1 = b : b \equiv_c a : b \ ) \\ & \Longrightarrow & a \equiv_c a(a * b) = b(b * a) \equiv_c b \ , \\ & \Downarrow & \\ a \equiv_c b & \Longrightarrow & a * b \equiv_c 1 \\ & \Longrightarrow & (a * c) : (b * c) = a * (c : (b * c)) \equiv_c 1 \ , \end{array}$$

man beachte in der letzten Zeile, dass $\equiv_c$ (auch) Halbverbandskongruenz ist, also $x \leq y \ \& \ y \equiv_c 1$ zu $x \equiv_c 1$ führt.
Somit ergibt sich dual $(b * c) : (a * c) \equiv_c 1$, woraus $a * c \equiv_c b * c$ resultiert. Komplementäre Halbgruppen sind nicht notwendig $\wedge$-abgeschlossen, doch erfüllen subdirekte Produkte von linear geordneten komplementären Halbgruppen zwangsläufig die Gleichung $a * b \perp b * a$, die äquivalent ist zu der Gleichung $a : b \perp b : a$ und auch zu $a : (b * a) \vee b : (a * b) = a \wedge b$, wie wir sahen. Darüber hinaus gelten in diesem Falle die weiteren Distributivgesetze:

$$(\mathrm{D}^{\cdot}\wedge) \qquad x(a \wedge b)y = xay \wedge xby$$

$$(\mathrm{D}^{*}\wedge) \qquad \begin{array}{rcl} a * (b \wedge c) & = & a * b \wedge a * c \\ (a \wedge b) : c & = & a : c \wedge b : c \end{array}$$

$$(\mathrm{D}) \qquad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \ .$$

Infolgedessen mag man repräsentierbare komplementäre Halbgruppen auffassen als distributive verbandsgeordnete Algebren des Typs $(S, \cdot, c_x^*, c_x^{\cdot})$, und wir erhalten unmittelbar:

12. 2. 14 Korollar. *Eine komplementäre Halbgruppe ist repräsentierbar gdw. sie der Implikation genügt:*

$$(0^{\vee}) \qquad x \leq \tilde{p}(a), \tilde{q}(b) \ \Longrightarrow \ x \leq \tilde{p}(b) \vee \tilde{q}(a) \ .$$

DENN: Aus $(0^{\vee})$ folgt die Abgeschlossenheit nach unten vermöge der Implikation $x \leq a * b, b * a \Longrightarrow x \leq a * a \vee b * b = 1$. □

Dies liefert als eine weitere Charakterisierung

12. 2. 15 Korollar. *Eine komplementäre Halbgruppe ist repräsentierbar gdw. sie die Gleichung erfüllt – (vgl.* [15]) *:*

$$(0^{c}) \qquad (c * (b * a)c \vee c(b * a) : c) * x \vee (a * b) * x = x \ .$$

BEWEIS. Gelte zunächst Axiom $(0^\vee)$. Dann folgt fast unmittelbar

$$(0^\perp) \qquad a * b \perp c * (b * a)c\,,\ c(b * a) : c\,,$$

man definiere $\tilde{p}(a) := c * (b * a)c$ und $\tilde{q}(b) := a * b$. Insbesondere haben wir damit auch $a * b \wedge b * a = 1$ und erhalten folglich nach $(\mathrm{N}^*_\vee)$ aus 3.3.17 die Gleichung (0^c).

Gelte hiernach Axiom (0^c). Dann folgt zunächst $a * b \perp b * a$, man setze $c = 1$. Daher ist $(S, \leq)$ $\wedge$-abgeschlossen, und es gilt in jedem Falle

$$(i) \qquad x * yz \leq (x * y)z \quad (\ \&\ zy : x \leq z(y : x))$$

und wegen $(0^c) \rightsquigarrow (0^\perp)$ auch

$$(ii) \qquad ca^\perp \ = \ a^\perp c\,.$$

Schließlich lässt sich jedes $\tilde{p}(a)$ *via* Erweiterung durch Einsen ausdehnen zu

$$\ldots x_5((x_3 * (x_1 a)x_2)) : x_4) \ldots\,.$$

Daher dürfen wir ausgehen von einem Paar $\tilde{p}(a), \tilde{q}(b)$ mit $a \perp b$. Und dies führt bei wiederholter Anwendung von (i) und (ii) zu

$$\begin{array}{rcll}
\tilde{p}(a) \wedge \tilde{q}(b) & \leq & a^*\tilde{p}(1) \wedge b^*\tilde{q}(1) & (a^* \perp b^*) \\
& = & x_a x_p = x_b x_q & (x_a \leq a^*\,,\ x_p \leq \tilde{p}(1) \\
& & & (x_b \leq b^*\,,\ x_q \leq \tilde{q}(1)) \\
& = & (x_a \wedge x_b)(x_p \vee x_q) & (\text{wegen } a^* \perp b^*) \\
& \leq & \tilde{p}(1) \vee \tilde{q}(1) & \\
& \leq & \tilde{p}(b) \vee \tilde{q}(a)\,. &
\end{array}$$

Also folgt auch umgekehrt $(0^\vee)$ aus (0^c). Damit sind wir am Ziel. □

Der Leser beachte noch, dass die Beweismethode gezeigt hat, dass eine Verbandsgruppe schon dann repräsentierbar ist, wenn sie $a^\perp c \subseteq ca^\perp$ erfüllt.

Unmittelbar klar ist nach 12.2.15

12. 2. 16 Korollar. *Eine abelsche komplementärte Halbgruppe ist repräsentierbar genau dann, wenn sie $a * b \perp b * a$ erfüllt.*

Als nächstes wenden wir 12.2.14 an auf boolesche Algebren $(B, \vee, *)$ (mit $a * b := a' \wedge b)$. Dann folgt

12. 2. 17 Satz von Stone. *Jede boolesche Algebra zerfällt subdirekt in 2-elementige Komponenten und ist demzufolge ein Mengenkörper,* (s. [144]).

In ähnlicher Weise lässt sich zeigen, dass *normal residuierte* Verbände, siehe [14], distributive verbandsgeordnete Algebren sind, weshalb 12.2.3 auch in diesen Strukturen greift.
Und weiterhin sieht man leicht, dass dual residuierte Halbgruppen – siehe [147, 148, 149] – als komplementäre Halbgruppen betrachtet werden können, wenn man $a * b := 0 \vee b - a$ hinzunimmt. Somit erhalten wir:

12. 2. 18 Korollar. *Eine dual residuierte* (*kommutative*) *Halbgruppe ist repräsentierbar genau dann, wenn sie der Bedingung* $a - b \wedge b - a \leq 0$ *genügt* (s. [149]).

Endlich kommen wir zur Kegelalgeba $(C, *, :)$. Sie ist zunächst zu partial geordneten Algebren umzuetikettieren vermöge $c^*_x(a) := x * a$ und $c^{:}_x(a) := a : x$, und wir haben zu zeigen, dass diese Umetikettierung *kongruenzinvariant* ist. Sei also $\equiv_c$ eine Kongruenz von $(C, c^*_x, c^{:}_x)$ $(x \in C)$. Dann folgt

$$\begin{array}{rcl}
a \equiv_c b & \Longrightarrow & a * b \equiv_c a * a = 1 \ \&\ 1 = b * b \equiv_c b * a \\
(& \Longleftrightarrow & b : a \equiv_c a : a = 1 \ \&\ 1 = b : b \equiv_c a : b \ \ ) \\
 & \Longrightarrow & a \equiv_c a : (b * a) = b : (a * b) \equiv_c b \,, \\
 & \Downarrow & \\
a \equiv_c b & \Longrightarrow & a * b \equiv_c 1 \\
 & \Longrightarrow & (a * c) : (b * c) = a * (c : (b * c)) \equiv_c 1 \,,
\end{array}$$

also wie oben, dass $\equiv_c$ eine Kongruenz liefert.
Kegelalgebren sind $\wedge$-abgeschlossen, aber eine Kegel-Algebra muss nicht $\vee$-abgeschlossen sein, man betrachte etwa die um 1 erweiterte Menge der *Primzahlen* bezüglich $a * a := 1$ und $a * b := b$ im Falle $a \neq b$. Allerdings: Ist $\{a, b\}$ nach oben beschränkt, so existiert auch $\sup(a, b)$ in C , da jedes $[1, a]$ bezüglich der Ausgangsoperationen $*$ und $:$ einen Brick mit a als *Null* bildet. Folglich können wir die Bedingung (0) umformulieren zu:

$$(0') \qquad \tilde{p}(a) \wedge \tilde{q}(b) = \big((\tilde{p}(a) \wedge \tilde{q}(b)) \wedge \tilde{p}(b)\big) \vee \big((\tilde{p}(a) \wedge \tilde{q}(b)) \wedge \tilde{q}(a)\big)$$

Tatsächlich wird (0) auch hier zum Ziel führen, obwohl wir nicht über Verbandsideale verfügen. Dies ergibt sich zum einen mittels 12.2.18 – man setze $\tilde{p}(x) = x : b$ und $\tilde{q}(y) = a * y$. Doch auch auf dem Wege des Darstellungslemmas gelangen wir zum Ziel. Dies hat wesentlich damit zu tun, dass in den Beweis des Darstellungslemmas die Operation $\vee$ nicht einging und damit, dass wir lediglich „genug" „ideale Mengen" M – welcher Art auch immer – benötigen, die der Bedingung genügen:

$$\text{(C0)} \qquad \tilde{p}(b) \in M \ \&\ \tilde{q}(a) \in M \implies \tilde{p}(a) \in M \ \mathsf{V}\ \tilde{q}(b) \in M\,.$$

Nun hätten wir aber statt mit maximalen c meidenden Verbandsidealen auch mit maximalen c meidenden Filtern arbeiten können, und man sieht sofort, dass das mengentheoretische Komplement dieser Filter jeweils ein Primideal ist.
Dies regt an, in Kegelalgebren mit den Komplementen $\overline{F}$ von maximalen Filtern zu arbeiten. Deren gibt es genug, und es gilt natürlich die Implikation $a \wedge b \in \overline{F} \Longrightarrow a \in \overline{F} \ \mathsf{V}\ b \in \overline{F}$. Daher bleibt nur zu zeigen, dass sie (C0) erfüllen. Lägen nun aber $\tilde{p}(b)$ und $\tilde{q}(a)$ in $\overline{F}$, so lägen auch $\tilde{p}(a)\wedge\tilde{q}(b)\wedge\tilde{p}(b)$ und $\tilde{p}(a)\wedge\tilde{q}(b)\wedge\tilde{q}(a)$ in $\overline{F}$. Daher sind wir am Ziel, wenn wir zeigen können, dass im Falle der Existenz von $x \vee y$ aus $x, y \in \overline{F}$ folgt $x \vee y \in \overline{F}$.
Es sollte F aber maximal sein in der Menge der c meidenden Filter. Das bedeutet dann die Existenz eines $u \in F$ mit $x \wedge u \leq c$ und eines $v \in F$ mit $y \wedge v \leq c$, also mittels $w := u \wedge v$ die Herleitung

$$x \wedge w \leq c \ \&\ y \wedge w \leq c \leadsto (x \vee y) \wedge w \leq c\,.$$

Läge nun $x \vee y$ in F, so läge auch c in F. Also liegt $x \vee y$ nicht in F und somit in $\overline{F}$. Damit haben wir:

12. 2. 19 Korollar. *Eine Kegel-Algebra ist repräsentierbar genau dann, wenn sie die Bedingung* $(0')$ *erfüllt.*

Einen alternativen Beweis für das letzte Korollar liefert uns natürlich der Satz 6.6.1, denn gilt $(0')$, so erst recht $a * b \perp a : b$.

12.3 Ein perspektivischer Hinweis

Wie wir schon im letzten Beweis sahen, wirkt das Prinzip aus 12.2.3 immer dann, wenn eine *partial geordnete Algebra* – und dies mag eine beliebige Algebra $\mathfrak{A}$, bezogen auf die Gleichheitsrelation, sein – genug „ideale Mengen" besitzt, die der Bedingung genügen:

$$\text{(P)} \qquad \tilde{p}(b) \in M \ \& \ \tilde{q}(a) \in M \implies \tilde{p}(a) \in M \vee \tilde{q}(b) \in M$$

Dies führt zu weiteren Resultaten.

12. 3. 1 Korollar. *Jede beliebige partial geordnete Menge $(M, \leq) =: \mathfrak{M}$ ist subdirekt zerlegbar in höchstens 2-elementige Ketten.*

DENN: Wir betrachten $\mathfrak{M}$ bezüglich des identischen Operators. Dann ist die Familie aller $(a]$ $(a \in M)$ eine geeignete Familie idealer Mengen. □

Natürlich subsumiert der letzte Satz die Trivialität, dass jede Menge zerlegt werden kann in *singletons*. Denn man betrachte eine Menge als partial geordnete Algebra mit dem identischen Operator als Operation und der Gleichheitsrelation als Partialordnung.

12. 3. 2 Korollar. *Jeder beliebige $\vee$-Halbverband ist subdirektes Produkt 2-elementiger Ketten.*

DENN: Wir betrachten erneut die Familie aller $(a]$. □

12. 3. 3 Korollar. *Eine partial geordnete abelsche Gruppe $\mathfrak{G}$ ist repräsentierbar gdw. sie halb abgeschlossen ist, d. h., gdw. sie für jedes $n \in \mathbf{N}$ die Implikation erfüllt:* [1]

$$\text{(SC)} \qquad a^n \geq 1 \Longrightarrow a \geq 1 \, .$$

BEWEIS. Offenbar ist (SC) notwendig.
Sei nun (SC) erfüllt und a verschieden von b. Dann ist die Menge N strikt negativer Elemente multiplikativ abgeschlossen und es können im Falle $a \neq 1$ nicht a, N und a^{-1}, N beide ein *Untermonoid* erzeugen, da andernfalls $a^p \cdot n = 1$, also $a^p \geq 1$ und damit wegen (SC) $a \geq 1$ und analog $a^{-1} \geq 1$ einträte, also $a = 1$ – mit Widerspruch. Deshalb gibt es eine maximale Unterhalbgruppe $\mathfrak{M}$, die N enthält und o. B. d. A. das Element ab^{-1}, nicht aber 1. Wir zeigen, dass M ein Primideal ist im Sinne von (P).

(*i*) M ist ein o-Ideal, da $u < v \in M$ zu $uv^{-1} < 1 \ \& \ v \in M$ führt, was $(uv^{-1})v = u \in M$ impliziert.

[1] Es scheint, als habe CLIFFORD 1940 als erster die Repräsentierbarkeit partial geordneter Gruppen geklärt, siehe [53].
Ein weiterer Beweis findet sich bei DIEUDONNÉ 1941, siehe [63].

(ii) M ist prim, da $ax, by \in M$ & $ay, bx \notin M$ wegen der Maximalität von $\mathfrak{M}$ für geeignete m, k aus $\mathbf{N}$ zu $a^k y^k \cdot m = 1$ und damit weiter zu $a^{-k}y^{-k} = m \in M$und analog zu $b^{-k}x^{-k} \in M$ führen würde. Das lieferte aber wegen $a^k x^k, b^k y^k \in M$ den Widerspruch $a^{-k}b^k, a^k b^{-k} \in M$. □

Als Korollar des letzten Satzes erhalten wir

12. 3. 4 Korollar. *Eine abelsche Gruppe lässt genau dann eine Anordnung zu, wenn sie torsionsfrei ist.*

DENN: Lässt $\mathfrak{G}$ eine Anordnung zu, so ist $\mathfrak{G}$ natürlich *torsionsfrei,* und umgekehrt bedeutet Torsionsfreiheit nichts anderes als die Bedingung der Halbabgeschlossenheit im Blick auf die Gleichheitsrelation als Partialordnungsrelation. Deshalb führt Torsionsfreiheit zunächst zu einem subdirekten Produkt angeordneter Gruppen, das sich dann in einem zweiten Schritt *lexikographisch* ordnen lässt. □

Kapitel 13

Jakubík-Ketten in lo-Gruppoiden

Ein mathematisches Resultat mag einfallsreich sein oder fundamental, möglicherweise auch „nur" schön, oder aber gar schön und fundamental zugleich. Ein Resultat der letzten Art ist *Jakubík's Chain Theorem*, zumindest in den Augen des Verfassers. Es besagt:

13. 0. 5 Jakubík's Ketten Theorem. *Jede unbeschränkte konvexe Kette einer ℓ-Gruppe $\mathfrak{G}$, die das neutrale Element* 1 *enthält, ist ein direkter Faktor dieser Verbandsgruppe $\mathfrak{G}$.*

Beachte, jede unbeschränkte konvexe Kette ist eine *maximale Kette,* aber es können maximale unbeschränkte Ketten existieren, die nicht konvex sind. Man betrachte etwa in $(\mathbf{N}, \mid)$ die Kette

$$1, 2\,,\; 2 \cdot 3\,,\; 2 \cdot 3 \cdot 5\,,\; 2 \cdot 3 \cdot 5 \cdot 7\,,\; \ldots$$

Jakubík's Theorem wird vorgestellt in [102], und es wird dieser Gegenstand erneut aufgegriffen in [106]. Dort wird ein entsprechendes Theorem für *MV-Algebren* gegeben. Doch tatsächlich enthält jenes Papier mehr, wie im folgenden gezeigt werden soll.

13. 0. 6 Definition. Unter einem *Links-Divisor-Gruppoid*, kurz einem *LD-Gruppoid*, verstehen wir *ein* inf*-abgeschlossenes p.o.-Gruppoid* $\mathfrak{G} = (G, \wedge, \cdot\,, 1)$ mit *Einheitselement* 1, das also $a \cdot 1 = a = 1 \cdot a$, erfüllt und in dem zusätzlich gilt:

(LD) $$a \leq b \;\Rightarrow\; \exists\, x : a \cdot x = b$$

(DSM) $$\begin{aligned} a \cdot (b \wedge c) &= ab \wedge ac \\ (a \wedge b) \cdot c &= ac \wedge bc\,. \end{aligned}$$

Ist $\mathfrak{G}$ in diesem Sinne darüber hinaus ein *Rechts-Divisor-Gruppoid,* d.h. erfüllt $\mathfrak{G}$ zusätzlich

(RD) $$b \Rightarrow \exists\, y : y \cdot a = b$$

so nennen wir $\mathfrak{G}$ ein Divisor-Gruppoid, kurz ein D-Gruppoid.
Ist schließlich $\mathfrak{G}$ ein LD-Gruppoid mit

(RN) $$\forall\, a, b \,\exists\; a^\circ \perp b^\circ : (a \wedge b)a^\circ = a \;\&\; (a \wedge b)b^\circ = b\,,$$

so nennen wir $\mathfrak{G}$ ein *rechtsnormales LD-Gruppoid,* kurz ein *RN-LD-Gruppoid,* und folglich ein *RN-D-Gruppoid*, wenn $\mathfrak{G}$ sogar ein rechtsnormales D-Gruppoid ist.

Natürlich resultiert (LD) aus (RN), daher könnten wir das Axiom (LD) aus logischer Sicht „fallen lassen". Dennoch sei es hier zum Zwecke einer Akzentuierung als beschreibendes Axiom hinzugenommen. Man beachte

Bis hierher haben wir $\vee$-frei gearbeitet !

Als klassische Beispiele seien an dieser Stelle erwähnt *ℓ-Loops* und *Hoops*, das sind komplementäre Halbgruppen mit (N) $x \leq a * b, b * a \Longrightarrow x = 1$. Daher sind auch *partial geordnete Mengen,* betrachtet bezüglich $a * b = 1$ für $a \geq b$ und $a * b = b$ für $a \not\geq b$ einbezogen, insofern sich brouwersche Halbverbände mit (N) *subdirekt in Ketten* zerlegen lassen.
Sei von nun an a°, b° stets ein Paar von Elementen, das bezüglich a, b die Bedingung (RN) erfüllt. Unter dieser Voraussetzung sind dann mit x, y stets auch x°, y° *unvergleichbare Elemente.*
Und sei ferner im folgenden $\mathfrak{G}$, auch dort, wo dies nicht ausdrücklich erwähnt wird, ein positives RN-LD-Gruppoid, d.h. erfülle $\mathfrak{G}$ zusätzlich $1 \leq g \;\; (\forall g \in G)$.

13. 0. 7 Lemma. *Sei $\mathfrak{G}$ eine positives RN-LD-Gruppoid und seien $[1, a]$ und $[1, b]$ Ketten mit unvergleichbaren Elementen a, b. Dann folgt $a \perp b$.*

BEWEIS. Da a, b unvergleichbar sind, sind auch a° und b° unvergleichbar. Es gehören aber $a \wedge b$ und a° zu $[1, a]$ und $a \wedge b$ und b° zu $[1, b]$. Daher muss gelten $a \wedge b \leq a^\circ, b^\circ$, also $a \wedge b \leq a^\circ \wedge b^\circ = 1$. $\square$

Als Nächstes beweisen wir:

13. 0. 8 Ein Splitting Lemma.

(SP) $$y \leq ab \;\&\; (a \wedge y)y^\circ = y \Longrightarrow y = (y \wedge a)y^\circ \wedge yb \wedge ab = (y \wedge a)(y^\circ \wedge b)\,.$$

13. 0. 9 Lemma. *Sei $\mathfrak{G}$ ein positives RN-LD-Gruppoid und $[1, a]$ eine Kette aus $\mathfrak{G}$. Dann ist auch $[1, a^2]$ eine Kette.*

BEWEIS. Seien $x, y \in [\,1, a^2\,]$ unvergleichbar. Dann sind auch x° und y° unvergleichbar, was $x^\circ \neq 1 \neq y^\circ$ bedingt. Es gilt aber $(a \wedge x^\circ) \wedge (a \wedge y^\circ) = 1$ was $a \wedge x^\circ = 1 \vee a \wedge y^\circ = 1$ bedeutet, etwa $a \wedge x^\circ = 1$, und damit den Widerspruch $x^\circ \leq (x^\circ)^2 \wedge x^\circ a \wedge a x^\circ \wedge a^2 = (x^\circ \wedge a)(x^\circ \wedge a) = 1 \rightsquigarrow x^\circ = 1$ impliziert. □

Aus Lemma 13.0.9 folgt unmittelbar:

13. 0. 10 Lemma. *In einem positiven RN-LD-Gruppoid ist jede konvexe maximale Kette multiplikativ abgeschlossen.*

Schließlich stellen wir noch heraus:

13. 0. 11 Lemma. *In einem positiven RN-LD-Gruppoid gelten*

$$a \wedge bc = a \wedge ac \wedge bc = a \wedge (a \wedge b)c \tag{13.6}$$

$$a \wedge bc = a \wedge ba \wedge bc = a \wedge b(a \wedge c)\,. \tag{13.7}$$

Hiernach lässt sich beweisen:

13. 0. 12 Ein 1. Faktor-Theorem. *Sei $\mathfrak{G}$ ein positives RN-LD-Gruppoid und C eine unbeschränkte Kette aus $\mathfrak{G}$. Dann ist $G = C \cdot C^\perp$ und es ist $G = C \cdot C^\perp$ direkte Zerlegungen von $(G, \wedge)$.*

BEWEIS. Da C unbeschränkt ist. existiert zu jedem $a \in G$ ein x in C mit $x \not\leq a$, also mit $a \wedge x < x$. Seien nun $(a \wedge x) \cdot x^\circ = x$ und $(a \wedge x) \cdot a^\circ = a$ erfüllt.
Dann führt $a \wedge x < x$ zu $x^\circ \neq 1$, weshalb $x \wedge x^\circ \wedge a^\circ = 1 \rightsquigarrow a^\circ \wedge x = 1$.
Als Nächstes betrachten wir ein $c \in C$ oberhalb von x. Dann gehört $a^\circ \wedge c$ zu C und muss $a^\circ \wedge c \leq x$ erfüllen, also $a^\circ \wedge c = 1$.
Folglich ist a° *orthogonal* zu allen Elementen aus C, d. h. a° gehört zu $C^\perp$.
Dies impliziert $a = (a \wedge x) \cdot a^\circ \in C \cdot C^\perp$ für alle Elemente $a \in G$ und damit $G = C \cdot C^\perp$.
Zu zeigen bleibt: Aus $a = u.v = x.y \in C \cdot C^\perp$ folgt $u = x$ and $v = y$.
Hier führt das Splitting-Lemma zum Ziel, denn es gilt

$$x = (x \wedge u)(x^\circ \wedge v) = x \wedge u \rightsquigarrow x \leq u \rightsquigarrow x = u\,,$$

die letzte Folgerung aus Gründen der Dualität, und es gilt

$$y = (y \wedge u)(y \wedge v) = y \wedge v \rightsquigarrow y \leq v \rightsquigarrow y = v\,.$$

Schließlich erhalten wie im Falle $a \perp b, d$ & $c \perp b, d$ nmittels (13.6) und (13.7) :

$$\begin{aligned} ab \wedge cd &= a(b \wedge cd) \wedge cd \\ &= (a \wedge cd)(b \wedge cd) \wedge cd \\ &= (a \wedge c)(b \wedge d) \wedge cd \\ &= (a \wedge c)(b \wedge d)\,, \end{aligned}$$

d. h. $\wedge$ respektiert die Zerlegungseigenschaft. □

Soweit gelten alle Ergebnisse in jedwedem positiven RN-LD-Gruppoid $\mathfrak{G}$, und wir haben gezeigt, dass sich die Menge G als Cartesisches Produkt $G = C \cdot C^{\perp}$ schreiben lässt.
Damit können wir herleiten:

13. 0. 13 Ein 2. Faktor-Theorem. *Sei $\mathfrak{G}$ ein positives LD-Gruppoid mit*

(DSJ)
$$\begin{aligned} a \cdot (b \vee c) &= ab \vee ac \\ (a \vee b) \cdot c &= ac \vee bc \end{aligned}$$

und sei $G = C \times C^{\perp}$. Dann respektiert $\cdot$ die Operation $\times$.

BEWEIS. In jedem LD-Gruppoid gilt:

$$u \perp v \;\&\; u, v \leq w \;\&\; w = ux \Longrightarrow v = (u \wedge v) \cdot (v \wedge x) = v \wedge x \Longrightarrow uv \leq w\,,$$
also

$$u \perp v \Longrightarrow uv = u \vee v = vu\,. \tag{13.9}$$

Ist nun $a, c \in C$ & $b, d \in C^{\perp}$, so ist wegen $u \wedge vw \leq (u \wedge v)(u \wedge w)$ $ac \in C$ & $bd \in C^{\perp}$ erfüllt, und wir erhalten weiter

$$\begin{aligned} ab \cdot cd &\overset{(13.9)}{=} (a \vee b) \cdot (c \vee d) \\ &= ac \vee ad \vee bc \vee bd \\ &= ac \vee (a \vee d) \vee (b \vee c) \vee bd \\ &= ac \vee bd = ac \cdot bd\,, \end{aligned} \tag{13.10}$$

was zu beweisen war. □

Schließlich erhalten wir

13. 0. 14 Ein 3. Faktor-Theorem. *Sei $\mathfrak{G}$ ein RN-LD-Monoid und $S = C \times C^{\perp}$. Dann respektiert die Multiplikation die Operation $\times$.*

BEWEIS. Ist $\mathfrak{S}$ positiv, erhalten wir $a \bot b \Longrightarrow ab = a \vee b$ so wie oben. Folglich führt in diesem Fall sie Annahme $a, c \in C$ & $b, d \in C^{\bot}$ zur Assoziativität vermöge:

$$ab \cdot cd = a(bc)d = a(cb)d = (ac)(bd)\,.$$

Sei hiernach $\mathfrak{S}$ ein beliebiges *RN-DL-Monoid* und

$$a(1 \wedge a)^{-1} = u \cdot v, (1 \wedge a)^{-1} = x \cdot y \ \ (x, u \in C, y, v \in C^{\bot})\,.$$

Dann folgt

$$a = a(1 \wedge a)^{-1} \cdot (1 \wedge a) = uv \cdot x^{-1}y^{-1} = ux^{-1} \cdot vy^{-1}\,(u, x^{-1} \in C, v, y^{-1} \in C^{\bot})\,.$$

Sei hiernach $u_1, v_1, u_2, v_2 \in C$ & $x_1, y_1, x_2, y_2 \in C^{\bot}$ und

$$a = u_1 x_1^{-1} \cdot v_1 y_1^{-1} = u_2 x_2^{-1} \cdot v_2 y_2^{-1}\,.$$

erfüllt. Dann folgt

$$\begin{array}{rcl} u_1 v_1 \cdot (y_1 x_1)^{-1} & = & u_2 v_2 \cdot (y_2 x_2)^{-1} \\ & \rightsquigarrow & \\ (y_1 x_1)^{-1} \cdot u_1 v_1 & = & u_2 v_2 \cdot (y_2 x_2)^{-1} \\ & \rightsquigarrow & \\ u_1 v_1 \cdot y_2 x_2 & = & y_1 x_1 \cdot u_2 v_2 \end{array}$$

mit

$$u_1 v_1 \bot y_1 x_1 \text{ und } u_2 v_2 \bot y_2 x_2\,,$$

was zu $y_1 x_1 = y_2 x_2$ führt und damit nach Kürzung auch zu $u_1 v_1 = u_2 v_2$. Das bedeutet aber

$$S = (C \cup C^{-1}) \times (C^{\bot} \cup (C^{\bot})^{-1})\,.$$

Zu zeigen bleibt, dass $C \cup C^{-1}$ mit $C^{-1} := \{c^{-1} \,\big|\, c \text{ invertierbar } \& \ c \in C\}$ eine multiplikativ abgeschlossene Kette bildet.
Natürlich ist $C \cup C^{-1}$ eine Kette. Um zu beweisen, dass $C \cup C^{-1}$ multiplikativ abgeschlossen ist, unterscheiden wir:
FALL 1. Ist $1 \leq a \leq b$ und existiert a^{-1}, so erhalten wir $1 \leq a^{-1}b, ba^{-1} \leq b$ weshalb dann die Produkte ab^{-1} und ba^{-1} zu C gehören.
FALL 2. Ist $1 \leq b \leq a$ und existiert a^{-1}, so existiert auch b^{-1} und es gehören $b^{-1}a$ und ab^{-1} zu C. Das aber bedeutet, dass $a^{-1}b$ und ba^{-1} zu C^{-1} gehören. $\square$

Eine Anwendung auf ℓ-Loops

Das 2. Faktor-Theorem greift insbesondere bei ℓ-Loops. Um aber dieses Ergebnis in das Kapitel über d-Semi-Loops zu integrieren, sei noch ein spezieller Hinweis gegeben: Zur Erinnerung: In ℓ-Loops gelten

$$x \perp y \Longrightarrow ax \circ y = a \circ xy = a \circ yx = ay \circ x \tag{13.11}$$

und das Linksduale hierzu. Das bedeutet insbesondere $x \perp y \Longrightarrow xy = x \vee y$ und damit

$$\begin{aligned} ax \circ by &= ax \circ (b \vee y) \\ &= ax \circ b \vee ax \circ y \\ &= a \circ xb \vee a \circ xy \\ &= a \circ bx \vee a \circ xy \\ &= a \circ (bx \vee xy) \\ &= a \circ (bx \vee ((yx) : x)x) \\ &= a \circ ((b \vee (xy : x)) \circ x) \\ &= a \circ ((b \circ (xy : x)) \circ x) \\ &= a \circ (b \circ ((xy : x))x) \\ &= ab \circ ((xy : x))x) \\ &= ab \circ xy\,. \end{aligned}$$

Weiterhin überträgt sich diese Direkt-Zerlegung vom Kegel auf die Ganze ℓ-Loop, wie wir ober gezeigt haben.

Als Nächstes erhalten wir:

13. 0. 15 Proposition. *In ℓ-Loop-Kegeln erzeugen Atome total geordnete Unterhalbgruppen.*

BEWEIS. Sei $p > 1$ ein Atom: Dann ist $[1, p]$ eine Kette. Sei nun für alle Produkte $f(p)$ der Länge $|f(p)| \leq n$, also für alle Produkte mit höchstens n Komponenten p, das Intervall $[1, f(p)]$ eine Kette. Dann ist jedes $g(p)$ mit $|g(p)| = n+1$ vom Typ $h(p) \circ k(p)$, mit $|h(p)|, |k(p)| \leq n$, und o.B.d.A. $|h(p)| \leq |k(p)|$.

Nun ist aber nach 13.0.9 das Intervall $[1, k(p)^2]$ wieder eine Kette, weshalb $[1, h(p) \circ k(p)]$ ebenfalls eine Kette ist.

Folglich bildet (auch) die Menge P aller Produkte $m(p)$ eine Kette, man beachte, dass jedes $[1, f(g(p))]$ eine Kette bildet.

Weiterhin erfüllt P nach dem Splitting-Lemma die Kettenbedingung, da anderenfalls $p^n \backslash f(p)$ eine unendliche Kette wäre. Somit wird jedes $f(p)$

übertroffen von mindestens einem p^n,
Als nächstes beachten wir, dass $ap.b$ das Element ab bedeckt. Das bedeutet:
(1) $ap = xa \Longrightarrow x = p$ d.h. p „kommutiert" mit jedem a, insbesondere gilt damit $p \cdot q = 1 \Longleftrightarrow q \cdot p = 1$.
(2) Das Intervall $[1, p^n]$ wird ausgeschöpft von $\{1, p, p^2, p^3 = (p^2)p, ..., p^n\}$.
(3) Es ist $p^k p \circ p^m = p^k \circ pp^m$, da $p^n p \circ p^m = p^k \circ xp^m \ (\exists x)$ erfüllt ist mit $x = p^m \ (\exists m \in \mathbf{N})$, was $x = p$ impliziert.

Aus diesem Grunde erhalten wir fast unmittelbar $p^m \circ p^n = p^{m+n}$, also die Assoziativität für $(P, \circ)$ und somit – insgesamt – die Behauptung. $\square$

13. 0. 16 Proposition. *In ℓ-Loops erzeugen die Atome $p \geq 1$ total geordnete Untergruppen.*

BEWEIS. Nach (1) ist jedes Atom invertierbar. Folglich ist auf Grund der $\leq, \geq$-Dualität auch bewiesen, das die Menge N aller $(p^{-1})^n$ einen ℓ-Gruppen-Kegel bildet.
Zu zeigen bleibt, dass $P \cup N$ multiplikativ abgeschlossen und assoziativ ist. Das aber ergibt sich entlang der obigen Linien und mag deshalb dem Leser überlassen bleiben. $\square$

Schließlich erhalten wir einen neuen Zugang zu 11.4.3.

13. 0. 17 Korollar. *Sei $\mathfrak{L}$ eine d-Semi-Loop, deren Kegel die absteigende Kettenbedingung erfüllt. Dann ist $\mathfrak{L}$ eine direkte Summe von Kopien von* $(\mathbf{N}, +, \min)$ *und* $(\mathbf{Z}, +, \min)$.

Ketten in Clans

13. 0. 18 Lemma. *Sei $\mathfrak{S}$ ein Clan und C eine konvexe Kette in $\mathfrak{S}$. Dann ist auch $C * a$ eine konvexe Kette. Insbesondere bildet die Menge aller $c \wedge a \ (c \in C)$ eine konvexe Kette.*

BEWEIS. Betrachte $x * a, z * a \ (x \leq z \in C)$. Dann gilt $x * a \geq z * a$, weshalb $C * a$ total geordnet ist.
Sei hiernach $z * a \leq y \leq x * a$ mit $x, z \in C$. Dann liefert $y \leq x * a \leq a$ die Gleichheit $y = (a : y) * a$ und damit

$$z \geq (a : z) * a \geq a : y \geq (a : x) * a \geq x \rightsquigarrow a : y \in C\,.$$

Als ein Beispiel betrachten wir $(\mathbf{N}, *)$ wie oben und wählen ein $n \in \mathbf{N}$. Hier sind alle maximalen und konvexen Ketten vom Typ $p^0, p^1, p^2, \ldots p^k \ldots$ und es sind die Elemente des Typs $n \wedge p^n$ die *Primpotenzteiler* von n .

13. 0. 19 Ein 4. Faktor-Theorem. *Sei* $\mathfrak{G} = (G, *, :, \wedge, \vee)$ *ein Clan und sei* C *eine unbeschränkte Kette in* $\mathfrak{G}$. *Dann folgt* $\mathfrak{G} = \mathfrak{C} \times \mathfrak{C}^\perp$.

BEWEIS. Zur Erinnerung: in $\mathfrak{G}$ ist eine *partielle Multiplikation* $\circ$ erklärt für alle nach oben beschränkten Paare a, b. Dies bedeutet, dass der Beweis des 1. Faktor-Theorems auch in der vorliegenden Situation greift, d. h. eine Zerlegung $a = (a \wedge x) \circ a^\circ$ mit $a^\circ \perp C$ gewährleistet.
Wegen der Verbandsdistributivität folgt weiter fast direkt, dass $(C, \wedge, \vee)$ ein direkter Faktor von $(G, \wedge, \vee)$ ist.
Zu zeigen bleibt, dass wir im Falle $a, b \in C$ & $x, y \in C^\perp$ die Gleichheit $(a \vee x) * (b \vee y) = (a * b) \vee (x * y)$ erhalten, woraus der Rest aus Gründen der Dualität folgt. Wir erinnern an

$$u \perp v \;\Rightarrow\; u * v = v \tag{13.12}$$

$$u * (v \vee w) = u * v \vee u * w \tag{13.13}$$

$$(u \vee v) * w = u * w \wedge v * w\,, \tag{13.14}$$

und kalkulieren:

$$\begin{aligned}
(a \vee x) * (b \vee y)) &= ((a \vee x) * b) \vee ((a \vee x) * y) \\
&= ((a * b) \wedge (x * b)) \vee ((a * y) \wedge (x * y)) \\
&= ((a * b) \wedge b) \vee ((a * y) \wedge y)) \\
&= (a * b) \vee (x * y)\,.
\end{aligned}$$

Damit sind wir am Ziel. □

Im Falle, dass die betrachtete Kette C beschränkt ist, kann C ein direkter Faktor sein, muss aber nicht! Man betrachte hierzu den booleschen Verband auf der einen Seite und auf der anderen Seite das d-Monoid $(\mathbf{N}^\circ, \cdot, \wedge)$.

Als ein weiteres Beispiel sei der Brick erwähnt. Hier ist eine Kette genau dann ein direkter Faktor, wenn sie ein idempotentes Maximum u enthält, da jedes *idempotente Element* eine direkte Zerlegung erzeugt. Dies wurde oben für den kommutativen Fall bewiesen, überträgt sich aber leicht auch auf den nicht kommutativen Fall, da alle *Idempotenten* im *Zentrum* liegen.

Schließlich erwähnen wir das klassischste aller Beispiele:

13. 0. 20 Beispiel. *Man betrachte den $\mathbf{R}^n$. Hier sind die Geraden durch den Ursprung exakt alle maximalen konvexen Ketten durch O, das Einelement von $(\mathbf{R}^n, +, \vee, \wedge)$, und es ist der $\mathbf{R}^n$ das direkte Produkt je dreier „unabhängiger" dieser Geraden.*

Kapitel 14

Ideale – Linearität – Orthogonalität

Wir betrachten eine normale komplementäre Halbgruppe, wir betrachten eine positiv d-semiloop. In beiden Fällen haben wir es mit einer Verbandsstruktur zu tun, die den Bedingungen genügt:

(VGG) $\qquad (S,\cdot)$ ist ein *Gruppoid mit* 1.

(VGD) $\qquad (S,\wedge,\vee)$ ist ein distributiver Verband.

(VG∧) $\qquad \forall\, x,a,b,y : \quad x(a\wedge b)y \;=\; xay\wedge xby\,.$

(VG∨) $\qquad \forall\, x,a,b,y : \quad x(a\vee b)y \;=\; xay\vee xby\,.$

(RN) $\qquad \forall(a\wedge b)\ \exists\, a^\circ\bot b^\circ : \,(a\wedge b)\cdot a^\circ = a\ \&\ (a\wedge b)\cdot b^\circ = b\,.$

Man beachte, dass (VG∧) und (VG∨) wegen $1\in S$ auch einseitig gilt. Ferner sei betont, dass aus $a\cdot(b\wedge c) = ab\wedge ac$ und (RN) das Splitting-Lemma resultiert, also:

$$a\wedge bc = (a\wedge b)(a^\circ\wedge c)\,. \tag{14.6}$$

Wir wollen Strukturen dieses Typs als RNDV-Gruppoide – *rechtsnormale Divisoren-Verbandsgruppoide* bezeichnen und vereinbaren:

Grundgegebenheit sei in diesem Kapitel stets

ein RNDV-Gruppoid $\mathfrak{S} = (S,\cdot,\vee,\wedge)$.

Wir werden also Formulierungen wie „Sei $\mathfrak{S}$ ein RNDV-Gruppoid, dann...." oder ähnlich in den Definitionen und Propositionen unterdrücken.
Unsere Untersuchungen wurden angeregt durch die höchst verdienstvolle Lecture Note [7] von Übersichts- und Integrations-Charakter, die ihrerseits wiederum evoziert wurde durch Paul Conrad's „Introduction..." [57], und wir werden entlang Bigard-Keimel-Wolfenstein bewegen.

Es muss und soll aber betont werden, dass alle Ergebnisse, wenngleich hier auf Gruppoide bezogen, ihrem Wesen nach der tschechoslowakischen Schule, angeführt von Jan Jakubík, [103, 104, 105] und Ference Šik, [142], sowie den Beiträgen von Paul Conrad, [56, 57, 58], zuzuschreiben sind. Der Grund für die Übertragungsmöglichkeit der klassischen Theorie auf das RNDV-Gruppoid ist der stark distributive Charakter des RNDV-Gruppoids. Weder die Assoziativität noch die Kürzungsregeln sind für die Herleitungen diese Kapitels relevant, das scheint natürlich auch in [7] schon auf, wenn man sich auf den Kern der dortigen Herleitungen konzentriert.

Zur Erleichterung des Verständnisses empfehlen wir an dieser Stelle dem Leser, wo immer in diesem Kapitel die Rede von $\mathfrak{S}$ ist, sich an der Algebra $(\mathbf{N}^0, \cdot, \mathrm{GGT}, \mathrm{KGV})$ zu orientieren, bzw. in dieser Algebra die 0 durch eine endliche boolesche Algebra $\mathfrak{B}$ zu ersetzen und für $a \in \mathbf{N}, b \in B$ $ab = ba = b$ zu definieren.

Schließlich zur Notation: Weiterhin unterscheiden wir zwischen Trägermengen und den Strukturen, die sie tragen. So werden wir z.B. Ideale mit großen lateinischen Buchstaben, etwa $I, L, K...$ notieren, die Strukturen, die sie tragen hingegen mit großen gotischen Buchstaben, also mit $\mathfrak{I} := (I, \cdot, \wedge, \vee), ..., \mathfrak{L}, \mathfrak{K}$.

Endlich seien ein für alle Mal zu jedem Paar a, b Elemente a°, b° im Sinne von (RN) fest gewählt.

14.1 Ideale

14. 1. 1 Definition. Unter einem Ideal aus $\mathfrak{S}$ verstehen wir jedes *multiplikativ abgeschlossene Verbandsideal.*

Mit jeder Familie $\{I_\lambda\}$ von Idealen ist auch deren Durchschnitt ein Ideal, beachte $1 \in I_\lambda$.
Folglich erzeugt jede Untermenge A ein engstes A enthaltendes Ideal A^c, da S ein Ideal bildet. Ist $A insingleton \{a\}$ so notieren wir kürzer a^c. Offenbar gilt $\emptyset^{\,c} = \{1\}$. Damit folgt

14. 1. 2 Proposition. *Die Menge $C(\mathfrak{S})$ aller Ideale aus $\mathfrak{S}$ bildet einen vollständigen Verband bezüglich $\supseteq$.*

14. 1. 3 Proposition. *Sei M eine nicht leere Teilmenge von S. Dann ist*

M^c gleich der Menge aller endlichen Vereinigungen von Produkten, gebildet aus Elementen aus M.
Demzufolge ist der Verband aller Ideale algebraisch bezüglich der Summenbildung $\sum$.

DENN: Der Beweis folgt fast *per definitionem*, man beachte (VG$\vee$) und das erweiterte Splitting-Lemma. $\square$

Insbesondere ist demnach die „Summe" $A \vee B$ zweier Ideale – äquivalent auch bezeichnet mit $A+B$ – gleich dem Erzeugnis der Vereinigungsmenge, da nach Konstruktion A und B in dieser Menge enthalten sind, während diese Menge ein Unter-RNDV-Gruppoid eines jeden gemeinsamen Ober-Ideals von A und B bildet.
Dies liefert uns fast unmittelbar weiter

14. 1. 4 Proposition. *$C(\mathfrak{S})$ bildet sogar einen distributiven Verband bezüglich $\cap$ und $\vee$ $(+)$.*

BEWEIS. Zur Erinnerung: Verbandsdistributivität ist u.a. äquivalent zu der Implikation $a \leq b \vee c \Longrightarrow a = (a \wedge b) \vee (a \wedge c)$.
Mittels dieser Bedingung und des erweiterten Splitting-Lemmas gelangen wir dann garadeaus zu $A \cap (B \vee C) \supseteq (A \cap B) \vee (A \cap C)$. $\square$

14.2 Prime Ideale

Ein Ideal P aus $\mathfrak{S}$ heißt *prim*, wenn es verschieden ist von $\{1\}$ und die Implikation $ab \in P \Longrightarrow a \in P \bigvee b \in P$ erfüllt. Ein Ideal M heiße *minimal prim*, wenn es minimal ist in der Menge aller von $\{1\}$ verschiedenen Primideale. Offenbar ist S selbst ein primes Ideal und zusammen mit einer Kette $\{P_i\}$ $(i \in I)$ von primen Idealen ist auch ihr Durchschnitt D ein primes Ideal wegen

$$a \wedge b \in D \ \&\ a \notin D \Longrightarrow \exists P_j : a \notin P_j \Longrightarrow b \in D\,,$$

$\mathfrak{D}$ muss kein Primideal enthalten. Man denke an die zwei-elementige boolesche Algebra.
Existiert aber wenigstens ein Primideal P, so existiert – nach ZORN – auch ein minimal primes Ideal M, das sogar in P enthalten ist.

Denn, es ist mit jeder Kette von Primidealen auch ihr Durchschnitt D ein Primideal. Folglich umfasst jedes Primideal P nach ZORN ein minimal primes Ideal M.
Weiter ist mit jeder Kette von Idealen auch ihre Vereinigung ein Ideal. Folglich existieren, da $\{1\}$ ein Ideal ist, nach ZORN zu jedem $a \neq 1$ maximale Ketten von Idealen, die a nicht enthalten und damit Ideale M, maximal bezüglich der Eigenschaft, a zu meiden.
Solche maximalen Ideale werden als *Werte von* a bezeichnet. Diese Werte sind notwendig prim, was sich wie folgt einstellt:
Sei W ein Wert von a und $x \wedge y \in W$, aber $x, y \notin W$. Dann führt $R(x, y, x^\circ, y^\circ)$ zu $x^\circ, y^\circ \notin W$. Es gilt aber $x^\circ \wedge y^\circ = 1 \in W$. Betrachte nun die Menge $U := \{u \,\big|\, x^\circ \wedge u \in W\}$. Diese Menge bildet ein Ideal, wie man leicht sieht, und wegen $y^\circ \in U$ aber $y \notin W$ erhalten wir $a \in W \subset U$. Definiere nun $V = \{v \,\big|\, u \wedge v \ \ (\forall u \in U)\}$. Dann erhalten wir analog $a \in W \subset V$. Das aber bedeutet den Widerspruch $a \wedge a = a \in W$. Somit ist jeder Wert ein primes Ideal .

14. 2. 1 Definition. Zur Erinnerung: Ist $\mathfrak{L}$ ein Verband, so versteht man unter einem *Filter* jede Untermenge F mit $a, b \in F \iff a \wedge b \in F$. Insbesondere gehört also mit jedem a auch jedes $b \geq a$ zu F. Ein Filter heißt prim, wenn er $a \vee b \in F \Longrightarrow a \in F \bigvee b \in F$ erfüllt.
Ein Filter U heißt ein *Ultrafilter*, wenn er maximal ist unter allen Filtern, die 1 nicht enthalten.

14. 2. 2 Proposition. *Das mengentheoretische Komplement eines Primideals aus $\mathfrak{S}$ ist ein Primfilter – und umgekehrt.*
Und es ist das mengentheoretische Komplement eines Ultrafilters ein minimal primes Ideal – und umgekehrt das mengentheoretische Komplement eines minimal primen Ideals ein Ultrafilter.

BEWEIS. Die erste Behauptung ist fast evident.
Sei hiernach U an Ultrafilter und $x \leq y \notin U$, also $x \notin U$. Dann folgt

$$\begin{aligned} a, b \notin U &\Longrightarrow a \wedge x = 1 = b \wedge y \ \ (\exists\, x, y \in U) \\ &\Longrightarrow ab \wedge (ay \wedge xb \wedge xy) = 1 \\ &\Longrightarrow ab \notin U\,. \end{aligned}$$

Folglich ist das Komplement eines Ultrafilters ein primes Ideal P. Angenommen nun, P würde noch ein weiteres primes Ideal M echt umfassen,

dann wäre das Komplement von M ein Primfilter, der U echt enthalten würde, mit Widerspruch!
Sei schließlich M ein *minimal primes Ideal.* Dann ist das Komplement F von M ein Filter, nach Zorn eingebettet in einen Ultrafilter U, und es ist $S\backslash U$ ein primes Ideal, enthalten in M, also gleich M . Das bedeutet $F = U$, weshalb F ein Ultrafilter ist. $\square$

Unter den primen Idealen ist eine Klasse spezieller primer Ideale von besonderem Interesse, nämlich die Klasse der $\bigcap$-*primen Ideale.*

14. 2. 3 Definition. Wir nennen $R \in C\,(\mathfrak{S})$ regulär, auch $\bigcap$-prim, wenn R nicht Durchschnitt echter Ober-Ideale ist.

14. 2. 4 Proposition. *Das Ideal R ist regulär gdw. ein $c \notin R$ existiert, das zu allen Idealen A_i $(i \in I)$ gehört, die R echt enthalten.*

BEWEIS. Sei R regulär. Wir bilden den Durchschnitt D aller $A_i \in C\,(\mathfrak{S})$, die R echt enthalten und wählen ein $c \in D\backslash R$.
Dann gehört c zu allen Idealen von $\mathfrak{S}$, die R echt enthalten, also auch zu ihrem Durchschnitt. $\square$

Weiter gilt

14. 2. 5 Proposition. *Jedes Ideal C ist Durchschnitt von regulären Idealen.*

BEWEIS. Wir bilden den Durchschnitt D aller regulären Ideale, die C enthalten und nehmen an, es gäbe ein $d \in C\backslash D$. Dann könnten wir C ausdehnen zu einem (regulären) Wert von d, mit Widerspruch. $\square$

14. 2. 6 Definition. Sei C ein Ideal aus $\mathfrak{S}$. Dann verstehen wir unter der *Polaren* von $A \subseteq S$ in C, kurz der C-*Polaren* of A, die Menge

$$A^{\perp C} := \{x \,\big|\, a \wedge x \in C \;\; (\forall a \in A)\}\,.$$

Insbesondere nennen wir $A^{\perp\{1\}}$ die *Polare* von A, in Zeichen $A^{\perp}$. Weiter schreiben wir zur Vereinfachung $A^{\perp\perp}$ statt $(A^{\perp})^{\perp}$ und nennen $A^{\perp\perp}$ die *Bipolare* von A .

14. 2. 7 Proposition. *Sei P ein Ideal aus $\mathfrak{S}$. Dann sind paarweise äquivalent:*

(*i*) *P ist prim.*

(*ii*) $a \wedge b \in P \Longrightarrow a \in P \vee b \in P$.

(*iii*) $a \wedge b = 1 \Longrightarrow a \in P \vee b \in P$.

(*iv*) $\{A \,|\, P \subseteq A \in C(\mathfrak{S})\}$ *ist linear geordnet.*

BEWEIS. $(i) \Longrightarrow (ii)$, wegen

$$\begin{aligned} a \wedge b \in P &\Longrightarrow a^{\perp P} \cap b^{\perp P} \subseteq P \\ &\Longrightarrow a^{\perp P} \subseteq P \vee b^{\perp P} \subseteq P \\ &\Longrightarrow a \in P \vee b \in P \,. \end{aligned}$$

$(ii) \Longrightarrow (iii)$ ist evident.

$(iii) \Longrightarrow (iv)$. Seien A und B zwei Ideale und sei $a \in A$, $b \in B$ beliebig gewählt. Dann folgt $a \wedge b \in A \cap B$ und $R(a, b, a^\circ, b^\circ)$ $(a^\circ \in A \ \&\ b^\circ \in B)$. Seien hiernach A , B unvergleichbar mit $a^\circ \in A \backslash B$ und $b^\circ \in B \backslash A$. Dann folgt $a^\circ \wedge b^\circ = 1 \Longrightarrow a^\circ = 1 \vee b^\circ = 1$, mit Widerspruch!

$(iv) \Longrightarrow (i)$ folgt erneut fast unmittelbar. □

14. 2. 8 Definition. Sei R ein reguläres Ideal und c in Element im Sinne von 14.2.4. Dann bezeichnet man R als einen *Wert* von c und symbolisiert die Menge aller Werte von c mittels $\mathrm{val}(c)$.

14. 2. 9 Das Projektions-Theorem. *Sei C ein Ideal aus $\mathfrak{S}$. Dann liefert $A \longmapsto C \cap A$ offenbar eine surjektive Abbildung von $C(\mathfrak{S})$ auf $C(\mathfrak{C})$.*
Ist dann M ein Wert von $c \in C$ in $\mathfrak{S}$, so ist $M \cap C$ ein Wert von c in $\mathfrak{C}$ und jeder Wert von c in $\mathfrak{C}$ ist von dieser Art.
Darüber hinaus ist die Restriktion dieser Funktion auf Ideale von $\mathfrak{S}$, die C nicht enthalten, sogar eine Bijektion.

BEWEIS. Sei M ein Wert von $c \in C$ und gehöre d zu $C \backslash M$. Dann gehört c zu dem Erzeugnis von M und d in $\mathfrak{S}$ und damit nach 14.2.7 auch zu dem Erzeugnis aller $m \wedge d$ $(m \in M)$ und folglich zu $c \in ((C \cap M), d)^c$. Also ist $M \cap C$ eine Wert von d in C .
Sei nun D ein Wert von $c \in C$ in C . Dann lässt D eine Ausdehnung zu einem Wert M von c in $\mathfrak{S}$ zu, und dieser Wert erfüllt $D = M \cap C$. Folglich ist die definierte Abbildung surjektiv.
Seien schließlich A , B zwei verschiedene reguläre Ideale von $\mathfrak{S}$, die C nicht enthalten . Dann sind auch $A \cap C$ und $B \cap C$ verschieden. Denn, sei

$A \cap C = B \cap C$ und A ein Wert von a, B eine Wert von b. Gehörte dann d zu $C \backslash (C \cap A \cap B)$, so wäre $A \cap C = B \cap C$ ein Wert von $c = a \wedge b \wedge d$ in $\mathfrak{C}$, woraus der Widerspruch resultieren würde:

$$c \notin C \cap A \cap B \ \& \ c \in C \cap (A \vee B) = (C \cap A) \vee (C \cap B) = C \cap A \cap B\,. \quad \square$$

14.3 Polaren

Zur Erinnerung: Zwei Elemente a, b heißen orthogonal, wenn sie $a \wedge b = 1$, auch symbolisiert durch $a \perp b$ erfüllen.

14. 3. 1 Proposition. *Zwei Elemente $a \neq 1 \neq b$ sind orthogonal, gdw. ihre Werte paarweise unvergleichbar sind.*

BEWEIS. Gilt $a \not\perp b$, so lässt jeder Wert von $a \wedge b$ eine Ausdehnung zu einem Wert A von a und zu einem Wert B von b zu. Diese aber sind unvergleichbar.
Und gilt $a \perp b$, so kann kein Paar A, B vergleichbarer Werte von a und b existieren, da aus $A \subseteq B$, z.B., folgen würde $a \notin A \ \& \ b \notin A$, mit Widerspruch zu $a \wedge b = 1$. $\square$

Hiernach wenden wir uns einem detaillierten Studium der Polaren zu. Zunächst haben wir offenbar

$$A \supseteq B \implies B^{\perp} \supseteq A^{\perp}\,. \tag{14.7}$$

und damit

$$a \in A \Longrightarrow a^{\perp} \supseteq A^{\perp} \Longrightarrow a^{\perp\perp} \subseteq A^{\perp\perp} \subseteq A\,. \tag{14.8}$$

Weiter gilt *per definitionem* für jeden Homomorphismus h von $(S, \wedge)$

$$h(A^{\perp}) \subseteq h(A)^{\perp}\,. \tag{14.9}$$

Sodann erhalten wir

$$A \subseteq A^{\perp\perp} \quad \text{und} \quad A^{\perp} = A^{\perp\perp\perp}\,. \tag{14.10}$$

BEWEIS. $A \subseteq A^{\perp\perp}$ impliziert $A^{\perp} \subseteq A^{\perp\perp\perp}$, und $A^{\perp} \supseteq A^{\perp\perp\perp}$ resultiert aus (14.7). $\square$

14. 3. 2 Korollar. *A ist Polare gdw. $A = A^{\perp\perp}$ erfüllt ist.*

Die Orthogonalität von Elementen aus S ist aufs Engste verknüpft mit der Orthogonalität der Ideale aus $\mathfrak{S}$. Zunächst erhalten wir mittels der Polaren-Arithmetik:

14. 3. 3 Proposition. *Jede Polare A ist ein Ideal .*

Dies führt zu

$$x \perp A \iff x^c \cap A^c = \{1\}\,. \tag{14.11}$$

BEWEIS. $x\perp A \Longrightarrow x^c \subseteq A^\perp \Longrightarrow A \subseteq x^{c\perp} \Longrightarrow A^c \subseteq x^{c\perp} \Longrightarrow x^c \cap A^c = \{1\}$ und $x^c \cap A^c = \{1\} \Longrightarrow y \wedge z = 1\ (\forall\ y \in x^c, z \in A^c)\,.$ □

Zusätzlich hat sich ergeben:

$$A^\perp \;=\; (A^c)^\perp. \tag{14.12}$$

Im weiteren werden wir die Menge der Polaren von $\mathfrak{S}$ mit $P(\mathfrak{S})$ bezeichnen. Offenbar ist $P(\mathfrak{S})$ partial geordnet. Tatsächlich gilt aber sehr viel mehr. Doch bevor wir fortfahren betonen wir, dass man zu unterscheiden hat zwischen der (*Ideal-*)*Hülle* zweier Polaren und ihrer P-(*olaren-*)*Hülle.* Um deutlich zu machen, welche Hülle jeweils gemeint ist, werden wir den Index p einsetzen. $\vee_p$ bezieht sich dann auf die Bildung der Polaren-Summe, $\vee$ auf die Bildung der Ideal-Summe.

$$(\bigvee A_i)^\perp \;=\; \bigcap(A_i{}^\perp)\ \ (i \in I)\,. \tag{14.13}$$

BEWEIS. Nach (14.7) ist die linke Seite in der rechten Seite enthalten. Und gehört *vice versa* x zu der rechten Seite, so ist x orthogonal zu allen A_i, und damit auch zu $\bigvee A_i$, weshalb auch die rechte Seite in der linken enthalten ist. □

Insbesondere ist nach (14.13) der Durchschnitt von Polaren wieder eine Polare. Als unmittelbare Konsequenz erhalten wir damit:

14. 3. 4 Korollar. $P(\mathfrak{S})$ *ist eine* MOORE'*sche Familie.*

14. 3. 5 Korollar. *Die Menge der Polaren bildet einen vollständigen Verband.* $\mathfrak{P}(\mathfrak{S})$ *bezüglich*

$$\bigwedge A_i := \bigcap A_i \ \text{ and } \ \bigvee\nolimits_p A_i := (\bigcap A_i{}^\perp)^\perp \quad (i \in I)\,. \tag{14.14}$$

BEWEIS. Nach (14.13) ist mit jeder Familie von Polaren auch deren Durchschnitt eine Polare und die zweite Behauptung folgt aus

$$\begin{aligned} P \supseteq \bigvee A_i &\iff P^\perp \subseteq \bigcap A_i{}^\perp \\ &\iff P \supseteq (\bigcap A_i{}^\perp)^\perp \quad (i \in I)\,, \end{aligned}$$

fertig! □

Als nächstes zeigen wir, dass die Polaren nicht nur einen vollständigen Verband bilden, sondern sogar eine vollständige boolesche Algebra. Wir beginnen mit

14. 3. 6 Proposition. *Die Abbildung $A \longmapsto A^{\perp\perp}$ respektiert obere und untere Grenzen und liefert einen Homomorphismus des Verbandes der Ideale aus $\mathfrak{S}$ auf den Verband $\mathfrak{P}(\mathfrak{S})$ der Polaren. Somit ist der Verband der Polaren distributiv.*

BEWEIS. Seien A, B zwei Ideale. Dann folgt

$$(A \vee B)^{\perp\perp} \supseteq A^{\perp\perp} \vee_p B^{\perp\perp} \supseteq A, B \tag{14.15}$$

und damit, man beachte, dass $A^{\perp\perp}$ eine Polare bildet,

$$(A \vee B)^{\perp\perp} = A^{\perp\perp} \vee_p B^{\perp\perp}\,. \tag{14.16}$$

Als Nächstes erhalten wir

$$(A \cap B)^{\perp\perp} = A^{\perp\perp} \cap B^{\perp\perp}\,. \tag{14.17}$$

DENN, sei $x \in A^{\perp\perp} \cap B^{\perp\perp}$ und $y \in (A \cap B)^\perp$. Dann folgt $a \in A$, $b \in B \Longrightarrow a \wedge b \in A \cap B$ und

$$a \wedge b \wedge x \wedge y = 1 \ \rightsquigarrow\ b \wedge x \wedge y \in A^\perp \cap A^{\perp\perp} = \{1\}\,.$$

Und das führt zu $\qquad x \wedge y \in B^{\perp\perp} \cap B^\perp = \{1\}$,

also zu $x \in (A \cap B)^{\perp\perp}$ – da y beliebig gewählt wurde. □

Aus der vorhergehenden Proposition folgt fast unmittelbar

$$a^{\perp\perp} \cap b^{\perp\perp} = (a \wedge b)^{\perp\perp}\,, \tag{14.18}$$

DENN: $\qquad a^{\perp\perp} \cap b^{\perp\perp} = a^{c\perp\perp} \cap b^{c\perp\perp} = (a^c \cap b^c)^{\perp\perp} = (a^c \cap b^c)^{\perp\perp}\,.$ □

Darüber hinaus erfüllt jede Polare A nach 14.3.5

$$A \cap A^\perp = \{1\} \ \text{ and } \ A \vee_p A^\perp = S\,. \tag{14.19}$$

Damit können wir als Hauptergebnis dieses Abschnitts formulieren:

14. 3. 7 Proposition. *$P(\mathfrak{S})$ bildet einen booleschen Verband. Das bedeutet insbesondere, dass $P(\mathfrak{S})$ die Gleichungen erfüllt:*

$$A \vee_p \bigwedge B_i = \bigwedge (A \vee_p B_i)\,. \tag{14.20}$$

$$A \cap \bigvee\nolimits_p B_i = \bigvee\nolimits_p (A \cap B_i)\,. \tag{14.21}$$

BEWEIS. Die genannten Gesetze gelten in jeder vollständigen booleschen Algebra, zur Erinnerung: es gilt $u \vee v = u \vee (\overline{u} \wedge v)$, also

$$u \vee v \leq u \vee w \Longleftrightarrow \overline{u} \wedge v \leq \overline{u} \wedge w\,,$$

woraus die Implikation resultiert:

$$\begin{aligned} \bigwedge (a \vee b_i) = a \vee (\overline{a} \wedge x) &\Longrightarrow \overline{a} \wedge x \leq \overline{a} \wedge b_i \quad (i \in I) \\ &\Longrightarrow \bigwedge (a \vee b_i) \leq a \vee \bigwedge b_i \quad (i \in I)\,. \end{aligned}$$

Damit sind wir aus Gründen der Dualität am Ziel. □

14.4 Filets und z-Ideale

14. 4. 1 Definition. Sei $a \in S$. Dann nennt man die Bipolare $a^{\perp\perp}$ auch die von a erzeugte *Hauptpolare*. Wir notieren die Menge aller Hauptpolaren aus $\mathfrak{S}$ mittels $PP(\mathfrak{S})$.

Unmittelbar aus 14.3.6 resultiert:

14. 4. 2 Proposition. *$\mathfrak{P}\mathfrak{P}(S)$ bildet einen Unterverband des Verbandes aller Polaren.*

Sei $f : V \longmapsto V'$ eine Verbandshomomorphismus und habe V' ein Minimum z'. Dann nennen wir die Menge $\{x \mid f(x) = z'\} =: \ker(f)$ den *Kern* von f.

14. 4. 3 Proposition. *Die Abbildung $\phi : a \longmapsto a^{\perp\perp}$ definiert einen Homomorphismus von $(S, \wedge, \vee)$ auf $\mathfrak{P}\mathfrak{P}(S)$, und die assoziierte Verbandskongruenz $\sim_f$ ist die gröbste Kongruenz von $\mathfrak{S}$ mit Kern $\{1\}$.*

BEWEIS. Offenbar ist ϕ eine Verbandskongruenz mit Kern $\{1\}$. Sei nun ρ ebenfalls eine Kongruenz mit Kern $\{1\}$. Dann folgt aus $x\,\rho\,y$ zunächst $x \wedge a = 1 \Longrightarrow (y \wedge a)\,\rho\,1 \Longrightarrow y \wedge a = 1$ und damit weiter $x^{\perp\perp} = y^{\perp\perp}$. □

14. 4. 4 Definition. Wir bezeichnen die Kongruenz $\sim_f$ als die *Filet-Kongruenz* von $\mathfrak{S}$ und deren Klassen $F(a)$ als die *Filets* von $\mathfrak{S}$.

Man halte fest: $a \sim_f b$ ist gleichbedeutend mit $a^{\perp\perp} = b^{\perp\perp}$.

14. 4. 5 Proposition. *Die Filets aus $\mathfrak{S}$ sind konvex und abgeschlossen bezüglich der Multiplikation sowie bezüglich der beiden Verbandsoperationen.*

BEWEIS. Aus (14.10) folgt

$$a^{\perp\perp} = b^{\perp\perp} \Longrightarrow a^{\perp} = b^{\perp} \Longrightarrow (ab)^{\perp\perp} = (aa)^{\perp\perp} = a^{\perp\perp} .$$

Der Rest ergibt sich aus (14.15) and (14.16). □

14. 4. 6 Proposition. *Sei F das Filet von a , dann ist F^c gleich $a^{\perp\perp}$.*

BEWEIS. Zunächst haben wir $x \in F \Longrightarrow x^{\perp\perp} = a^{\perp\perp} \Longrightarrow x \in a^{\perp\perp}$, also $F \subseteq a^{\perp\perp}$, und damit $F^c \subseteq a^{\perp\perp}$.
Sei nun $x \in a^{\perp\perp}$. Dann folgt $(x \vee a)^{\perp\perp} = x^{\perp\perp} \vee a^{\perp\perp} = a^{\perp\perp}$, also $x \vee a \in F$ und folglich $x \in F^c$, und damit $a^{\perp\perp} \subseteq F^c$. □

14. 4. 7 Definition. Als *z-Ideal* bezeichnen wir jedes Ideal, das abgeschlossen ist bezüglich $\sim_f$.

14. 4. 8 Proposition. *Sei $A \subseteq S$, Dann sind paarweise äquivalent:*

(i) *A ist ein z-Ideal.*

(ii) *A ist Vereinigung einer nach oben gerichteten Menge von Bipolaren.*

(iii) *A ist Vereinigung aller Elemente eines $\mathfrak{P}\mathfrak{P}(S)$.*

(iv) *A ist Vereinigung aller Elemente eines Unterverbandes von $\mathfrak{P}(S)$.*

(v) *A ist Vereinigung einer nach oben gerichteten Menge von Polaren.*

BEWEIS. $(i) \Longrightarrow (ii)$. Zunächst erhalten wir nach Voraussetzung von (i) die Implikation $x \in A \Longrightarrow F(x) \subseteq A \Longrightarrow C(F(x)) \subseteq A \Longrightarrow x^{\perp\perp} \subseteq A$, also $A = \bigcup x^{\perp\perp}\ (x \in A)$. Weiterhin folgt $x, y \in A \Longrightarrow x \vee y \in x^{\perp\perp} \vee y^{\perp\perp} = (x \vee y)^{\perp\perp} \subseteq A$.

$(ii) \Longrightarrow (iii)$. Sei $A = \bigcup {x_i}^{\perp\perp}\ (i \in I)$ für ein nach oben gerichtetes System ${x_i}^{\perp\perp}$. Dann erfüllt für das System aller $x^{\perp\perp} \subseteq {x_j}^{\perp\perp}\ (\exists\, j \in I)$ unsere Behauptung.

$(iii) \Longrightarrow (iv) \Longrightarrow (v)$ gilt *a fortiori.*

$(v) \Longrightarrow (i)$. Wir betrachten $A = \bigcup A_i{}^\perp$ $(i \in I)$ mit einem nach oben gerichteten System von Polaren $A_i{}^\perp$. Dann erhalten wir

$$y \sim_f x \in A_j{}^\perp \ \ (\exists\, j \in I) \Longrightarrow y \in y^{\perp\perp} \subseteq A_j{}^{\perp\perp} \subseteq A\,. \qquad \square$$

Als nächstes stellen wir eine Charakterisierung von *Filet respektierenden Kongruenzen vor.*

14. 4. 9 Proposition. *Sei h ein Homomorphismus $\mathfrak{S}$ auf $\mathfrak{T}$. Dann sind die beiden Aussagen äquivalent:*

(i) $a^\perp = b^\perp \Longrightarrow h(a)^\perp = h(b)^\perp$

(ii) $H := \ker(h)$ *ist ein z-Ideal .*

BEWEIS. $(i) \Longrightarrow (ii)$. Sei (i) erfüllt und $h(a) = e$. Dann folgt

$$\begin{aligned} b^\perp = a^\perp \ \&\ a \in H &\Longrightarrow h(b)^{\perp\perp} = h(a)^{\perp\perp} = \{e\} \\ &\Longrightarrow h(b) = e \\ &\Longrightarrow b \in H\,. \end{aligned}$$

$(ii) \Longrightarrow (i)$. Wir zeigen zunächst $h(a)^\perp \supseteq h(a^{\perp\perp})^\perp$ und damit

$$(\star) \qquad h(a)^\perp = h(a^{\perp\perp})^\perp\,.$$

WEGEN:

$$\begin{aligned} h(x) \in h(a)^\perp &\Longrightarrow h(x) \wedge h(a) = h(1) \\ &\Longrightarrow h(x \wedge a) = h(1) \\ &\Longrightarrow x \wedge a \in ker(h)) \\ &\Longrightarrow (x \wedge a)^{\perp\perp} \subseteq ker(h) \\ &\Longrightarrow x^{\perp\perp} \cap a^{\perp\perp} \subseteq ker(h) \\ &\Longrightarrow x \wedge y \in ker(h) \ \ (\forall y \in a^{\perp\perp}) \\ &\Longrightarrow h(x) \wedge h(y) = h(1) \ \ (\forall y \in a^{\perp\perp}) \\ &\Longrightarrow h(x) \in h(a^{\perp\perp})^\perp\,. \end{aligned}$$

Hiernach erhalten wir mittels $(\star)$

$$\begin{array}{rcl} a^\perp & = & b^\perp \\ & \Longrightarrow & \\ h(a)^\perp = h(a^{\perp\perp})^\perp & = & h(b^{\perp\perp})^\perp = h(b)^\perp\,, \end{array}$$

was zu beweisen war $\square$

Schließlich gilt:

14. 4. 10 Proposition. *Es sind paarweise äquivalent* (*i*) *Jedes Ideal C ist ein z-Ideal .*

(*ii*) *Jedes $a \in S$ erfüllt $a^c = a^{\perp\perp}$.*

(*iii*) *$a^{\perp\perp} = b^{\perp\perp}$ ist äquivalent zu $a^c = b^{\,c}$.*

BEWEIS. $(i) \Longrightarrow (ii)$, denn $a^c \subseteq a^{\perp\perp}$ ist stets erfüllt, und Bedingung (i) impliziert, dass jedes z-Ideal vom Typ a^c *per definitionem* $a^{\perp\perp} \subseteq a^c$ erfüllt.
$(ii) \Longrightarrow (iii)$ ist evident.
$(iii) \Longrightarrow (i)$, denn Bedingung (iii) zieht nach sich

$$b \sim_f a \in C \Longrightarrow a^{\perp\perp} = b^{\perp\perp} \Longrightarrow b^c = a^c \subseteq C \Longrightarrow b \in C\,. \qquad \square$$

14.5 Minimal prime Ideale

Minimal prime Ideale auf der einen Seite und *Polaren* auf der anderen Seite sind eng miteinander verwoben. Es zeigt sich nämlich dass jedes prime Ideal ein z-Ideal ist, also eine Vereinigung von Polaren, während auf der anderen Seite jede Polare Durchschnitt von minimal primen Idealen ist. Wir beginnen mit der zweiten Behauptung.

14. 5. 1 Proposition. *Jedes $A^\perp \neq S$ eines RNDV-Gruppoids $\mathfrak{S}$ ist Durchschnitt aller minimal primen Ideale, die A nicht enthalten.*

BEWEIS. Wir zeigen, dass $A^\perp$ der Durchschnitt aller Werte von Elementen aus A ist und hiernach, dass alle minimal primen Ideale, die C nicht enthalten, zu diesem Durchschnitt beitragen.
Da $A^\perp$ ein Ideal ist, kann $A^\perp$ bezüglich eines jeden $a \in A$ ausgedehnt werden zu einem Wert von a . Wir betrachten nun den Durchschnitt D aller Werte dieses Typs. Dann folgt $D = A^\perp$, da anderenfalls ein $x \in D\backslash A^\perp$ und ein $a \in A$ existieren würden mit $x \wedge a \in D\backslash A^\perp$, ein Widerspruch!
Schließlich trägt jedes minimal prime Ideal $P \not\supseteq A$ zu dem Durchschnitt bei wegen $a \notin P \Longrightarrow P \supseteq a^\perp \Longrightarrow P \supseteq A^\perp$. $\square$

Wie oben gezeigt liefert die Abbildung $M \longrightarrow S\backslash M$ eine Bijektion zwischen der Menge aller minimal primen Ideale und der Menge aller Ultrafilter von $\mathfrak{S}$, und diese Abbildung liefert weiter auf kanonische Weise eine Bijektion zwischen der Menge aller minimal primen Ideale aus $\mathfrak{S}$ und der Menge aller Ultrafilter des Verbandes $\mathfrak{PP}(S)$, da die Abbildung $a \longmapsto a^{\perp\perp}$ einen surjektiven Verbandshomomorphismus von $(S, \wedge, \vee)$ auf $\mathfrak{PP}(S)$ liefert mit $1 \neq a \longmapsto a^{\perp\perp} \neq \{1\}$.

14. 5. 2 Proposition. *Sei P ein* eigentlich primes Ideal *aus* $\mathfrak{S}$ *. Dann sind paarweise äquivalent:*

(i) *P ist ein minimal primes Ideal .*

(ii) $P = \bigcup x^{\perp}\ \ (x \notin P)$.

(iii) $y \in P \Longrightarrow y^{\perp} \not\subseteq P$.

BEWEIS. $(i) \Longrightarrow (ii)$. Sei P prim. Dann erhalten wir $x \notin P \Longrightarrow x^{\perp} \subseteq P$. Sei hiernach P sogar minimal prim. Dann bildet $S\backslash P$ einen Ultrafilter, weshalb zu jedem $x \in P$ ein $y \in S\backslash P$ existiert mit $x \perp y$. Folglich wird ganz P ausgeschöpft von $\bigcup x^{\perp}\ \ (x \notin P)$.

$(ii) \Longrightarrow (iii)$. Im Falle (ii) ist jedes $y \in P$ orthogonal zu mindestens einem $x \notin P$.

$(iii) \Longrightarrow (i)$. Im Falle (iii) ist die Menge $S\backslash P$ ein Ultrafilter. □

Aus dem soeben bewiesenen Ergebnis folgt noch stärker:

14. 5. 3 Proposition. *Sei C ein Ideal aus $\mathfrak{S}$ und U ein Ultrafilter aus C . Dann bildet die Menge $\bigcup x^{\perp}\ \ (x \in U)$ ein minimal primes Ideal P in $\mathfrak{S}$, und jedes minimal prime $M \not\supseteq C$ ist von dieser Art.*

BEWEIS. Sei U ein Ultrafilter aus $\mathfrak{C}$. Wir zeigen zunächst, dass die Teilmenge $V := \{x \,|\, \exists\, u \in U : x \geq u\}$ ein Ultrafilter aus $\mathfrak{S}$ ist. Das beweist dann den ersten Teil
Zu diesem Zweck seien $x \in S\backslash V$ und u beliebig aus U gewählt und damit auch Element aus V. Dann folgt $x \wedge u \in C\backslash U$, da sonst x zu V gehören müsste. Folglich existiert ein $y \in U$ mit $x \wedge u \wedge y = 1$ und damit auch ein $u \wedge y \in V$ mit $x \wedge (u \wedge y) = 1$.
Sei nun M ein minimal primes Ideal aus $\mathfrak{S}$, das C nicht enthält. Wir definieren $V := S\backslash M$ und $U = V \cap C$. So erhalten wir U als einen Ultrafilter aus C, und es bilden die Elemente $x \geq u \in U$ einen Ultrafilter in $\mathfrak{S}$, der den Ultrafilter V wegen $v \geq u \wedge v \in U$ enthält. Folglich muss nach dem ersten Teil dieser Ultrafilter gleich V sein. Es gilt aber die Implikation $u \leq v \Longrightarrow v^{\perp} \subseteq u^{\perp}$ und damit $M = \bigcup v^{\perp}\ \ (v \in V) = \bigcup u^{\perp}\ \ (u \in U)$. □

Schließlich erwähnen wir noch als eine gewisse Anwendung von 14.5.1 und als Verallgemeinerung von Proposition 14.5.2.

14. 5. 4 Korollar. *Sei P ein primes Ideal aus $\mathfrak{S}$. Dann ist der Durchschnitt D aller minimal primen Ideale, die in P enthalten sind, gleich $N := \bigcup x^{\perp}\,(x \notin P)$.*

BEWEIS. Offenbar gilt $N \subseteq D$.
Sei nun $a \in D\backslash N$. Dann folgt $a \wedge x \neq 1$ $(\forall x \notin P)$. Folglich ist in diesem Falle die Menge aller x mit $a \wedge x \neq 1$ $(x \in S\backslash P)$ ein Filter F, der $S\backslash P$ enthält und eingebettet ist in einen Ultrafilter U, der a enthält. Also wäre $S\backslash U$ ein minimal primes Ideal, enthalten in P, aber ohne a, ein Widerspruch! □

14.6 Direkte Faktoren

In diesem Abschnitt werden wir Ideale als *Unterstrukturen* betrachten. Deshalb werden wir hier Ideale auch als RNDV-Gruppoide aus $\mathfrak{S}$ bezeichnen.

14. 6. 1 Proposition. *Sei $\mathfrak{S}$ ein RNDV-Gruppoid und seien $\mathfrak{A}, \mathfrak{B}$ RNDV-Gruppoide aus $\mathfrak{S}$. Dann gilt $\mathfrak{S} = \mathfrak{A} \otimes \mathfrak{B}$ gdw. $S = A \cdot B$, $A = B^{\perp}$ und $B = A^{\perp}$.*

BEWEIS. $a \wedge b \neq 1$ würde bedeuten, dass $a \wedge b$ verschiedene Zerlegungen hat. Also ist die Bedingung notwendig.
Doch nach den Regeln der Arithmetik ist sie auch hinreichend. □

Als nächstes erhalten wir

14. 6. 2 Proposition. *Ein RNDV-Gruppoid $\mathfrak{A}$ aus $\mathfrak{S}$ ist ein direkter Faktor von $\mathfrak{S}$, wenn sie $A \cdot A^{\perp} = S$ erfüllt, und in diesem Falle erfüllt sie darüber hinaus $A = A^{\perp\perp}$.*

BEWEIS. $A \cdot A^{\perp} = S$ impliziert $A^{\perp\perp} \cdot A^{\perp} = S$ mit $A = A^{\perp\perp}$, der Rest ist klar. □

14. 6. 3 Korollar. *Sei $\mathfrak{C}$ ein RNDV-Gruppoid aus $\mathfrak{S}$. Dann ist $\mathfrak{A}^{\perp}$ in direkter Faktor von $\mathfrak{C}$ gdw. $A^{\perp} \subseteq C \subseteq A^{\perp}A^{\perp\perp}$. erfüllt ist.*

Hiernach sind wir in der Lage zu zeigen:

14. 6. 4 Proposition. *Seien $\mathfrak{A}$, $\mathfrak{B}$ direkte Faktoren von $\mathfrak{S}$. Dann gilt*

$$(\mathfrak{A} \cap \mathfrak{B})^{\perp} = \mathfrak{A}^{\perp} \vee \mathfrak{B}^{\perp} = \mathfrak{A}^{\perp} \cdot \mathfrak{B}^{\perp}.$$

BEWEIS. Sind $\mathfrak{A}$, $\mathfrak{B}$ direkte Faktoren, so erhalten wir zunächst

$$AA^{\perp} = S = BB^{\perp} \Longrightarrow (A \cap B)(A^{\perp} \vee B^{\perp}) = S$$

mit $(A \cap B) \cap (A^\perp \vee B^\perp) = \{1\}$. Deshalb gilt $(A \cap B)^\perp = A^\perp \vee_p B^\perp$, also

$$A^\perp \vee_p B^\perp \;=\; A^\perp \cdot B^\perp$$

aufgrund der Gleichungen $(A \cap B) \cdot (A^\perp B^\perp) = S$ und $A^\perp B^\perp \subseteq A^\perp \vee_p B^\perp$ sowie der Eindeutigkeit der Komplemente in distributiven Verbänden. $\square$

14. 6. 5 Korollar. *Die direkten Faktoren eines RNDV-Gruppoids bilden eine boolesche Unteralgebra des Verbandes der Polaren.*

Selbstverständlich sind linear geordnete RNDV-Gruppoide direkt unzerlegbar. Ein weniger triviales Beispiel ist das der Verbandsgruppe aller stetigen Funktionen $f : \mathbf{R} \longrightarrow \mathbf{R}$. Hier hat z. B. die Funktion $f : x \longmapsto 1$ keine Zerlegung in orthogonale Komponenten, was sich unmittelbar aus der Stetigkeit ergibt.
Hiernach wenden wir uns unendlichen direkten Produkten zu.

14. 6. 6 Definition. Sei $\mathfrak{A}_i \;\; (i \in I)$ eine Familie von RNDV-Gruppoiden aus $\mathfrak{S}$ und $\mathfrak{B}_j$ für jedes $j \in I$ das RNDV-Gruppoid, das in $\mathfrak{S}$ von der Vereinigung aller $A_i \;\; (i \neq j)$ erzeugt wird. Ist dann $\mathfrak{S}$ für jedes $i \in I$ das direkte Produkt von $\mathfrak{A}_i$ und $\mathfrak{B}_i$, so nennen wir $\mathfrak{S}$ ein inneres direktes Produkt der Faktoren $\mathfrak{A}_i$ und schreiben $\mathfrak{P} = \bigotimes \mathfrak{A}_i \;\; (i \in I)$.

Als Folge von 14.6.5 führt diese Definition nacheinander zu

14. 6. 7 Proposition. *Sei* $\mathfrak{A}_i \;\; (i \in I)$ *eine Familie von RNDV-Gruppoiden aus* $\mathfrak{S}$ *. Dann ist* $\mathfrak{S}$ *gleich* $\bigotimes \mathfrak{A}_i \;\; (i \in I)$ *gdw.* $\mathfrak{S}$ *erzeugt wird von den* $\{A_i\}$ *und zudem jedes* $i \neq j \Longrightarrow A_i \subseteq {A_j}^\perp$ *erfüllt ist.*

14. 6. 8 Proposition. $\mathfrak{S} = \bigotimes \mathfrak{A}_i \;\; (i \in I)$ *impliziert, dass jedes RNDV-Gruppoid* $\mathfrak{C}$ *aus* $\mathfrak{S}$ *direkt zerlegt wird via* $\mathfrak{C} = \bigotimes (\mathfrak{A}_i \cap \mathfrak{C}) \;\; (i \in I)$.

14. 6. 9 Proposition. *Sind* $\mathfrak{S} = \bigotimes \mathfrak{A}_i \;\; (i \in I)$ *und* $\mathfrak{S} = \bigotimes \mathfrak{B}_j \;\; (j \in J)$ *zwei innere direkte Zerlegungen von* $\mathfrak{S}$ *, so ist auch* $\bigotimes (\mathfrak{A}_i \cap \mathfrak{B}_j) \;\; (i, j \in I \times J)$ *eine innere direkte Zerlegung von* $\mathfrak{S}$.

14. 6. 10 Korollar. *Besitzt* $\mathfrak{S}$ *eine innere direkte Zerlegung in direkt unzerlegbare Komponenten, so ist diese Zerlegung eindeutig bestimmt.*

14.7 Lexikographische Erweiterungen

Ein Beispiel: Sei $\mathfrak{A}$ eine linear geordnete Gruppe und $\mathfrak{B}$ eine beliebige Verbandsgruppe. Wir setzen $(a_1, b_1) < (a_2, b_2)$ gdw. $a_1 < a_2$ oder $a_1 = a_2$ und $b_1 < b_2$. Auf diese Weise entsteht eine neue Verbandsgruppe $\mathfrak{A} \circ \mathfrak{B}$. genannt das *lexikographische Produkt* von $\mathfrak{B}$ über $\mathfrak{A}$. Offenbar bildet dann $\mathfrak{A}$ eine *primes Ideal*, das von jedem Element aus $S \backslash A$ majorisiert wird.
Analoges gilt für RNDV-Gruppoide. Man wähle etwa $(\mathbf{N}, \cdot, \mathrm{GGT}, \mathrm{KGV})$ als $\mathfrak{A}$ und eine boolesche Algebra als $\mathfrak{B}$.
Das motiviert die Definition:

14. 7. 1 Definition. Sei C eine Primideal aus $\mathfrak{S}$. Dann nennen wir $\mathfrak{S}$ *lexikographische Extension*, kurz *Lextension* von $\mathfrak{C}$, wenn jedes $s \in S \backslash C$ jedes $c \in C$ majorisiert.

Lextensionen spielen eine bedeutende Rolle in der Verbandsgruppenstrukturtheorie. Wir werden sehen, dass die Ergebnisse, wie sie formuliert sind in Bigard-Keimel-Wolfenstein, [7], mit schwachen Ausnahmen auch im Falle eines RNDV-Gruppoids gelten
Wir beginnen mit

14. 7. 2 Proposition. *Sei C ein Ideal aus $\mathfrak{S}$. Dann sind paarweise äquivalent*

(i) *$\mathfrak{S}$ ist eine Lextension von $\mathfrak{C}$.*

(ii) *C ist prim und vergleichbar mit allen Idealen L aus $\mathfrak{S}$.*

(iii) *C enthält alle von S verschiedenen Polaren aus $\mathfrak{S}$.*

(iv) *C enthält alle minimal primen Ideale aus $\mathfrak{S}$.*

(v) *Jedes $a \in S$ außerhalb von C besitzt exakt einen Wert.*

(vi) *Jedes $a \in S$ außerhalb von C erfüllt $a^\perp = \{1\}$.*

BEWEIS. $(i) \Longrightarrow (ii)$. (i) impliziert *per definitionem*, dass C prim ist. Sei nun L eine weiteres Ideal mit $L \not\subseteq C$. Dann majorisieren die Element aus $L \backslash C$ die Menge C. Daher erfüllt $C \subseteq L$.

$(ii) \Longrightarrow (iii)$. Gilt (ii), so is das Ideal C prim und vergleichbar mit allen Polaren. Somit folgt aus $A^\perp \not\subseteq C$ zunächst $A^{\perp\perp} \subseteq C$, also $A^{\perp\perp} \subseteq A^\perp$, und damit als nächstes $A \subseteq A^{\perp\perp} = \{1\}$, was $A^\perp = S$ bedeutet.

$(iii) \Longrightarrow (iv)$. Zu Erinnerung: jedes minimal prime Ideal is ist Vereinigung von Polaren.

$(iv) \Longrightarrow (v)$. Gelte $a \notin C$ und seien V und W Werte von a. Dann enthalten V und W minimal prime Ideale, die ihrerseits enthalten sind in C. Daher ist C vergleichbar mit V und auch mit W, und also enthalten in V und in W. Das bedeutet, dass V uns W eine gemeinsames primes Ideal enthalten. Also sind V und W vergleichbar.

$(v) \Longrightarrow (vi)$. Sei $1 \neq a \perp b \neq 1$ und $a \notin C$. Dann ist a assoziiert mit einem Wert $W(b)$ und b mit einem Wert $W(a)$. Aber sowohl $W(a)$ als auch $W(b)$ lassen ein Erweiterung zu dem eindeutig bestimmten $W(a \vee b)$ zu. So erhalten wir $W(a) = W(a \vee b) = W(b)$, mit Widerspruch!

$(vi) \Longrightarrow (i)$. Nach (vi) ist das Ideal C prim, gemäß 14.2.7 (vi), und im Falle $x \in S \backslash C$, $y \in C$ existieren Elemente x°, y° mit $x^\circ \notin C$ derart dass $(x \wedge y)x^\circ = x$ und $(x \wedge y)y^\circ = y$ erfüllt sind. Das aber impliziert $y^\circ = 1$ nach Annahme, und also $y \leq x$, weshalb $\mathfrak{C}$ eine Lextension von $\mathfrak{C}$ ist. □

Hiernach folgt fast unmittelbar

14. 7. 3 Lemma. *Sei* $C \subseteq H \subseteq S$ $(C, H \in C(\mathfrak{S}))$. *Dann ist* $\mathfrak{S}$ *eine Lextension von* $\mathfrak{C}$ *gdw.* $\mathfrak{S}$ *eine Lextension von* $\mathfrak{H}$ *und* $\mathfrak{H}$ *eine Lextension von* $\mathfrak{C}$ *ist.*

BEWEIS. Man beachte 14.7.2 □

14. 7. 4 Definition. Unter dem *Lexkern* eines RNDV-Gruppoids $\mathfrak{S}$, notiert mittels $\mathrm{Lex}(\mathfrak{S})$, verstehen wir die Hülle aller eigentlichen Polaren P aus $\mathfrak{S}$ in $C(\mathfrak{S})$, also, vergleiche 14.7.2 – die Hülle aller minimal primen Ideale.
Gilt $\mathrm{Lex}(\mathfrak{S}) = \mathfrak{S}$, so nennen wir $\mathfrak{S}$ *lex-einfach.*
Gilt hingegen $\mathrm{Lex}(\mathfrak{S}) \neq \mathfrak{S}$, so nennen wir $\mathfrak{S}$ ein *Lex-RNDV-Gruppoid*

Nach dieser Definition ergeben sich fast unmittelbar:

14. 7. 5 Lemma. $\mathfrak{A} \supseteq \mathfrak{B} \Longrightarrow \mathrm{Lex}(\mathfrak{A}) \supseteq \mathrm{Lex}(\mathfrak{B})$.

14. 7. 6 Lemma. $\mathfrak{S}$ *ist Lextension von* $\mathfrak{C}$ *gdw.* $\mathrm{Lex}(\mathfrak{S})$ *in* $\mathfrak{C}$ *enthalten ist.*

14. 7. 7 Lemma. *Jedes linear geordnete konvexe Unter-RNDV-Gruppoid von* $\mathfrak{S}$ *einer Kardinalität* ≥ 2 *ist ein Lex-RNDV-Gruppoid.*

Ferner ist $\mathfrak{S}$ offenbar linear geordnet gdw. $\mathrm{Lex}(\mathfrak{S}) = \{1\}$ ist.

14. 7. 8 Proposition. $\mathrm{Lex}(\mathfrak{S})$ *ist das größte lex-einfache konvexe RNDV-Gruppoid aus* $\mathfrak{S}$.

BEWEIS. Ist Lex$(\mathfrak{S})$ eine Lextension von $\mathfrak{C}$, dann ist gemäß den voran gegebenen Bemerkungen auch $\mathfrak{S}$ eine Lextension von $\mathfrak{C}$, was $C = \text{Lex}(\mathfrak{S})$ bedeutet.
Sei nun $\mathfrak{L}$ mit $L \in C(\mathfrak{S})$ lex-einfach. Dann gilt – man beachte 14.7.2 (ii) – Lex$(\mathfrak{S}) \supseteq L$ oder Lex$(\mathfrak{S}) \subseteq L$. Es kann aber nicht gelten Lex$(\mathfrak{S}) \subset L$ da L lex-einfach ist. □

Als nächstes zeigen wir

14. 7. 9 Proposition. *Sei $\mathfrak{a}^c$ das von a erzeugte RNDV-Gruppoid. Dann ist $\mathfrak{a}^c$ ein Lex-RNDV-Gruppoid gdw. a genau einen Wert besitzt.*

BEWEIS. Sei $\mathfrak{a}^c$ ein Lex-RNDV-Gruppoid. Dann gehört a zu $\mathfrak{a}^c \backslash \text{Lex}(\mathfrak{a}^c)$ und hat folglich genau einen Wert in $\mathfrak{a}^c$. Daher hat in diesem Falle a auch nur einen Wert in $\mathfrak{S}$, man beachte 14.2.9.
Habe nun umgekehrt a nur einen Wert in $\mathfrak{S}$. Dann hat a auch in $\mathfrak{a}^c$ nur einen Wert W. Dann aber ist W Wert auch aller anderen Elemente aus $a^c \backslash W$. Folglich besitzt in $\mathfrak{a}^c$ jedes $V \in \text{val}(k)$ $(k \notin W)$ eine Ausdehnung zu W. Damit hat dann auch jedes $k \notin W$ exakt einen Wert, weshalb $\mathfrak{a}^c$ nach 14.7.2 (v) ein Lex-RNDV-Gruppoid ist. □

14. 7. 10 Proposition. *Jedes Paar von Lex-RNDV-Gruppoiden $\mathfrak{A}$, $\mathfrak{B}$ aus $\mathfrak{S}$ ist orthogonal oder vergleichbar.*

BEWEIS. Angenommen, es wären $\mathfrak{A}$ und $\mathfrak{B}$ weder vergleichbar noch orthogonal. Dann existierten zwei Elemente $a \in A \backslash B$ und $b \in B \backslash A$ mit $a \wedge b > 1$. Wir zeigen, dass dies zu $\mathfrak{a}^c \subseteq \mathfrak{b}^c$ oder aber zu $\mathfrak{b}^c \subseteq \mathfrak{a}^c$ führt.
Nach 14.7.9 sind sowohl $\mathfrak{a}^c$ als auch $\mathfrak{b}^c$ Lex-RNDV-Gruppoide. Daher gäbe es zu a bzw. b in $\mathfrak{S}$ Werte C bzw. D mit $b \in B \subseteq C \in \text{val}(a)$ bzw. $a \in A \subseteq D \in \text{val}(b)$, und darüber hinaus enthielten diese Werte ein gemeinsames primes Ideal M, z. B. einen Wert zu $a \wedge b$. Daraus würde dann $C \subseteq D \vee D \subseteq C$ resultieren, trotz $C \not\supseteq \{a, b\} \not\subseteq D$. □

Man beachte, nach 14.7.10 vermag man von der lokalen Struktur eines $\mathfrak{s}^c$ auf die globale Struktur von $\mathfrak{S}$ zu schließen und umgekehrt von der globalen Struktur von $\mathfrak{S}$ auf die lokale Struktur dieses $\mathfrak{s}^c$.

14. 7. 11 Proposition. *Sei $\mathfrak{A}$ ein Lex-RNDV-Gruppoid aus $\mathfrak{S}$. Dann gilt*

$$s \notin A \times A^{\perp} \implies s > a \ (\forall\, a \in A)\,.$$

BEWEIS. Sei L der Lex-Kern von A, $s \notin A \times A^\perp$ sowie $t \in A\backslash L$ und sei $R(s,t,s^\circ,t^\circ)$. Dann folgt wegen $t = (s \wedge t)t^\circ \notin L$ und der Annahme $s \wedge t \in L$ zunächst $t^\circ \in A\backslash L$ und hiernach weiter:

$$\begin{array}{lrcl} & t^\circ \wedge (s^\circ \wedge a) & = & 1 \ (\forall\, a \in A) \\ \Longrightarrow & s^\circ \wedge a & = & 1 \ (\forall\, a \in A) \\ \Longrightarrow & s^\circ & \in & A^\perp \\ \Longrightarrow & s & \in & A \times A^\perp\,, \end{array}$$

mit Widerspruch. Folglich gilt $s \geq s \wedge t > L$, also $s > L$ für alle $s \notin A \times A^\perp$. Bleibt zu zeigen $s \geq t \in A\backslash L$. Hierzu betrachten wir s°. Da t und damit auch $s \wedge t$ zu A gehören, zur Erinnerung $s \notin A \times A^\perp$, kann das Element s° nicht zu $A \times A^\perp$ gehören. Folglich muss t° zu L gehören, da sonst $t^\circ \wedge s^\circ \neq 1$ folgen würde. Auf diese Weise erhalten wir $s^\circ \geq t^\circ \rightsquigarrow t^\circ = 1$, also $s \geq t$ und damit $s > A$. □

14. 7. 12 Korollar. *Jedes Lex-RNDV-Gruppoid $\mathfrak{A}$, das nach oben durch kein $s \notin A$ beschränkt ist, ist ein direkter Faktor des RNDV-Gruppoids $\mathfrak{S}$.*

14. 7. 13 Proposition. *Seien A und B zwei Ideale aus $\mathfrak{S}$ und sei A echt enthalten in B. Dann sind paarweise äquivalent:*

(*i*) *$\mathfrak{B}$ ist eine Lextension von $\mathfrak{A}$.*

(*ii*) *$\mathfrak{B}^{\perp\perp}$ ist eine Lextension von $\mathfrak{A}$.*

(*iii*) *Für alle b aus $B\backslash A$ gilt $\mathfrak{b}^{c\perp} = b^\perp = B^\perp$.*

BEWEIS. $(i) \Longrightarrow (ii)$. Gilt $B^{\perp\perp} = B$, so ist nichts zu zeigen. Anderenfalls, sei $1 < x \in B^{\perp\perp}\backslash B$ erfüllt. Dann kann x nicht zu $B \times B^\perp$ gehören, beachte $B \times B^\perp = B \vee B^\perp$ und

$$(B \vee B^\perp) \cap B^{\perp\perp} = (B \cap B^{\perp\perp}) \vee (B^\perp \cap B^{\perp\perp}) = B \cap B^{\perp\perp}.$$

Folglich gilt $x > B$, also ist $\mathfrak{B}^{\perp\perp}$ eine Lextension von $\mathfrak{B}$ und damit auch von $\mathfrak{A}$.

$(ii) \Longrightarrow (iii)$. Sei $\mathfrak{B}^{\perp\perp}$ eine Lextension von $\mathfrak{A}$. Dann ist auch $\mathfrak{B}$ eine Lextension von $\mathfrak{A}$. Denn gilt $x \in B\backslash A$ und $x \in b^\perp$, so erfüllt jedes $y \in B$ die Implikation $b \perp x \Longrightarrow b \perp y \wedge x \Longrightarrow y \wedge x = 1$ und damit $x \in B^\perp$. Somit ist $\mathfrak{B}$ nach 14.7.2 (*vi*), Lextension von $\mathfrak{A}$.

$(iii) \Longrightarrow (i)$. Sei $b \in B \backslash A$, $x \in B$ und $b \wedge x = 1$. Dann folgt nach (iii) $x \in B \cap b^{\perp} = B \cap B^{\perp} = \{1\}$. Somit gilt (i) nach 14.7.2 (vi). □

14. 7. 14 Korollar. *Ist $\mathfrak{B}$ eine Lextension von $\mathfrak{A}$ in $\mathfrak{S}$ dann ist $\overline{\overline{\mathfrak{B}}}$ eine maximale Lextension von $\mathfrak{A}$ in $\mathfrak{S}$.*

BEWEIS. Nach 14.7.10 bilden die Lextensionen $\mathfrak{C}$ von $\mathfrak{A}$ mit $\mathfrak{B} \subseteq \mathfrak{C}$ eine Kette. Daher existiert höchstens eine maximale Lextension des betrachteten Typs. Sei nun $B^{\perp\perp} \subseteq C$ erfüllt und $\mathfrak{C}$ eine Lextension von $\mathfrak{A}$. Dann erhalten wir nach 14.7.13 (iii) zunächst $B^{\perp} = C^{\perp}$ und damit dann weiter die Inklusion $B^{\perp\perp} \subseteq C \subseteq C^{\perp\perp} = B^{\perp\perp}$. □

14. 7. 15 Proposition. *Sei $\mathfrak{B}$ eine Lextension von $\mathfrak{A} \neq \{1\}$ in $\mathfrak{S}$. Dann folgt $A^{\perp} = B^{\perp}$.*

BEWEIS. $B^{\perp} \subseteq A^{\perp}$ gilt *a fortiori.*
Sei nun $x \in A^{\perp}$ & $b \in B$. Dann erhalten wir $b \wedge x \in B$ und $a \wedge x \wedge b = 1$ für alle a aus A, also $b \wedge x \in A^{\perp} \cap B$. Es gehört aber $b \wedge x$ zu A, da $b \wedge x \in B \backslash A$ nach sich zöge $b \wedge x \geq a \in A$ und damit $A = \{1\}$, mit Widerspruch!
Daher erhalten wir $b \wedge x \in A$ und somit $b \wedge x \in A \cap A^{\perp}$, also $b \wedge x = 1$, was $x \in B^{\perp}$ bedeutet, woraus schließlich $A^{\perp} \subseteq B^{\perp}$ resultiert. □

Erneut sei betont:

14. 7. 16 Korollar. *Im Falle $\{1\} \neq A \in C(\mathfrak{S})$ bilden die Lextensionen von $\mathfrak{A}$ eine Kette mit Maximum $\mathfrak{A}^{\perp\perp}$.*

Im weiteren studieren wir die Relationen zwischen den linear geordneten Idealen aus $\mathfrak{S}$ auf der einen Seite und den Polaren und minimal primen Idealen aus $\mathfrak{S}$ auf der anderen Seite. Hier erhalten wir vorweg:

14. 7. 17 Proposition. *Sei P eine eigentliche Polare aus $\mathfrak{S}$. Dann sind paarweise äquivalent*

(i) *P ist linear geordnet.*

(ii) *P ist maximal in der Menge der linear geordneten Ideale.*

(iii) *$P^{\perp}$ ist prim.*

(iv) *$P^{\perp}$ ist minimal prim.*

(v) *$P^{\perp}$ ist eine maximale Polare.*

(vi) *P is a minimale Polare.*

BEWEIS. $(i) \Longrightarrow (ii)$. Sei (i) erfüllt und C ein linear geordnetes Ober-Ideal von P. Dann ist $\mathfrak{C}$ nach 14.7.7 eine Lextension von $\mathfrak{P}$ mit $\overline{\overline{\mathfrak{C}}} \supseteq \overline{\overline{\mathfrak{P}}}$, und es ist gemäß 14.7.13 zusammen mit $\mathfrak{C}$ auch $\overline{\overline{\mathfrak{C}}}$ eine Lextension von $\mathfrak{P}$ und gemäß 14.7.16 die Bipolare $\overline{\overline{\mathfrak{P}}}$ eine maximale Lextension von $\mathfrak{P}$ in $\mathfrak{S}$. Das liefert dann $C^{\perp\perp} \supseteq P^{\perp\perp} = P \rightsquigarrow C = P$.

$(ii) \Longrightarrow (iii)$. Sei $R(x,y,x^\circ,y^\circ)$ und $x \wedge y \in P^\perp$, aber x°, $y^\circ \notin P^\perp$. Dann existieren Elemente a, $b \in P$ mit $1 \neq x^\circ \wedge a \in P$ & $1 \neq y^\circ \wedge b \in P$. Da P linear geordnet ist, folgt hieraus weiter $x^\circ \wedge y^\circ > 1$, mit Widerspruch! Also ist $P^\perp$ prim.

$(iii) \Longrightarrow (iv)$, da – gemäß 14.5.1 – jede Polare Durchschnitt von minimal primen Idealen ist.

$(iv) \Longrightarrow (v)$. Sei $P^\perp$ minimal prim und $P^\perp \subseteq Q^\perp \subseteq M$ mit einem minimal primen Ideal M erfüllt. Dann folgt $P^\perp = Q^\perp$.

$(v) \Longrightarrow (vi)$. Beachte die Antitonie von $A \longmapsto A^\perp$ in der booleschen Algebra der Polaren.

$(vi) \Longrightarrow (i)$. Sei x, $y \in P$ erfüllt und gelte $R(x,y,x^\circ,y^\circ)$. Dann impliziert $x^\circ \neq 1$ zunächst $P = x^{\circ\perp\perp}$, da P minimal ist. Und das führt weiter zu $y^\circ \in x^{\circ\perp} \cap x^{\circ\perp\perp}$, also zu $y^\circ = 1$ und damit zu $y \leq x$. $\square$

Als nächstes stellen wir vor:

14. 7. 18 Proposition. *Sei C eine konvexe Menge aus $\mathfrak{S}$ mit $1 \in C$. Dann sind paarweise äquivalent:*

- (i) *C ist linear geordnet.*
- (ii) *$C^{\perp\perp}$ ist linear geordnet.*
- (iii) *C^c ist linear geordnet.*

BEWEIS. $(i) \Longrightarrow (ii)$. Im Falle $C^{\perp\perp} = \{1\}$ sind wir am Ziel. Anderenfalls sei $1 \neq x \in C^{\perp\perp}$ erfüllt. Dann kann x nicht zu $C^\perp$ gehören. Folglich existiert bezüglich x zumindest ein $c_x \in C$ mit $x \wedge c_x \neq 1$. Daher ist kein Paar von Elementen aus $C^{\perp\perp}$ orthogonal, da C linear geordnet ist. Folglich führt $R(a,b,a^\circ,b^\circ)$ zu $a^\circ = 1 \vee b^\circ = 1$. Es sind aber je zwei Elemente aus $C^{\perp\perp}$ vergleichbar.

$(ii) \Longrightarrow (iii) \Longrightarrow (i)$ ist evident. $\square$

14. 7. 19 Korollar. *Die linear geordneten Polaren aus $\mathfrak{S}$ sind exakt die maximalen konvexen Ketten.*

BEWEIS. Sei P eine linear geordnete Polare und $C \supseteq P$ eine maximale konvexe Kette. Dann erhalten wir $C = C^{\perp\perp}$ nach 14.7.18 und $C = P$ nach 14.7.17, da P eine Polare und $C = C^{\perp\perp} \supseteq P$ eine minimale Polare ist. □

Damit können wir formulieren:

14. 7. 20 Korollar. *Sei C eine maximale und konvexe Kette aus $\mathfrak{S}$ ohne obere Schranke außerhalb von C. Dann ist $\mathfrak{C}$ ein direkter Faktor von $\mathfrak{S}$.*

BEWEIS. Man beachte 14.7.12 □

Als ein Beispiel geben wir $\{p^n\}$ $(n \in \mathbf{N}^0)$ mit primem p als eine maximale konvexe Kette von $(\mathbf{N}, \cdot, \mathrm{GGT}, \mathrm{KGV})$.

14. 7. 21 Korollar. *Für Elemente $a \neq 1$ sind paarweise äquivalent*

(i) *Das Intervall $[\,1, a\,]$ ist linear geordnet.*

(ii) *$a^{\perp\perp}$ ist linear geordnet.*

(iii) *a^c ist linear geordnet.*

Dies suggeriert zu erklären:

14. 7. 22 Definition. Wir nennen $a \in S$ *basisch* in $\mathfrak{S}$, wenn $[\,1, a\,]$ linear geordnet ist.

Offenbar ist jedes Paar basischer Elemente orthogonal oder vergleichbar. Ferner hat jedes basische Element nach 14.7.9 und 14.7.2 exakt einen Wert. Offenbar sind in $(\mathbf{N}, \cdot, \mathrm{GGT}, \mathrm{KGV})$ exakt die Primzahlpotenzen basisch.

14.8 RNDV-Gruppoide mit einer Basis

In diesem Abschnitt studieren wir $(\mathbf{N}, \cdot, \mathrm{GGT}, \mathrm{KGV})$ „in Verallgemeinerungen".

14. 8. 1 Definition. Sei B eine Teilmenge von S. Dann nennen wir B *orthogonal*, wenn B den Bedingungen genügt:

(i) $1 \notin B$.

(ii) Je zwei Elemente aus B sind orthogonal.

Offenbar gilt nach Zorn:

14. 8. 2 Lemma. *Jede orthogonale Untermenge von $\mathfrak{S}$ besitzt eine Ausdehnung zu einer maximalen orthogonalen Untermenge.*

Weiter erhalten wir ohne Schwierigkeiten:

14. 8. 3 Lemma. *Eine orthogonale Untermenge U ist genau dann maximal, wenn $U^{\perp} = \{e\}$ bzw. äquivalent hierzu $U^{\perp\perp} = S$ erfüllt ist.*

14. 8. 4 Definition. Unter einer *Basis* verstehen wir eine maximale orthogonale Untermenge B, bestehend aus lauter basischen Elementen von S. Weiterhin nennen wir $\mathfrak{S}$ basisch, wenn $\mathfrak{S}$ eine Basis besitzt.

Als Beispiel betrachte man $(\mathbf{N}^0, \cdot, \text{ GGT })$. Eine Basis bilden hier alle Mengen $\{p^n\}_{(p\ prim,\ 1 \leq n \in \mathbf{N})}$.

Die Menge aller Basen ist aufs engste verknüpft mit der Menge aller Polaren aus $\mathfrak{S}$.

14. 8. 5 Proposition. *Es sind paarweise äquivalent*

- (i) *$\mathfrak{S}$ besitzt eine Basis.*
- (ii) *Jedes $a > 1$ majorisiert mindestens ein basisches Element.*
- (iii) *Die Algebra der Polaren ist atomar.*
- (iv) *Jede Polare $\neq S$ ist Durchschnitt maximaler Polaren.*
- (v) *$\{1\}$ ist Durchschnitt maximaler Polaren.*

BEWEIS. $(i) \Longrightarrow (ii)$. Sei B eine Basis und a nicht aus B. Dann gilt für mindestens ein $b \in B$ die Beziehung $a \not\perp b$, also ist $1 \neq a \wedge b < b$ und deshalb $(a \wedge b)^{\perp\perp} \subseteq b^{\perp\perp}$ erfüllt. Folglich ist $(a \wedge b)^{\perp\perp}$ linear geordnet und $a \wedge b$ somit basisch.

$(ii) \Longrightarrow (iii)$. Sei A eine Polare und b ein basisches Element aus A. Dann gilt $b^{\perp\perp} \subseteq A$, und es ist $b^{\perp\perp}$ eine minimale Polare, wegen 14.7.17.

$(iii) \Longrightarrow (iv)$. Sei $\mathfrak{B}$ ein beliebige boolesche Algebra. Dann liefert die Beziehung

$$0 \neq a < \bigwedge m_i \text{ mit } m_i = \overline{p_i} \text{ und } p_i$$

ein Atom $p \leq \bigwedge(m_i \wedge \overline{a})$ mit dem *Co-Atom* $\overline{p} \geq a$ & $\overline{p} \not\geq \bigwedge m_i$. Und das liefert $a = \bigwedge m_i$.

$(iv) \Longrightarrow (v)$ *a fortiori.*

$(v) \Longrightarrow (i)$. Sei P_i $(i \in I)$ die Familie aller maximalen Polaren. Dann ist jedes ${P_i}^{\perp}$ ein linear geordnetes ${b_i}^{\perp\perp}$. Folglich ist jedes b_i basisch und es sind je zwei verschiedene Elemente b_i , b_j orthogonal.

Bleibt zu zeigen, dass die Menge dieser Elemente $\{b_i\}$ eine Basis bildet, also dass $\{b_i\}^{\perp} = \{1\}$ erfüllt ist.

Zu diesem Zweck sei $x \in b_i{}^\perp$ $(\forall i \in I)$ angenommen. Dann folgt $b_i{}^\perp = P_i$, wegen $b_i{}^\perp \supseteq P_i{}^{\perp\perp} = P_i$, und somit $x \in \bigcap b_i{}^\perp = \bigcap P_i = \{1\}$. □

14.8.5 (ii) liefert sofort:

14. 8. 6 Korollar. *Ein RNDV-Gruppoid $\mathfrak{S}$ ist basisch gdw. seine konvexen RNDV-Unter-Gruppoide basisch sind.*

Maximale Polaren sind minimal prime Ideale. Somit sagt uns 14.8.5, dass in einem jeden RNDV-Gruppoid mit Basis eine Familie von primen Idealen mit Durchschnitt $\{1\}$ existiert. Dieses Ergebnis wird verschärft durch

14. 8. 7 Proposition. *Ein RNDV-Gruppoid $\mathfrak{S}$ ist basisch gdw. eine minimale Familie von primen Idealen P_i $(i \in I)$ existiert mit*

$$\bigcap P_i \ (i \in I) = \{1\} \ \textit{und} \ \bigcap P_i \ (i \neq j \in I) \neq \{1\}\,.$$

BEWEIS. **(a)** Sei die Bedingung erfüllt.
Prime Ideale P erfüllen $P^{\perp\perp} = P$ oder $P^{\perp\perp} = S$. Denn wegen $P \subseteq P^{\perp\perp}$ ist die Bipolare $P^{\perp\perp}$ prim, beachte 14.2.7. Daher ist $P^{\perp\perp}$ gleich S oder s ist – nach 14.7.17 – $P^{\perp\perp}$ eine maximale Polare und deshalb ein minimal primes Ideal aus $\mathfrak{S}$.
Sei hiernach $\mathcal{F}$ eine minimale Familie im Sinne des Satzes mit $P \in \mathcal{F}$, und sei D der Durchschnitt aller $Q \neq P$ aus $\mathcal{F}$. Dann folgt wegen $D \cap P = \{1\}$ zunächst $P^\perp \supseteq D \neq 1$, also $P = P^{\perp\perp} \neq S$, woraus sich weiter gemäß 14.7.17 ergibt, dass P eine maximale Polare ist. Folglich ist $\mathcal{F}$ eine Unterfamilie aus der Familie aller maximalen Polaren aus $\mathfrak{S}$.
Sei auf der anderen Seite C eine maximal Polare und damit zugleich ein minimal primes Ideal. Dann existiert ein Element a mit $C = a^\perp$ und ein $P \in \mathcal{F}$ mit $a \notin P$. Das aber impliziert $C = a^\perp \subseteq P$, also $C = P$, da C maximal gewählt ist. Somit ist P eine Polare und folglich hat $\mathfrak{S}$ eine Basis.
(b) Habe hiernach $\mathfrak{S}$ eine Basis. Dann ist nach 14.8.5 (v) die Menge $\{1\}$ gleich dem Durchschnitt aller maximalen Polaren, weshalb nur zu zeigen bleibt, dass die Familie aller maximalen Polaren minimal ist im Sinne des Satzes. Das aber folgt da die b_i aus 14.8.5 $(v) \Longrightarrow (i)$ eine Basis bilden, also der Bedingung $b_i \in b_j{}^\perp$ $(j \neq i \in I)$ genügen und somit $b_i \in P_j{}^{\perp\perp} = P_j$ $(j \neq i \in I)$ erfüllen. □

14.9 Ortho-finite RNDV-Gruppoide

14. 9. 1 Definition. Sei $\mathfrak{S}$ ein RNDV-Gruppoid. Wir sagen, das Element a habe die *Höhe* n, wenn es unterhalb von $a^{\perp\perp}$ eine maximale Kette von Polaren der Länge n gibt.

Nach den Regeln der *Modularität* haben alle maximalen Ketten die Länge n, falls nur eine dieser Ketten diese Bedingung erfüllt. .

14. 9. 2 Proposition. *Für die Elemente aus $\mathfrak{S}$ sind paarweise äquivalent:*

(i) *a hat die Höhe n .*

(ii) *Es existiert eine maximale Kette*
$\{1\} \subset P_1 \subset P_2 \ldots \subset P_n = a^{\perp\perp}$ von Polaren P_i unterhalb $a^{\perp\perp}$.

(iii) *$a^{\perp\perp}$ hat eine Basis der Länge n .*

(iv) *a liegt in allen minimal primen Idealen bis auf höchstens n viele.*

(v) *Ist M eine orthogonale Menge unterhalb von a , so enthält M höchstens n Elemente.*

BEWEIS. $(i) \Longrightarrow (ii)$ gilt nach Definition.

$(ii) \Longrightarrow (iii)$. Gelte (ii) und sei $\{1\} \subset P_1 \subset \cdots \subset P_n = a^{\perp\perp}$ eine Kette im Sinne des Satzes. Dann sind die Mengen $P_{i+1} \cap P_i{}^{\perp}$ paarweise 1-disjunkt und daher linear geordnet. Denn wären die Elemente $x\,,\, y \in P_{i+1} \cap P_i{}^{\perp}$ unvergleichbar, so lägen x° und y° in $P_{i+1} \cap P_i{}^{\perp}$, und es läge die von $P_i{}^{\perp}$ und x° erzeugte Polare wegen $P_i \subset (P_i \cup \{x\})^{\perp\perp} \subseteq P_{i+1} \backslash \{y\}$, streng zwischen P_i und P_{i+1}, man beachte dass $y \neq 1$ zu $P_i{}^{\perp}$ gehört und deshalb nicht zu $P_i{}^{\perp\perp}$.

$(iii) \Longrightarrow (iv)$. Wir zeigen ein wenig mehr, nämlich: Sei $\{a_1, \ldots, a_n\}$ eine Basis von $a^{\perp\perp}$. Dann gehört a exakt nicht zu den maximalen Polaren, also minimal primen Idealen $a_i{}^{\perp}$ $(1 \leq i \leq n)$.
Sei hiernach $\{a_1, \ldots, a_n\}$ eine Basis von $a^{\perp\perp}$. Dann ist z. B. der Träger des von $\{a_2, \ldots, a_n\}$ erzeugten Unter-RNDV-Gruppoids gleich $a_1^{\perp}$, also eine Polare, weshalb im Falle $a \in a_1^{\perp}$ folgen muss $a^{\perp\perp} \subseteq a_1^{\perp}$, mit Widerspruch! Somit kann a zu keinem der $a_i^{\perp}$ gehören, die ja maximale Polaren, also minimal prime Ideale sind.
Ist aber M minimal prim und $a \notin M$, so folgt $a^{\perp} \subseteq M$, und es kann kein a_i zu M gehören, da $a_i \in M \Longrightarrow a_i^{\perp\perp} = M$ zu $a \in a^{\perp\perp} \subseteq a_i^{\perp}$ führen würde.

$(iv) \Longrightarrow (v)$. Seien $a_1, \ldots, a_m \leq a$ paarweise orthogonal. Wir bilden die Kette

$$a_1{}^\perp, (a_1 \vee a_2)^\perp, \ldots, (a_1 \vee a_2 \vee \ldots \vee a_m)^\perp .$$

Diese Kette liefert – analog zum Procedere unter $(ii) \Longrightarrow (iii)$ – m paarweise orthogonale Basiselemente mit einer oberen Schranke, etwa b. Dann können wir aber wie unter $(iii) \Longrightarrow (iv)$ schließen, dass b und folglich auch a nicht exakt zu m minimal primen Idealen gehört, was $m \leq n$ bedeutet.

$(v) \Longrightarrow (i)$, da eine Kette im Sinne des Satzes von größerer Länge als n zu mehr als n vielen paarweise orthogonalen Elementen unterhalb von a führen würde, man konsultiere den Beweis von $(ii) \Longrightarrow (iii)$. □

Die nächste Proposition betrifft den Fall eines globalen n.

14. 9. 3 Proposition. *In $\mathfrak{S}$ sind paarweise äquivalent:*

- (i) *a ist von endlicher Höhe.*
- (ii) *Jedes z-Ideal Z erfüllt $a \in Z^{\perp\perp} \Longrightarrow a \in Z$.*
- (iii) *Jede nach oben beschränkte orthogonale Menge ist endlich.*
- (iv) *Die Menge der speziellen Polaren $P \supseteq a^{\perp\perp}$ erfüllt die Maximalbedingung.*
- (v) *Die Menge der in $a^{\perp\perp}$ enthaltenen Polaren, ist endlich.*

BEWEIS. $(i) \Longrightarrow (ii)$. Gehöre a zu $Z^{\perp\perp}$ und sei $\{a_1, \ldots, a_n\}$ eine Basis zu $a^{\perp\perp}$. Dann gilt $a_i \in Z^{\perp\perp}$ $(1 \leq i \leq n)$ und damit $a_i \notin Z^\perp$. Folglich existiert zu jedem $1 \leq i \leq n$ ein $z_i \in Z$ mit $1 < a_i \wedge z_i$. Es ist B aber basisch und damit $a_i{}^{\perp\perp}$ eine minimale Polare. Dies führt als nächstes zu $a_i \in a_i{}^{\perp\perp} = (a_i \wedge z_i)^{\perp\perp} \subseteq z_i{}^{\perp\perp} \subseteq Z$. Auf diese Weise erhalten wir $a \in a^{\perp\perp} = (a_1 \vee \ldots \vee a_n)^{\perp\perp} \subseteq Z$.

$(ii) \Longrightarrow (iii)$. Sei $\{a_i\}$ $(i \in I)$ maximal in der Menge aller orthogonalen Mengen unterhalb von a. Wir betrachten die Vereinigung Z aller $b^{\perp\perp}$ mit $b \in \bigvee a_i{}^c$. Dann ist Z ein z-Ideal, erzeugt von den Elementen a_i, und aus $a^{\perp\perp} \supseteq (\bigvee a_i{}^c)^{\perp\perp}$ folgt $a^{\perp\perp} = (\bigvee a_i{}^c)^{\perp\perp}$, da die Polaren eine boolesche Algebra bilden. Das führt dann zu $a \in a^{\perp\perp} = (\bigvee a_i{}^c)^{\perp\perp} = Z^{\perp\perp} \Longrightarrow a \in Z$. Somit existiert ein Element $b \in \bigvee a_i{}^c$ mit $a \in b^{\perp\perp}$. Andererseits existiert eine finite Untermenge J in I mit $b \in \bigvee a_j{}^c$ $(j \in J)$. Das aber impliziert $I = J$. Denn, wäre a_k ein a_i mit $k \notin J$, so würde auf der einen Seite folgen $b \in a_k{}^\perp$ und damit auf der anderen Seite $a \in b^{\perp\perp} \subseteq a_k{}^\perp$, also $a_k \in a^\perp \cap a^{\perp\perp}$.

$(iii) \Longrightarrow (iv)$. Wie oben gezeigt, liefert jede Kette von eigentlichen Polaren eine orthogonale Menge von der Anzahl der Glieder dieser Kette.

$(iv) \Longrightarrow (v)$. Die Menge der Polaren eines RNDV-Gruppoids, also auch von $a^{\perp\perp}$, bildet eine boolesche Algebra, und das Komplement einer maximalen Polare ist eine minimale Polare. Das bedeutet: gäbe es unendlich viele minimale und damit atomare Polaren, so existierte auch eine unendliche aufsteigende Kette von Polaren – mit Widerspruch!

$(v) \Longrightarrow (i)$ ist evident. □

14. 9. 4 Korollar. *Für $\mathfrak{S}$ sind paarweise äquivalent:*

(i) *Jedes a ist von endlicher Höhe.*

(ii) *Jede nach oben beschränkte orthogonale Menge ist endlich.*

(iii) *Jedes z-Ideal ist in Polare.*

Angeregt durch 14.9.3 erklären wir als nächstes:

14. 9. 5 Definition. $\mathfrak{S}$ heiße *orthofinit*, wenn jede nach oben beschränkte orthogonale Menge endlich ist.

14. 9. 6 Proposition. *Für $\mathfrak{S}$ sind paarweise äquivalent:*

(i) *$\mathfrak{S}$ besitzt eine endliche Basis.*

(ii) *$\mathfrak{S}$ ist gleich einem $a^{\perp\perp}$ mit einem a von endlicher Höhe.*

(iii) *$\mathfrak{S}$ hat nur endlich viele minimal prime Ideale.*

(iv) *$\mathfrak{S}$ hat nur endlich viele Polaren.*

(v) *Jede orthogonale Menge aus $\mathfrak{S}$ ist endlich.*

BEWEIS. $(i) \Longrightarrow (ii)$. Man konsultiere die vorauf gegangenen Entwicklungen und 14.9.2.

$(ii) \Longrightarrow (iii)$ resultiert ebenfalls aus 14.9.2.

$(iii) \Longrightarrow (iv)$ folgt daraus, dass jede Polare Durchschnitt von minimal primen Idealen ist.

$(iv) \Longrightarrow (v)$, da zusammen mit den Elementen a_i auch die Bipolaren ${a_i}^{\perp\perp}$ paarweise orthogonal sind.

$(v) \Longrightarrow (i)$. Man wähle eine maximale orthogonale Menge $\{a_i\}$ $(1 \leq i \leq n)$ und setze $a_1 \vee \ldots \vee a_n =: a$. Dann gilt $S = a^{\perp\perp}$ – nach 14.9.2. □

14.10 Projizierbare RNDV-Gruppoide

14. 10. 1 Definition. $\mathfrak{S}$ heiße *projizierbar*, wenn $\mathfrak{S}$ der Gleichung genügt:

$$\text{(PR)} \qquad a^\perp \times a^{\perp\perp} \;=\; S \;\; (\forall a \in S)\,,$$

also, wenn $\mathfrak{S}$ auf jedes $a^{\perp\perp}$ projiziert werden kann.
Weiterhin nennen wir $\mathfrak{S}$ *semi-projizierbar*, wenn $\mathfrak{S}$ der Gleichung genügt:

$$\text{(SP)} \qquad (a \wedge b)^\perp \;=\; a^\perp \vee b^\perp\,.$$

14. 10. 2 Proposition. *Ist $\mathfrak{S}$ projizierbar, so ist $\mathfrak{S}$ auch semiprojizierbar.*

BEWEIS. Wähle Elemente $a\,,\, b \in S$. Dann gilt $a^\perp \times a^{\perp\perp} = S = b^\perp \times b^{\perp\perp}$ und damit $a^\perp \vee a^{\perp\perp} = S = b^\perp \vee b^{\perp\perp}$. Das liefert

$$(a^\perp \vee b^\perp) \vee (a^{\perp\perp} \cap b^{\perp\perp}) = S = (a^\perp \vee b^\perp) \vee (a \wedge b)^{\perp\perp}$$

mit 1-disjunkten Komponenten, also $S = (a^\perp \vee b^\perp) \cdot (a \wedge b)^{\perp\perp}$ und damit $a^\perp \vee b^\perp = (a \wedge b)^{\perp\perp\perp} = (a \wedge b)^\perp$. □

14. 10. 3 Proposition. *Ist $\mathfrak{S}$ assoziativ und projizierbar, so ist $\mathfrak{S}$ auch* repräsentierbar.

BEWEIS. Nach Definition gilt $s \cdot a^\perp = a^\perp \cdot s$. Wir betrachten nun

$$xay \wedge ubv = x(a \wedge b)a^\circ y \wedge u(a \wedge b)b^\circ v \text{ mit } a^\circ \in b^\perp, b^\circ \in a^\perp\,.$$

Dann gibt es Elemente $a^* \in b^\perp, b^* \in a^\perp$ mit

$$\begin{aligned} xay \wedge ubv &= x(a \wedge b)ya^* \wedge u(a \wedge b)vb^* \\ &\leq (x(a \wedge b)y \vee u(a \wedge b)v)(a^* \wedge b^*) \\ &\leq xby \vee uav\,. \end{aligned}$$

.
Damit sind wir nach 12.2.6 am Ziel. □

Semiprojizierbare RNDV-Gruppoide sind definiert über Polarenbegriffe. Entsprechend erhalten wir mittels primer Ideale

14. 10. 4 Proposition. *Ein RNDV-Gruppoid $\mathfrak{S}$ ist semiprojizierbar gdw. jedes eigentliche prime Ideal P genau ein minimal primes Ideal enthält, nämlich $\bigcup x^\perp \;\, (x \notin P) =: N$.*

BEWEIS. Sei $\mathfrak{S}$ semiprojizierbar und enthalte das eigentlich prime Ideal P etwa die beiden verschiedenen minimal primen Ideale $A\,,\, B$. Dann existieren Elemente a, b mit $a \in A\backslash B,\ b \in B\backslash A$, weshalb sogar ein orthogonales Paar $a^\circ \in A\backslash B,\ b^\circ \in B\backslash A$ existiert mit $a^{\circ\perp} \subseteq B$ und $b^{\circ\perp} \subseteq A$. Das aber führt zu

$$S = (a^\circ \wedge b^\circ)^\perp \ = \ a^{\circ\perp} \vee b^{\circ\perp} = P\,,$$

mit Widerspruch! Damit ist die Bedingung notwendig.

Hiernach zeigen wir, dass die Bedingung auch hinreicht. Hierzu beachten wir, dass stets $a^\perp \vee b^\perp \subseteq (a \wedge b)^\perp$ erfüllt ist.
Sei nun $x \notin a^\perp \vee b^\perp$ und sei P ein Wert von x mit $P \supseteq a^\perp \vee b^\perp$. Dann ist nach 14.5.2 die Vereinigung $N = \bigcup x^\perp\ \ (x \notin P)$ das eindeutig bestimmte in P enthaltene minimal prime Ideal. Da weiterhin $a^\perp$ und $b^\perp$ in P enthalten sind, folgt ferner $a\,,\ b \notin N$, also $a \wedge b \notin N$ und damit $(a \wedge b)^\perp \subseteq N \subseteq P$. Folglich führt uns $x \notin a^\perp \vee b^\perp$ zu $x \notin (a \wedge b)^\perp$. Damit sind wir am Ziel. □

Es ist unser nächstes Ziel, die Klasse der projizierbaren RNDV-Gruppoide zu charakterisieren, so wie wir die Klasse der semiprojizierbaren RNDV-Gruppoide charakterisiert haben.

14. 10. 5 Proposition. *Sei P ein eigentliches primes Ideal. Dann ist die Vereinigung aller primen z-Ideale, die enthalten sind in P, gleich der Menge aller $p \in P$ mit $p^{\perp\perp} \subseteq P$.*

BEWEIS. Liege p in einem z-Ideal, das enthalten ist in P. Dann folgt *per definitionem* $p^{\perp\perp} \subseteq P$. Bleibt zu zeigen, dass für jedes $p \in P$ mit $p^{\perp\perp} \subseteq P$ ein primes z-Ideal $Z \subseteq P$ existiert mit $p \in Z$.
Zu diesem Zweck definieren wir $\mathcal{F} := \{x^{\perp\perp} \,\big|\, x \notin P\}$. Dann bildet $\mathcal{F}$ einen Filter im Verband aller Bipolaren aus $\mathfrak{S}$, die $p^{\perp\perp}$ nicht enthalten. Folglich können wir $\mathcal{F}$ zu einem maximalen Filter $\mathcal{H}$ dieses Typs ausdehnen. Wir definieren nun $Z := \{z \,\big|\, z^{\perp\perp} \notin \mathcal{H}\}$ und werden zeigen, dass dieses Z „passt".
Hierzu verifizieren wir zunächst, dass Z operativ abgeschlossen ist. Dies ist evident mit Blick auf die Verbandsoperationen. Bleibt die Multiplikation. Wir wählen $a\,,\ b \in Z$. Dann folgt bezüglich der Multiplikation:

$$\begin{array}{rcl} a, b \in Z & \rightsquigarrow & a^{\perp\perp}\,,\ b^{\perp\perp} \notin \mathcal{H} \\ & \Longrightarrow & \\ \exists\, x^{\perp\perp}, y^{\perp\perp} \in \mathcal{H} : & & a^{\perp\perp} \cap x^{\perp\perp} \subseteq p^{\perp\perp} \supseteq b^{\perp\perp} \cap y^{\perp\perp}\,, \end{array}$$

was zu $\qquad (ab)^{\perp\perp} \cap (x \wedge y)^{\perp\perp} \ = \ (a^{\perp\perp} \vee b^{\perp\perp}) \cap (x^{\perp\perp} \cap y^{\perp\perp}) \subseteq p^{\perp\perp}$

führt und folglich $(ab)^{\perp\perp} \notin \mathcal{H}$, also $ab \in Z$ impliziert. Es ist Z aber auch eine Untermenge von P, wegen

$$z \in Z \Longrightarrow z^{\perp\perp} \notin \mathcal{H} \Longrightarrow z^{\perp\perp} \notin \mathcal{F} \Longrightarrow z \in P\,.$$

Somit ist Z ein primes z-Ideal mit $p \in Z \subseteq P$. □

Hiernach sind wir in der Lage als ein Analogon von 14.10.4 zu beweisen:

14. 10. 6 Proposition. $\mathfrak{S}$ *is projizierbar gdw. jedes eigentliche Primideal P genau ein primes z-Ideal enthält, nämlich $N := \bigcup x^{\perp}$ $(x \notin P)$.*

BEWEIS. Sei $\mathfrak{S}$ projizierbar und sei Z ein primes, in P enthaltenes z-Ideal. Dann gilt $a \notin P \Longrightarrow a^{\perp} \subseteq Z$ und damit weiter $N \subseteq Z$. Wir betrachten nun ein $z \in Z$ und ein $s \notin P$. Dann gilt $s = u \cdot v$ für in geeignetes $u \in z^{\perp}, v \in z^{\perp\perp} \subseteq Z \subseteq P$ und daher mit $u \notin P$. Das führt weiter zu $z \in u^{\perp} \subseteq N$. Demzufolge gilt $Z = N$. Es ist die aufgestellte Bedingung also notwendig.
Die aufgestellte Bedingung ist aber auch hinreichend. Denn im Falle von $a^{\perp} \times a^{\perp\perp} \neq S$ würde ein eigentliches $a^{\perp} \times a^{\perp\perp}$ existieren und damit ein $a^{\perp} \times a^{\perp\perp}$ umfassendes eigentliches primes Ideal P. Das aber bedeutet: ist Z das eindeutig bestimmte prime z-Ideal in P, so folgt $a \in a^{\perp\perp} \subseteq Z \subseteq P$, und es müsste nach Voraussetzung ein $b \notin P$ existieren mit $a \in b^{\perp}$, woraus sich $b \notin P$ & $b \in a^{\perp} \subseteq P$ ergäbe, mit Widerspruch! □

Literaturverzeichnis

[1] Abbot, J. C.: *Semi-boolean Algebra.* Mat. Ves. **4** (19) (1967), 177-198.

[2] Aczél, J.: *Quasigroups, nets and nomograms.* Adv. Math. **1** (1965), 383-450.

[3] Arnold, I.: *Ideale in kommutativen Halbgruppen.* Math. Sb. **36** (1929), 401-407.

[4] Baer, R.: *Free sums of groups and their generalizations, An analysis of the associative law.* Am. Journ. Math. **71** (1949), 706-742.

[5] Banaschewski, B.: *On lattice-ordered groups.* Fund. Math. **55** (1964), 113-122.

[6] Bigard, A.: *Sur les z-sous-groupes d'un groupe réticulé.* C.R. Acad. Sc. Paris **266** (1968), 261-262.

[7] Bigard, A., Keimel, K. and S. Wolfenstein: *Lecture Notes in Mathematics: Groupes et Anneaux Réticulés.* Springer-Verlag Berlin-Heidelberg-New York 1977.

[8] Billhardt, B.: *Zum Clan der normalen Teibarkeitshalbgruppe.* Dissertation, promoted by B. Bosbach, Kassel 1981.

[9] Birkhoff, G.: *Lattice-ordered groups.* Ann. Math. **43** (1942), 298-331.

[10] Birkhoff, G.: *Lattice theory.* Amer. Math. Soc. Coll. Publ. 1. ed. 1940.

[11] Birkhoff, G. and R. S. Pierce: *Lattice-ordered rings.* Ann. Acad. Bras. d. Cienc. (1956), 41-69.

[12] Blok, W. J. and I. M. A. Ferreirim: *The structure of hoops.* Alg. Univ. **43** (2000), 233-257.

[13] Blyth, T. S.: *Lattices and ordered Agebraic Structures.* Springer-Verlag, London Limited 2005

[14] Bosbach, B.: *Komplementäre Halbgruppen. Ein Beitrag zur instruktiven Idealtheorie.* Math. Ann. **161** (1965), 279 - 295.

[15] Bosbach, B.: *Komplementäre Halbgruppen. Eine Darstellungstheorie.* Math. Ann. **179** (1968), 1 - 14.

[16] Bosbach, B.: *Komplementäre Halbgruppen. Axiomatik und Arithmetik.* Fund. Math. **64** (1969), 257 - 287.

[17] Bosbach, B.: *Komplementäre Halbgruppen. Kongruenzen und Quotienten.* Fund. Math. **69** (1970), 1 - 14.

[18] Bosbach, B.: *Zur Theorie der Teilbarkeitshalbgruppen.* Semig. For. **3** (1971), 1 - 30.

[19] Bosbach, B.: *Rechtskomplementäre Halbgruppen. Axiome, Polynome, Kongruenzen.* Math. Z. **124** (1972), 273 - 288.

[20] Bosbach, B.: *Residuation-Groupoids.* Bull. de l'Acad. Pol. des Sc., Série des sciences math., astr. et phys. Vol. **XXII**, No. 2, (1974), 103 - 104.

[21] Bosbach, B.: *ℓ-group-cone and boolean algebra. A common one-identity-axiom.* Coll. Math. Soc. J. Bolyai **17** (1975), 41 - 56.

[22] Bosbach, B.: *Schwache Teilbarkeitshalbgruppen.* Semig. For. **12** (1976), 119 - 135.

[23] Bosbach, B.: Concerning ℓ-group- (cone-) lattices. Coll. Math. Soc. J. Bolyai **17** (1977), 153 - 159.

[24] Bosbach, B.: *Residuation groupoids and lattices.* Studia Sc. Math **13** (1978), 433 - 457.

[25] Bosbach, B.: *Teilbarkeitshalbgruppen und Quaderalgebren.* Semig. For. **20** (1980), 319 - 334.

[26] Bosbach, B.: *Residuation groupoids.* Resultate Math. **5** , (1982) 107 - 122.

[27] Bosbach, B.: *Concerning Bricks.* Acta Math. Ac. Sc. Hung. **38** (1981), 89 - 104.

[28] Bosbach, B.: *Concerning cone algebras.* Alg. Univ. **15** (1982), 58 - 66.

[29] Bosbach, B.: *Concerning semiclans.* Arch. Math. (Basel) **37** (1981), 316-324.

[30] Bosbach, B.: *Teilbarkeitshalbgruppen, Lecture Note* Kasseler Mathematische Schriften 1996. (250 pages)

[31] Bosbach, B.: *A representation theorem for completely join distributive algebraic lattices.* Per. Math. Hung. **13** (1982), 113 - 118.

[32] Bosbach, B.: *Teilbarkeitshalbgruppen mit vollständiger Erweiterung.* J. Alg. **83** (1983), 237 - 255.

[33] Bosbach, B.: *Teilbarkeitshalbgruppen. Orthogonalität und Linearität.* Kasseler Mathematische Schriften 1987.

[34] Bosbach, B.: *Separative Teilbarkeitshalbgruppen.* Contributions to general algebra **6** (1988), 49 - 65.

[35] Bosbach, B.: *Lattice ordered binary systems.* Acta Sci. Math. **52** (1988), 257 - 289.

[36] Bosbach, B.: *Hyperarchimedische Teilbarkeitshalbgruppen.* Czech. Math. J. **39** (1989), 528 - 543.

[37] Bosbach, B.: *Representable divisibility semigroups.* Proc. Edinb. Math. Soc. **34** (1991), 45 - 64.

[38] Bosbach, B.: *Idealhalbgruppen.* Kassel 1994, ein privates Manuskript.

[39] Bosbach, B.: *Teilbarkeitshalbgruppen, Lecture Note* Kasseler Mathematische Schriften 1996. (250 pages), ein privates Manuskript.

[40] Bosbach, B.: *Residuationsstrukturen.* Kassel, 1997, 2003, 2006 , ein privates Manuskript.

[41] Bosbach, B.: *Convex chains in lattice monoids and lattice loops* Acta Sci. Math **67** (2001), 57 - 75.

[42] Bosbach, B.: *Residuation Groupoids – Again.* Result. Math. **53** (2009), 77 - 51.

[43] Bosbach, B.: *Divisibility Groupoids – Again.* Result. Math. **57** (2010), 257 - 285.

[44] Büchi, J. R.: *The collected works of J. Richard Büchi.* Springer, 1990.

[45] Büchi, J. R. and T. M. Owens: *Complemented monoids and hoops.* An unpublished manuscript.

[46] Bruck, R.H.: *A Survey of Binary Systems.* Ergebnisse der Mathematik, Springer 1958.

[47] Burris, S. and H. P. Sankappanavar: *A Course in Universal Algebra* Springer, Berlin-Heidelberg-New York, 1981.

[48] Chang, C. C.: *Algebraic analysis of many-valued logics.* Trans. Amer. Math. Soc. **88** (1958), 467 - 490.

[49] Chang, C. C.: *A new proof of completeness of the Łukasiewicz axioms.* Trans. Amer. Math. Soc. **93** (1959), 74 - 80.

[50] R. L. O. Cignoli and D. Mundici. *An elementary presentation of the equivalence between MV-algebras and ℓ-groups with strong unit.* Special issue on Many-valued Logics (D. Mundici, ed.), Studia Logica 61 (1998), 4964.

[51] Cignoli, R. L. O., D'Ottaviano Itala M. L. and D. Mundici: *Algebraic Foundations of Many-valued Reasoning.* Trends in Logic **7**. Kluwer Academic Publishers, Dordrecht/Boston/London, 2000.

[52] Clifford, A. H.: *Arithmetic and idealtheory in commutative semigroups.* Ann. Math. **39** (1938), 594 - 630

[53] Clifford, A. H.: *Partially ordered abelian groups.* Ann. Math. **41** (1940), 465 - 473.

[54] Clifford, A. H.: *Naturally totally ordered commutative semigroups.* Amer. J. Math. **76** (1954), 631 - 646.

[55] Clifford, A. H. and G. B. Preston.: *The algebraic theory of semigroups.* Amer. Math. Soc. Math. Surveys 1961.

[56] Conrad, P. F.: *The lattice of all convex ℓ-subgroups of a lattice-ordered group.* Czech. Math. J. **15** (1965), 101 - 123

[57] Conrad, P. F.: *Introduction de la théorie des groupes réticulés.* Paris, Sécrétariat mathématique 1967.

[58] Conrad, P.F.: *Lex-subgroups of lattice-ordered groups.* Czech. Math. J. **18** (1968), 86 - 103.

[59] Day, A.: *A characterization of modularity for congruence lattices of algebras.* Canad. Math. Bull. **12** (1969), 167 - 173.

[60] Dedekind, R.: *Was sind und was sollen die Zahlen?*

[61] Diego, A.: *Sur les algébres de Hilbert.* Collection de Logique Mathématique Sr. A **21**, Gauthier Villars, Paris, 1966

[62] Diem, J. E.: *A radical for lattice-ordered rings.* J. Math. **25** (1968), 71 - 82.

[63] Dieudonné, J.: *Sur la theorie de la divisibilité.* Bull. Soc. Math. France **69** (1941), 133 - 144.

[64] Dilworth, R. P.: *Non commutative residuated lattices.* Trans. Amer. Math. Soc. **44** (1938), 426-444.

[65] Dilworth, R. P.: *Abstract commutative ideal theory.* Pacific J. Math. **12** (1962), 481 - 498.

[66] Dvurečenskij, A. and M. G. Graziano: *Remarks on representations of minimal clans.* Tatra Mt. Math. Publ. (1998), 31 - 53.

[67] Dvurečenskij, A. and Sylvia Pulmannová: *New Trends in Quantum Structures.* Kluwer Academic Publishers, Dordrecht/ Boston/ London, 2000.

[68] Dvurčenskij, A. and J. Rachunek *Probalistic Avariging in Boundeed $R\ell$-Monoids.* Semig. Forum (2006), 190 - 206.

[69] Esteva, F., Godo, L., Hájek, P., and F. Montagna: *Hoops and fuzzy logic.* J. Logic Computat. **13**, (2003), 531-555.

[70] Evans, T.: *Lattice-ordered loops and quasigroups.* J. Alg. **16** (1970), 218 - 226.

[71] Evans, T. and P. A. Hartman: *Varieties of lattice-ordered algebras.* Alg. Univ. **17** (1983), 376 - 392.

[72] Everett, C. J. and S. Ulam: *On ordered groups.* Trans. Amer. Math. Soc. **57** (1945), 208 - 216.

[73] Fan, K.: *Partially ordered additive groups of continuous functions.* Ann. Math. **51** (1950), 409 - 427.

[74] Ferreirim, I. M.: *On Varieties and Quasivarieties of Hoops and their Reducts.* Ph. D. Thesis, University of Illinois at Chicago, 1992.

[75] Fleischer, I.: *Functional representation of partially ordered groups.* Ann. Math. **64** (1956), 260 - 263.

[76] Frink, O.: *Topology in lattices.* Trans. Amer. Math. Soc. **57** (1942), 569 - 582.

[77] Fried, E.: *Representations of partially ordered groups.* Acta. Sc. Math. **26** (1965), 15 - 18.

[78] Fuchs, L.: *Partially ordered algebraic systems.* Pergamon Press, Oxford 1963.

[79] Fuchs, L.: *Teilweise geordnete algebraische Strukturen.* Studia Mathematica, Vandenhoek & Ruprecht, Göttingen 1966.

[80] Fuchs, L.: *On partially ordered algebras I.* Coll. Math. **13** (1966), 116 - 130. II. Acta Sc. Math. **16** (1965), 35 - 41.

[81] Fuchs, L.: *A remark on lattice ordered semigroups.* Semig. For. **7** (1974), 372 - 374.

[82] Galatos, N.: *Varieties of Residuated Lattices.* PhD dissertation, promoted by C. Tsinakis, Vanderbilt University, 2003.

[83] Georgescu, G.: *Bosbach states on fuzzy strucures.* Soft Computing **8** (2004), 217-230.

[84] Gispert, J. and D. Mundici: *MV-Algebras: a variety for magnitudes with archimedean units.* Alg. Univ. **53**, 2005, 7-43.

[85] Glivenko, V.: *Sur quelques points de la logique de M. Brouwer.* Bull. Acad. Sci. Belgique **15** (1929) 183 - 188.

[86] Grätzer, G.: *On the spectra classes in universal algebra.* Proc. Amer. Math. Soc. **18** (1967) 729 - 735.

[87] Grätzer, G.: Two Mal'cev type theorems in universal algebra. J. Comb. Th. **8** (1970) 334 - 372.

[88] P. Hájek, P.: *Meta mathematics of fuzzy logic.* Kluwer, 1998.

[89] Hartman, P. A.: *Ordered Quasigroups and Loops.* Ph. D. Thesis Emory University, 1971.

[90] Hartman, P. A.: *Integrally closed and complete ordered quasigroups and loops.* Proc. Amer. Math. Soc. **33** (1972), 250 - 256.

[91] Henriksen, M. and J. R. Isbell: *Lattice-ordered rings and function rings.* Pac. J. Math. **12** (1962), 533 - 565.

[92] Heinemann, G. *Ein Beitrag zur Theorie der Residuationsgruppoide.* Dissertation, Kassel 1977.

[93] Higman G. and B. H. Neumann: *Groups as groupoids with one law.* Publ. Math. Debr. **2** (1951), 215 - 221.

[94] Hölder, O.: *Die Axiome der Quantität und die Lehre vom Maß.* Ber. d. Sächs. Ges. d. Wiss. Leipzig, Math. Phys. Cl. (1901), 1 - 64.

[95] Holland, W. C.: *The lattice-ordered group of automorphisms of an ordered set.* Mich. Journ. **10** (1963), 399 - 408.

[96] Horn, A. and A. Tarski: *Measures in boolean algebras.* Trans. Amer. Math. Soc. (1948), 467 - 497.

[97] Iséki, K.: *Structure of special ordered loops.* Port. Math. **10** (1951), 81 - 83.

[98] Iséki, K., Arai Y. and S. Tanaka: *Characterizations of BCI, BCK-algebras.* Proc. Jap. Academy **42** (1966), 105 - 107.

[99] Iséki, K. and S.Tanaka: *An introuction into the theory of BCK-algebras.* Math. Jap. **23** (1978), 1 - 26.

[100] Iwasawa, K.: *On the structure of conditionally complete lattice-groups.* Jap. J. Math. **18** (1943), 777 - 789.

[101] Jaffard, P.: *Les systémes d'idéux.* Dunod, Paris 1960.

[102] Jakubík, J.: *Konvexe Ketten in ℓ-Gruppen.* Časopis pěst. Mat. **84** (1959), 53 - 63.

[103] Jakubík, J.: *Lattice-ordered groups with a basis.* Math. Nachr. **53** (1972), 217 - 236.

[104] Jakubík, J.: *Lattice-ordered groups of finite breadth.* Coll. Math. **27** (1973), 13 - 20.

[105] Jakubík, J.: *Strongly projectable lattice-ordered groups.* Czech. Math. J. **26** (1976), 642 - 652.

[106] Jakubík, J.: *Convex chains in MV-algebras,* Slovaca **51** (2001), 151 - 166.

[107] Jakubík, J.: *Convex chains in pseudo MV-algebras,* Czechoslovak Math. J. **53** (2003), 113 - 125.

[108] Jónsson, B.: *Algebras whose congruence lattices are distributive.* Math. Scand. **21** (1967), 110 - 121

[109] Kappos, D.A.: *Probability algebras and stochastic spaces.* Academic Press, New York and London, 1969.

[110] Keimel, K.: *Représentation d'anneaux réticulés dans des faisceaux.* C. R. Acad. Sci. Paris **266** (1968), 124 - 127.

[111] Keimel, K.: *Anneaux réticulés quasi-réguliers et hyper-archimédiens.* C. R. Acad. Sci. Paris **266** (1968), 524 - 525.

[112] Keimel, K.: *Darstellung von Halbgruppen und universellen Algebren durch Schnitte in Garben; bireguläre Halbgruppen.* Math. Nachr. **45** (1970), 81 - 96.

[113] KEIMEL, K.: *Représentation de groupes et d'anneaux réticulés par des sections dans des faísceaux.* Thése Sci. Math. Paris 1970.

[114] KEIMEL, K.: *The representation of lattice-ordered groups and rings by sections in sheaves.* Lecture Notes in Mathematics **248** 1971, 1 - 98.

[115] KRAUSS, P. H. and D. M. CLARK.: *Global subdirect products.* Memoirs of Amer. Math. Soc., **17**, Number 210, 1979.

[116] ŁUKASIEWICZ, J.: *O logice trójwarkościowej.* Ruch Filozofizny, **6** (1920), 170 - 171.

[117] ŁUKASIEWICZ, J. AND A. TARSKI: *Untersuchungen über den Aussagenkalkül.* Comptes Rendus des séances de la Société des Sciences et des Lettres de Varsovie, Classe III, **23** (1930), 30 - 50.

[118] LORENZEN, P.: *Abstrakte Begründung der multiplikativen Idealtheorie.* Math. Z. **45** (1939), 533 - 553.

[119] LORENZEN, P.: *Über halbgeordnete Gruppen.* Math. Z. **52** (1950), 483 - 526.

[120] MAL'CEV A. I.: *On the general theory of algebraic systems (auf russisch).* Math. Sbornik **35** (1954), 3 - 20.

[121] MCFADDEN, R.: *Congruence relations on residuated semigroups.* J. London Math. Soc. **37** (1962), 242 - 248.

[122] MCKENZIE, R.: *On equational theories of lattices.* Math. Scand. **27** (1970), 24 - 38.

[123] MERLIER, THÉRÈSE.: *Sur les demi-groups réticulés et les o-demigroupes.* Semig. For. **2** (1971), 64 - 70.

[124] MOLINARO, I.: *Demigroupes residutifs I.* J. Math. Pures Appl. **39** (1960) 319 - 356.

[125] MOLINARO, I.: *Demigroupes residutifs II.* J. Math. Pures Appl. **40** (1961) 43 - 110.

[126] MUNDICI D. and L. O. CIGNOLI: *Algebraic foundations of many valued reasoning.* Dordrecht, Kluwer, 1999.

[127] NAIK, N., SWAMY, B. L. N. and S. S. MISRA: *Lattice-ordered commutative loops.* Math. Sem. Notes, Kobe University **8** (1980), 57 - 71.

[128] NEUMANN, B.: *On a problem of G. Grätzer.* Publ. Math. Debrecen **6** (1967), 325 - 329.

[129] PAP, E. editor: *Handbook of Measure Theory.* I, II. North-Holland, 2002.

[130] Padmanabhan R. and R. W. Quackenbush.: *Equational theories of algebras with distributive congruences.* Proc. Amer. Math. Soc. **41** (1973), 373 - 377.

[131] Petrich, M.: *Inverse Semigroups.* John Wiley & Son, New York, 1984.

[132] Pixley, A. F.: *Distributivity and permutability of congruence relations in equational classes of lattices.* Proc. Amer. Math. Soc. **14** (1963), 105 - 109.

[133] Råchunek, J.: *A non commutative generalization of MV-Algebras.* Czech. Math. J. **52** (2002), 255-273.

[134] Repnitzkii, V. B.: *On subdirectly irreducible lattice-ordered semigroups.* Semig. For. **29** (1984), 277 - 318.

[135] Repnitzkii, V. B.: *Varieties of lattice-ordered semigroups.* (Diss. Cand. Acad. of Sc. of Moldavia, Kichinew) 1984.

[136] B. Riečan and T. Neubrunn: *Integral, measure, and ordering.* Kluwer, 1997.

[137] Riesz, F.: *Sur la theorie générale des operations linéaires.* Ann. Math. **41** (1940), 174 - 206.

[138] Ribenboim, P.: *Un théoréme de réalisation des groupes réticulés.* Pac. J. Math. **10** (1960), 305 - 308.

[139] Rump, W.: *A Decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation.* Adv. Math **193**, (2005) 40-55.

[140] Rump, W.: *Semidirect Products in Algebraic Logic and Solutions of the Quantum Yang-Baxter Equation.* J. of Alg. and its Appl. **7** (2008), 471-490.

[141] Rump, W.: *L-algebras, self-similarity, and l-groups.* J. Algebra **320** (2008), 2328-2348.

[142] Šik, F.: *Über subdirekte Summen geordneter Gruppen.* Czech. Math. J. **10** (1960), 400 - 424.

[143] Smith, F. A.: *A subdirect decomposition of additively idempotent semirings.* J. Nat. Sc. & Math. **7** (1967), 253 - 257.

[144] Stone, M. H.: *The theory of representations for boolean algebras.* Trans. Amer. Math. Soc. **40** (1936), 37 - 111.

[145] Stone, M. H.: *Applications of the theory of boolean rings to general topology.* Trans. Amer. Math. Soc. **41** (1937), 375 - 481.

[146] Stone, M. H.: *A general theory of spectra I/II.* Nat. Ac. Sci., **26/27**, 280 - 283/83 - 87, 1940/41.

[147] Swamy, K. L. N.: *Dually residuated lattice ordered semigroups.* Math. Ann. **159** (1965), 105 - 114.

[148] Swamy, K. L. N.: *Dually residuated lattice ordered semigroups II.* Math. Ann. **160** (1965), 64 - 71.

[149] Swamy, K. L. N.: *Dually residuated lattice ordered semigroups III.* Math. Ann. **167** (1966), 71 - 74.

[150] Tarski, A. and J. Łukasiewicz: *Investigations into the Sentential Calculus, in: Logic, Semantics, Metamathematics.* Oxford University Press, 1956, pp. 38-59. Reprinted by Hackett Publishing Company, Indianapolis, 1983.

[151] Tarski, A.: Fund. Math. **16** (1929), 195 - 197.

[152] Testov, V. A.: *On the theory of lattice-ordered quasigroups.* In Webs and Quasigroups, Kalinin University 1981, 153 - 157.

[153] Traczyk, T.: *On the variety of bounded commutative BCK-algebras.* Math. Jap. **247** (1979), 283 - 292.

[154] Tychonov, X.: *Über die topologische Erweiterung von Räumen.* Mat.Ann. **102** , (1929), 544 - 561.

[155] van der Waerden, B. L.: *Zur Produktzerlegung der Ideale in ganz-abgeschlossenen Ringen.* Math. Ann. **101** (1929), 293 - 308.

[156] Ward, M.: *Residuated distributive lattices.* Duke Math. J. **6** (1940), 641 - 651.

[157] M. Ward and R. P. Dilworth, *Residuated lattices.* Proc. Nat. Acad. Sci. USA **24** (1938)

[158] Ward, M. and R. P. Dilworth.: *Residuated lattices.* Trans. Amer. Math. Soc. **45** (1939), 335 - 354.

[159] Weinberg, E. C.: *Completely distributive lattice-ordered groups.* Pac. J. Math. **12** (1962), 1131 - 1137.

[160] Wille, R.: *Kongruenzklassengeometrien.* Lecture notes **113** Springer, Berlin-Heidelberg-New York 1970.

[161] Wyler, O.: *Clans.* Comp. Math. **17** (1965), 172 - 189.

[162] ZELINSKY, D. *Non associative valuations.* Bull. Amer. Math. Soc. **54** (1948), 175 - 183.

[163] ZELINSKY, D.: *On ordered loops.* Amer. J. Math. **70** (1948), 681 - 697.

Index

Abbildung, 289
  innere, 289
abgeschlossen, 23, 217, 219
  $\vee$-abgeschlossen, 23, 81
  $\wedge$-abgeschlossen, 23, 58, 81
  ganz -, 154, 213
  inf -, 299
  multiplikativ, 301, 303
  operativ, 338
ableitbar, 11
Algebra, 55, 249, 285
  boolesche, 99, 284, 294
  geordnete
    partial, 296
  Kegel -, 159, 247, 296
  partial geordnete, 284
  Verbands -, 284
  verbandsgeordnete, 285
archimedisch
  stark, 76
  streng, 24
Archimedizität, 203
Arithmetik
  Grenz -, 213
assoziativ, 25, 251
  mon -, 251, 266
  potenz -, 251, 266, 269
Atom, 215, 259, 304
  Hyper -, 215, 217
atomar, 216, 332
atomlos, 217
Automorphismus
  Anti -, 197

Basis, 332
bedecken, 259
Bedingung, 75
  Galois -, 17
  Mal'cev, 75
  Pixley, 75
Bereich, 209
  Bézout -, 209
  Integritäts -, 209
beschränkt, 14, 156
  0-beschränkt, 156
  nach unten, 261
Bewertung, 220
  partielle, 220
    maximale, 220
binäres System, 249
  verbandsgeordnetes, 250
Bisektion, 77
Brick, 125, 144, 156, 233
  dualer, 208

Charakter, 48
  von endlichem, 48
Chinesischer Restsatz, 74
Clan, 125
  Semi -, 237
clopen, 212

D.C.C., 251
Darstellung
  Binär -, 77
  Garben -, 212
  topologische, 212
Darstellungslemma, 286
direkt
  semi -, 86
distributiv, 258
  durchschnitts -, 14, 193
  kongruenz -, 121, 159, 250
  vereinigungs -, 14
  voll -, 290
  vollständig, 14
Distributivität
  Links -, 253
Dualgruppe, 10
DV-AML
  semiprim, 50

6
Ebene
  reelle, 307
einfach, 215
Einheit
  Links -, 30
Eins, 27
  Links -, 27
  Rechts -, 27
Einselement, 26
Einsteiler
  Links -, 88
  Rechts -, 88
Element
  basisches, 331
  Eins -, 299
  Halbprim -, 55
  idempotentes, 84, 306
  positives, 21
  Vollprim -, 55
Elemente
  unvergleichbare, 300
Endomorphismus
  Ketten -, 290
  Ordnungs -, 290
ergänzt, 23
  rechts -, 23
Erweiterung, 127, 252, 277
  u-Ideal -, 277
  v-Ideal -, 277
  Kegel -, 134
  Produkt -, 129, 136
  Quotienten -, 250
  rechtskomplementäre, 136
  Schnitt -, 277
  vollständige, 252
e-unitär, 8
Extension
  lexicographische, 325

Faktor, 218
  direkter, 283, 299
    innerer, 283
    sub -, 283
  Vollprim -, 54
Filet, 318
Filter, 312
  Ultra -, 312
finit
  ortho -, 336
fremd
  teiler -, 36
Fundamentalgleichung, 108
Funktion, 110

- additive, 140, 153
- algebraische, 110
- Maß -, 138, 219
- stetige, 218
- Term -, 208

Garben, 212
geordnet
- halbverbands -, 250
- linear, 24, 56, 251, 268
- partial, 249, 252, 290
- teilweise, 28
- total, 304
- verbands -, 249, 250

geschnitten, 9
Gesetz
- Distributiv -, 13

Grenze
- obere, 14
- untere, 14

group
- lattice -, 20

Gruppe, 218, 249
- ℓ -, 20, 197
- abelsche, 99
- angeordnete
  - vollständig, 218
- freie
  - abelsche, 251
- geordnete, 218
- linear geordnete, 325
- Quasi -, 249
  - partial geordnete, 252
  - Verbands -, 249, 251
- Verbands -, 20, 86, 99, 250, 284
  - abelsche, 284
  - kegel, 86
  - Kegel einer, 24
  - Kegel einer mit 0, 24
  - Quasi -, 285

Gruppoid, 25, 249, 252
- Divisor, 300
- Doppel -, 25
- Kürzungs -, 250, 252
- LD -, 299
- Links-Divisor -, 299
- LRR -, 247
- po -, 299
- positives RN-LD -, 300
- Rechts-Divisor, 300
- rechtsnormales LD -, 300
- Residuations -
  - duales, 173
- RN-D -, 300
- RN-LD -, 300
- Verbands -, 249, 250, 285
  - rechtsnormales, 283

Halbgruppe, 23, 25, 28, 249, 251
- archimedische d -, 204
- bisimple, 88
- Ideal -, 284
- idempotente, 23
- inverse, 84, 88
- kürzbare, 23
  - komplementäre, 57, 115
  - rechts -, 23
- komplementäre, 23, 34, 284, 293
  - archimedische, 24
  - brouwersche, 60
  - kürzbare, 60
  - links -, 23
  - normale, 233
  - rechts -, 23, 25, 28, 99

linear geordnete, 55
mit Komplementen, 206
rechts-kürzbare, 23
reguläre, 84
residuierte
abelsche, 284
RNDV -
repräsentierbare, 337
streng archimedische, 55
Teilbarkeits -, 209, 284
Verbands -, 249
verbandsgeordnete, 288
Zerlegungs -, 24, 54, 55
Halbverband, 24, 297
$\vee$ -, 297
brouwerscher, 24, 25, 300
Halm, 212
Höhe
eines Elementes, 334
Hülle, 144
Ideal -, 316
Komplementen -, 144
Polaren -, 316
Quotienten -, 144
Holoid, 24, 54
vollkanonisches, 24
Homomorphismus
Halbgruppen -, 85
Inversen -, 85
Hoop, 300

Ideal, 64, 68, 274, 276
$*$-Ideal, 68
$\bigcap$-prim, 313
o-Ideal, 297
t-Ideal, 48
u-Ideal, 274
v-Ideal, 38, 276
z-Ideal, 319
endliches, 38
Halb -, 68
Haupt -, 13, 209
Ideal
$\bigcap$-primes, 313
minimal primes, 313, 321
primes, 325
idempotentes, 41
maximales, 216
minimales, 217
Ordnungs -, 45, 247
primes
eigentlich, 322
Quotienten -, 209
Rechts -, 64
Rees -, 72
reguläres, 313
Verbands -, 274
Voll -, 68
Idempotent, 38, 84, 85, 211, 213–216, 306
idempotent, 60
identitiv, 111
injektiv, 201
Intervall, 215
abgeschlossenes, 251, 289
Einheits -, 218
reelles Einheits -, 215
Inverseneigenschaft, 249, 264
Inverses, 260
Rechts -, 260, 269
involutorisch, 199
irreduzibel
subdirekt, 194

isomorph, 79
anti -, 79
verbands -, 201
isoton, 80, 284, 285
Isotonie, 11
Isotop, 251

Kegel, 250
- Algebra, 143
- Clan, 143
einer ℓ-Gruppe, 21
negativer, 250, 253
positiver, 250
Verbandsgruppen -, 247
Kegel-Algebra
0-abgeschlossene, 159
Kern, 279, 318
einer Kongruenz, 318
Kette, 9, 14, 268
2-elementige, 296
Jakubík -, 299
maximale, 299
Kettenbedingung, 251
absteigende, 251, 268
aufsteigende, 268
Körper
Mengen -, 294
kofinal, 273
koinitial, 273
kommutativ, 251
kompakt, 212
Komplement, 28, 144
Links -, 23, 57, 257
Rechts -, 23, 28, 257
komplementär
abschnitts -, 13
rechts -, 64
Komponente, 73
Kongruenz, 64, 268
- klasse, 74
Filet -, 318
Filet respektierende, 320
kürzbare, 279
Links -, 64
R -, 138
Rechts -, 64
Rees - , 72
Kongruenzen, 74
vertauschbare, 74
konvex, 220, 223
kürzbar, 29, 60
links -, 23, 29, 77
Kürzung
relative, 161

Länge, 108
einer Kette, 334
Lemma
Divisor, 53
Splitting, 300
lexikographisch, 298
Lextension, 325
linear komponiert, 285
Loop, 93, 249
d-semi -, 250, 253
partial geordnete, 252
positive d-semi -, 262
Teilbarkeits-semi, 252
Verbands -, 93, 99, 249, 250, 253, 262, 284, 300
- Kegel, 121, 250, 253
mit Inverseneigenschaft, 251
repräsentierbare, 280
verbandsgeordnete, 288

Mächtigkeit, 24
Maß, 223
  partielles, 223
  stetiges, 156
Matrix, 2×2, 291
Maximum, 217
Menge, 279
  geordnete
    partial, 9, 296, 300
  konvexe, 279
  orthogonale, 331
  Potenz -, 24
modular
  kongruenz -, 121
Modularität, 334
Monoid, 54, 288
  EN-DL -, 303
  Unter -, 297
  Verbands -, 284
    abelsches, 284
  verbandsgeordnetes, 288
Monomorphismus, 219
Multiplikation
  partielle, 306
MV -
  Algebra, 299

Null, 295
Nullabschluss, 144

Operation, 284
  assoziative, 23
  binäre, 23
Operator, 205
  involutorischer, 205
Ordnung, 250
  lineare, 250
  Partial -, 88
  vollständige, 250
Ordnungsautomorphismus, 24
Ordnungsproblem, 251
orthogonal, 36, 214, 260, 280, 301

Paar
  orthogonales, 262
Partialordnung
  isotone, 80
Peano, 246
Polar
  Bi -, 313
Polare, 73, 270, 313
  C-Polare zu A, 313
  Bi-Polare, 336
  Haupt -, 318
  maximale, 329
  minimale, 329
Polynom, 74, 274
  - funktion, 286
  - kette
    Wille -, 74
  Malzew -, 74
  Pixley -, 74
  Multiplikations -, 274
positiv, 260
Positivbereich, 261
Potenz, 259
prim, 37, 259
  halb -, 37, 55
  minimal, 311, 329
  voll -, 37
  vollständig
    $\bigcap$ -, 194
Problem
  Darstellungs -, 284

Produkt, 86
  direktes, 24, 60, 215
  kartesisches, 86, 270, 302
  lexikographisches, 325
punktweise, 219

Quader, 156
Quotient, 276
  Rechts -, 276

Raum
  boolescher, 212
  Hausdorff -, 218
Redukt, 125
  Kegel -, 144
  Residuations -, 125
reelle Achse, 250
Regeln
  de Morgan'sche, 208
Relation
  2-stellig, 9
repräsentierbar, 73, 251, 279
residuiert, 294
  dual, 295
  normal, 294
Restklassensystem, 290
Ring, 62, 284
  boolescher, 24, 59
  Funktionen -, 291
  idempotenter, 114
    ohne 1, 19
  Verbands -, 284, 285, 290, 291
RNDV-Gruppoid, 309
  direkter Faktor eines, 328
  konvexes Unter -, 326
  Lex -, 326
  lex-einfaches, 326
  Lex-Kern eines, 326
  Lextension eines, 325
  ortho-finites, 334, 336
  projizierbares, 337
  semiprojizierbares, 337
  zerlegbares, 324

Schnitt, 218
  -vervollständigung, 218
Schranke, 14, 274
  obere, 14, 274
  untere, 274
selbstdual, 11
semiclan
  pb -, 237
semiloop
  d-semiloop
    repräsentierbare, 252, 284
  Teilbarkeits -, 250
  vollständige, 289
state, 76
Stelle, 284
Stellenzahl, 284
Struktur
  geordnete
    repräsentierbare , 284
  Verbands -, 285
  verbandsgeordnete, 285
subdirekt, 24, 294
surjektiv, 201

teilen, 273
  links -, 273
  rechts -, 273
Teiler, 23, 28
  All -, 63
  Links -, 23, 28, 56

Primpotenz -, 306
Rechts -, 23, 56
Term, 285
Theorem
1. Faktor -, 301
2. Faktor -, 302
3. Faktor -, 302
Jakubík-Ketten -, 299
Topologie
Intervall -, 217
natürliche, 219
Produkt -, 219
Relativ -, 219
torsionsfrei, 297, 298
Träger, 212
Typ, 249

überdecken, 217

Variable, 110, 274
Initial -, 286
Varietät, 102
Verband, 10
abschnittskomplementärer, 59
algebraischer, 193
boolescher, 24, 57
distributiver, 12, 59, 284, 309
Halb -, 199, 252
brouwerscher, 33
komplementärer, 13
Kongruenz - , 194
Multiplikations -, 53
sup-Halb -, 9
Vektor -, 219
verbandsdistributiv, 288
Verbandsgruppe
abelsche, 251
Kegel einer, 25, 99
Verbandsideal
maximales, 286
Verbandsordnung, 250
verbunden, 9
vergleichbar, 9, 213, 215
paarweise, 213
un -, 215
vertauschbar, 159
kongruenz -, 121, 159, 250
verträglich, 131
Vervollständigung, 273
vollständig, 14, 260, 268
bedingt, 14, 269
Vollständigkeit, 203, 251

Wert, 314
Würfel, 215
- algebra, 218
Gitter -, 215
Wurzel
Quadrat -, 77

Zahl, 24, 159, 218
natürliche, 24
Ordinal -, 24
Prim -, 159, 295
rationale, 24, 218
Zentrum, 38, 306
zerlegbar, 61, 215
direkt, 215
Zerlegung
direkte, 213, 301, 306
Primelement -, 251
subdirekte, 213, 218, 251, 300
zusammenhängend, 212, 217
un -, 212

total, 212, 218
zweibasig, 102