MAGISTER-ASPEKTE
der Mathematik

ausgewählt und vorgestellt von

Bruno Bosbach

2013

Zu dieser Sammelmappe

Im folgenden stellen wir einige Veranstaltungen zusammen, die sich in der vieljährigen Praxis des Autors bewährt haben.

Zunächst wenden wir uns einer Vorlesung zur Linearen Algebra zu. Sie entstand über einen langen Zeitraum hinweg als 2-semestrige 4+2-Veranstaltung und hat die Jordan'sche Normalform als Schwerpunkt zum Ziel.
Zugabe ist ein Primer von Sonia Leach zum Single-Value-Decomposition-(SVD)-Verfahren. Es wird z. B. eingesetzt bei der Deutschen Luft- und Raumfahrt-Gesellschaft (DLR Göttingen) und ebenso bei der Deutschen Bundesbank (DBB Frankfurt).

Hieran schließt sich eine Algebra an, die stringent *ab ovo* hin zum Fundamentalsatz der Algebra führt und daneben die klassischen Konstruktionsprobleme und den Satz von Wedderburn anbietet.

Im Rahmen der geltenden Studienordnungen konnten Diplom-Kandidaten wählen zwischen LINAL-I+ALG und LINAL-I+LIN-AL-II. L-3-Kandidaten hingegen war als Pflichtpensum im Grundstudium zumindest eine der beiden Veranstaltungen LINAL-I oder ALG aufgegeben.

Als eine Veranstaltung *ab ovo* war(en) „Graphen für alle (Studiengänge)", sehr beliebt. Initiiert durch das Königsberger Brückenproblem (Leonhard Euler), befeuert durch Färbungsprobleme, vitalisiert durch den interdisziplinären Mengerschen Satz, angeboten nach „uralten Rezepten" von Denes König, praxis-bezogen und theorie-orientiert, da konnte jeder mitmachen.

Die hier vorgestellte Vorlesung über Ringe bietet zum einen eine Einführung in die klassische Idealtheorie, zum anderen die phantastische Artin'sche DCCL-Kombinatorik und als Ergänzung eine Analyse der faktoriellen Ringe.

Endlich befassen wir uns mit Fragen der Ordnung, dem EINS und KEINS. Darunter als Highlight der Satz von Wilson, nach dem der Körper $\mathbf{R}$ der reellen Zahlen unendlich viele (paarweise verschiedene) nicht lineare Verbandsordnungen zulässt. Eine Versammlung von Mathematikern historischen Ranges: *ein wahres Festival der Strukturen.* Schöner kann Mathematik nicht sein als reinste *„Bauhaus-Architektur".* Hier werden fundamentale Elemente der Kombinatorik, Algebra, Geometrie und Analysis *via* Ordnung verwoben.

Tempora mutantur ... Die Zeiten ändern sich und die Paradigmen auch, so eignet sich wohl keine dieser Noten als Bologna-Modul. Indes: sie alle müssten

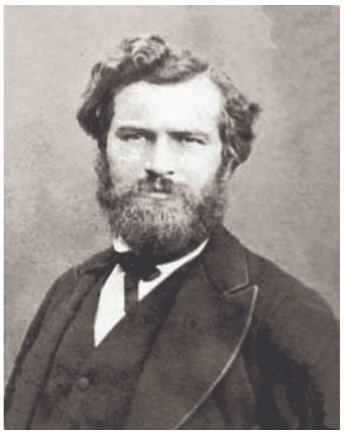
Anregungen enthalten für Seminare, Bachelor- und Magister-Arbeiten. Einfach mal stöbern,

Glückauf B.B.

Notizen zur Linearen Algebra

Bruno Bosbach

1998/1999



Camille Jordan
1838 -1922

Inhaltsverzeichnis

Zu diesem Skript

Das hier vorgelegte Skript erwuchs aus wiederholten Veranstaltungen des Verfassers zur Linearen Algebra, gegliedert in LINAL-I für Lehramt- und Diplom-Kandidaten und LINAL-II für Diplomanden.

Orientierung gaben dem Autor dabei ein Skriptum zur Vorlesung von Prof. Dr. F. W. Neuhaus (Köln) [4] aus dem Jahr 1949, aufgeschrieben von W. Kippels (später Dr. Kippels), sowie die Monographien von H. J. Kowalski [3], von O. Schreier/E. Sperner [5, 6] und – später – die „Bibel" von Howard Anton [1].

Hingewiesen sei aber auch auf die wiederholten Auflagen eines „Kompendiums" von Dr. Ralf Schaper am Fachbereich Mathematik, für Studenten eine wertvolle Fundgrube.

Er betreute die Übungen zu fast allen Veranstaltungen des Autors zur Linearen Algebra: kreativ, kooperativ – und – als „Erfolgs-Garant".

Übungen sind diesem Skript unter Berücksichtigung des breiten Übungsmaterials in [3] nicht beigefügt.

Beigesteuert wurde vom Autor ein Beitrag zur abstrakten linearen Abhängigkeit sowie die „didaktische" Aufbereitung der Jordanschen Normalform, wie es anerkennend von einem Kasseler Fach-Kollegen dem Sinn nach formuliert wurde – und die Komposition, bescheidener „Handschrift", wie es sich bei einem Skript versteht.

Schließlich möchten wir „a posteriori" dem Anwender mit einem Artikel von Sonja Leach zum Single-Value-Decomposition- (SVD)-Verfahren entgegen kommen. Dieses Verfahren wird z. B. eingesetzt bei der Deutschen Luft- und Raumfahrt-Gesellschaft (DLR) und ebenso bei der Deutschen Bundesbank (DBB) – ein großartiger Stoff für ein Seminar zur Numerik der Linearen Algebra, die in Kassel stets von Fach-Numerikern angeboten wurde und deshalb unter LINAL I/II nicht berücksichtigt werden musste.

Die TeX-Verarbeitung erfolgte seitens des Autors mit Unterstützung durch die „TeX-pertin" Helga Wasgindt, die u.a. die faszinierende Abbildung zur Ermittelung der Jordan'schen Normalform auf der Grundlage der damaligen Möglichkeiten entwarf, so dass der Autor sich auf die Einrichtung der Parameter beschränken konnte. Vielen Dank dafür!

Kapitel 1

Der Vektorraum

1.1 Hin zu den Wurzeln

Was ist lineare Algebra? [1)]
Lineare Algebra ist die Theorie der Vektorräume.

Was ist ein Vektorraum?

Wir starten vom $\mathbf{R}^3$. Er sei anschaulich bekannt.

Es ist unser erstes Ziel, seine *algebraische Struktur* abzuheben, zu abstrahieren (abzusehen) von „allem anderen" (was diesen Raum darüber hinaus auszeichnet).

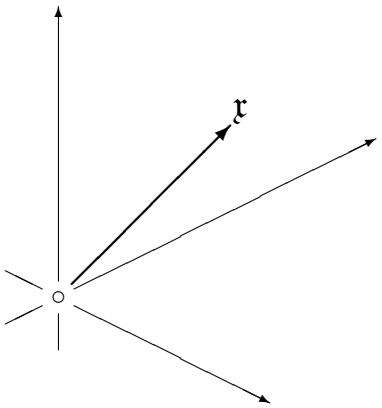
Der $\mathbf{R}^3$ wird bestimmt durch den **Körper** $\mathcal{R}$ der reellen Zahlen r, in diesem Zusammenhang bezeichnet als **Skalare** , und die **Gruppe** $\mathcal{G}$ seiner Vektoren $\mathfrak{x}$, die wir uns als *Pfeile* vorstellen können.

Darüber hinaus ist eine **S-Multiplikation** (skalare Multiplikation) erklärt, die jedem Paar $s, \mathfrak{x}$ einen eindeutig bestimmten Vektor $s\mathfrak{x}$ zuordnet.

Wir vergessen nun alles vom $\mathbf{R}^3$, außer: dass in $\mathcal{R}$ die *Buchstabenrechnung* gilt, dass in $\mathfrak{V}$ die *Buchstabenaddition* gilt und zwischen $\mathcal{R}$ und $\mathfrak{V}$ eine

[1)] Leser die sich ergänzend orientieren möchten, seien verwiesen auf Falko Lorenz, Lineare Algebra I, II, B · I Wissenschaftsverlag, Mannheim – Wien – Zürich, ISBN 3-411-03211-1 .

S-Multiplikation erklärt ist.



1. 1. 1 Definition. Sei $(K\,,+,\cdot)$ $=:\mathcal{K}$ ein **algebraischer Bereich**, in dem die *Buchstabenrechnung* gilt. Sei $(\mathfrak{V},\oplus)=:\mathcal{V}$ ein algebraischer Bereich, in dem die *Buchstabenaddition* gilt. Sei schließlich $\odot$ eine **Operation** , die jedem Paar $s,\mathfrak{x}$ $(s\in K,\,\mathfrak{x}\in\mathfrak{V})$ ein eindeutig bestimmtes Element $s\odot\mathfrak{x}$ aus $\mathfrak{V}$ zuordnet.

Dann nennen wir das Tripel $\mathbf{V}:=(\mathcal{K},\mathcal{V},\odot)$ einen **Vektorraum** , wenn gilt:

$$\begin{array}{lrcl}
\text{(V1)} & (a+b)\odot\mathfrak{x} & = & a\odot\mathfrak{x}\oplus b\odot\mathfrak{x}\\
\text{(V2)} & a\odot(\mathfrak{x}\oplus\mathfrak{y}) & = & a\odot\mathfrak{x}\oplus a\odot\mathfrak{y}\\
\text{(V3)} & a\odot(b\odot\mathfrak{x}) & = & (a\cdot b)\odot\mathfrak{x}\\
\text{(V4)} & 1\odot\mathfrak{x} & = & \mathfrak{x}.
\end{array}$$

Natürlich sind die eingeführten **Strukturen** noch zu präzisieren. Hierzu erklären wir zunächst:

1. 1. 2 Definition. Ein *ein algebraischer Bereich* $(G\,,*)=:\mathcal{G}$ heißt eine **abelsche Gruppe** , wenn $\mathcal{G}$ den Gesetzen genügt:

$$\begin{array}{lrcl}
\text{(A)} & a*(b*c) & = & (a*b)*c\\
\text{(K)} & a*b & = & b*a\\
\text{(G)} & \text{Jedes } a*x & \doteq & b \text{ ist lösbar.}
\end{array}$$

Hierin steht (A) für **Assoziativität** und (K) für **Kommutativität** .

1. 1. 3 Proposition. *In* $(G\,,*)$ *gilt genau dann die Buchstabenaddition, wenn* $(G\,,*)$ *die Gesetze* (A,K,G) *erfüllt.*

Hinweis: Wir müssen den Beweis der Algebra überlassen, wollen hier aber doch wenigstens zeigen, dass (G) eine eindeutige Subtraktion sichert. Hierzu vorweg:

$(G,*)$ besitzt ein **neutrales Element** e, d.h. ein Element e mit $a*e=a=e*a$.

DENN: Sind a und b aus G, so gibt es Elemente e bzw. c mit $a*e=a$ bzw. $a*c=b$. Für diese folgt dann

$$bei=(a*c)*e=(c*a)*e=c*(a*e)=c*a=b.$$

Daher ist e für alle x aus G ein **neutrales Element** in $\mathcal{G}$.

Sei hiernach $a*x=b*x$. Dann gibt es ein x' mit $x*x'=e$. Dies *impliziert* weiter:

$$\begin{array}{rcll} a & = & a*e & \text{(Vor)}\\ & = & a*(x*x') & \text{(Vor)}\\ & = & (a\star x)*x' & \text{(A)}\\ & = & (b*x)*x' & \text{(Vor)}\\ & = & b*(x*x') & \text{(A)}\\ & = & bei & \text{(Vor)}\\ & = & b\,, & \end{array}$$

weshalb die **Kürzungsregel** gilt, d. h. die **Implikation**:

$$a*x=b*x \implies a=b\,.$$

Bezeichnen wir nun e mit 0, $*$ mit $+$, die eindeutig bestimmte Lösung aus (G) mit $b-a$ sowie $0-a$ mit $-a$, so erhalten wir u. a.:

$$\begin{array}{rcl} a-(b-c) & = & (a-b)+c,\\ 0-(0-c) & = & (0-0)+c \\ -(-c) & = & c, \end{array}$$

also auch

und damit

wegen

$$\begin{array}{rcl} (b-c)+((a-b)+c) & \overset{\text{(A,K)}}{=} & (b-c)+c+(a-b)\\ & = & (c+(b-c))+(a-b)\\ & = & b+(a-b)\\ & = & a\\ & \rightsquigarrow & \\ (a-b)+c & = & a-(b-c). \end{array}$$

□

1. 1. 4 Definition. Eine **algebraische Struktur** $(K\,,+\,,\cdot)=:\mathcal{K}$ heißt ein Körper, wenn für $\mathcal{K}$ (in $\mathcal{K}$) gilt:

(G^+) $(\mathcal{K}\,,+)$ ist eine abelsche Gruppe

(G$^{\cdot}$) $\qquad (K-\{0\}\,,\,\cdot)$ ist eine abelsche Gruppe

(D) $$\begin{aligned} a\cdot(b+c) &= a\cdot b+a\cdot c \\ \&\ (a+b)\cdot c &= a\cdot c+b\cdot c\,. \end{aligned}$$

Es folgt:

1. 1. 5 Proposition. *In $\mathcal{K}$ gilt genau dann die Buchstabenrechnung, wenn $\mathcal{K}$ den Bedingungen* (G^{+}, G$^{\cdot}$, D) *genügt.*

Hinweis: Wie oben überlassen wir auch hier den Beweis der Algebra. Doch zeigen wir ausführlich, dass $a\cdot 0=0$ und damit $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ für alle a,b,c erfüllt ist, was sich wie folgt ergibt:

$$\begin{aligned} \underline{a\cdot 0}+a\cdot 0 &= a\cdot(0+0) \\ &= \underline{a\cdot 0}+0 \\ &\rightsquigarrow \\ a\cdot 0 &= 0. \end{aligned}$$

Hiernach kommen wir zur exakten Definition des Vektorraums:

1. 1. 6 Definition. Sei $\mathcal{K}=(K\,,\,+\,,\,\cdot)$ ein Körper. Sei $\mathcal{V}=(\mathfrak{V},\oplus)$ eine abelsche Gruppe. Sei weiter $\odot$ eine Operation $(s,\mathfrak{x})\mapsto s\odot\mathfrak{x}$ $(s\in K,\,\mathfrak{x}\in\mathfrak{V},\,s\odot\mathfrak{x}\in\mathfrak{V})$, die den Gesetzen (V1,. . . , V4) genügt – mit dem neutralen Element aus $(K-\{0\},\cdot)$ in der Rolle von 1.

Dann heißt das Tupel $(\mathcal{K}\,,\,\mathcal{V}\,,\,\odot)=:\mathbf{V}$ ein **Vektorraum** (auch ein **linearer Raum**) über $\mathcal{K}$. Insbesondere nennt man die Elemente $\mathfrak{x}\in\mathfrak{V}$ die **Vektoren** aus $\mathbf{V}$ und die Elemente $s\in K$ die **Skalare** des Vektorraums $\mathbf{V}$.

Gemäß den Gepflogenheiten in der Mathematik werden wir symbolisch nur dann zwischen $+$ und $\oplus$ bzw. zwischen $\cdot$ und $\odot$ unterscheiden, wenn Missverständnisse zu befürchten sind. Demzufolge wird in der Regel stehen

$$ac\,\mathfrak{x}+b\,\mathfrak{y}\ \text{ statt }\ (a\cdot c)\odot\mathfrak{x}\oplus b\odot\mathfrak{y},$$

und es zeigt diese Schreibweise, dass – wie bislang – die Operation $\cdot$ stärker binden soll als $\odot$ und $\odot$ stärker als die Operationen $+$ bzw. $\oplus$.

1. 1. 7 Proposition. *In jedem Vektorraum gilt:*

(i) $$s\mathfrak{o}\ =\ \mathfrak{o}$$

(ii) $$0\mathfrak{x} = \mathfrak{o}$$

(iii) $$-(s\mathfrak{x}) = (-s)\mathfrak{x} = s(-\mathfrak{x}).$$

BEWEIS. Wir setzen $\rightsquigarrow$ für: **es gilt, also**. Dann folgt:

(i) *via*
$$\begin{aligned} \underline{s\mathfrak{x}} + \mathfrak{o} &= s(\mathfrak{x} + \mathfrak{o}) \\ &= \underline{s\mathfrak{x}} + s\mathfrak{o} \\ &\rightsquigarrow \\ s\mathfrak{o} &= \mathfrak{o}, \end{aligned}$$

(ii) *via*
$$\begin{aligned} \underline{s\mathfrak{x}} + \mathfrak{o} &= (s+0)\mathfrak{x} \\ &= \underline{s\mathfrak{x}} + 0\mathfrak{x} \\ &\rightsquigarrow \\ 0\mathfrak{x} &= \mathfrak{o}, \end{aligned}$$

(iii) *via*
$$\begin{aligned} s\mathfrak{x} + (-s)\mathfrak{x} &= (s + (-s))\mathfrak{x} \\ &= 0\mathfrak{x} \\ &= \mathfrak{o} \\ &\rightsquigarrow \\ (-s)\mathfrak{x} &= -(s\mathfrak{x}) \end{aligned}$$

und der analogen Schlussweise bezüglich $s(-\mathfrak{x})$. □

1.2 Die lineare Hülle

Im $\mathbf{R}^3$ sind die einzelnen Vektoren durch ihre **Koordinaten** eindeutig bestimmt. In beliebigen Vektorräumen sind Koordinaten zunächst nicht gegeben, doch wird es uns unter geeigneten Bedingungen gelingen, „Achsen auszuzeichnen", mit deren Hilfe sich die Vektoren aus $\mathfrak{V}$ *kodieren* lassen. Hier befassen wir uns zunächst mit **Unterräumen.**

1. 2. 1 Definition. Sei $\mathbf{V}$ ein **K-Vektorraum**, d.h. ein Vektorraum über dem Körper $\mathcal{K}$ und $\mathfrak{U}$ eine Teilmenge von $\mathfrak{V}$. Dann nennen wir $\mathfrak{U}$ **abgeschlossen** in $\mathbf{V}$, wenn mit je zwei Vektoren $\mathfrak{x}, \mathfrak{y} \in \mathfrak{U}$ auch $\mathfrak{x} \oplus \mathfrak{y}$ in $\mathfrak{U}$ liegt, sowie mit jedem Vektor $\mathfrak{u} \in \mathfrak{U}$ auch jedes $s\mathfrak{u}\,(s \in K)$ zu $\mathfrak{U}$ gehört.

Also komprimierter: wenn mit jeder Menge von Vektoren aus $\mathfrak{U}$ auch alle **Linearkombinationen über** $\mathfrak{U}$ zu $\mathfrak{U}$ gehören.

1. 2. 2 Proposition. *Sei* $\mathfrak{U}_i \ (i \in I)$ *eine* **Familie** *von abgeschlossenen Vektormengen aus* $\mathfrak{V}$. *Dann ist auch* $\bigcap \mathfrak{U}_i \ \ (i \in I)$ *abgeschlossen.*

BEWEIS. Mit $\mathfrak{x}$ und $\mathfrak{y}$ liegt auch $\mathfrak{x} + \mathfrak{y}$ in allen $\mathfrak{U}_i \ (i \in I)$, so dass mit $\mathfrak{x}, \mathfrak{y} \in \mathfrak{D} := \bigcap \mathfrak{U}_i$ auch $\mathfrak{x}+\mathfrak{y}$ in allen $\mathfrak{U}_i$ und damit in $\mathfrak{D}$ liegt. Ferner erhalten wir analog die Implikation $\mathfrak{x} \in \mathfrak{D} \Longrightarrow s\mathfrak{x} \in \mathfrak{D}$. □

1. 2. 3 Definition. Seien **U** und **V** Vektorräume über $\mathcal{K}$. Dann nennen wir **U** einen **Unterraum** von **V**, wenn sich $\mathfrak{U}$ mit Blick auf seine Operationen als abgeschlossene Teilmenge von **V** auffassen lässt.

Offenbar ist der *engste* Unterraum **der Nullraum**, i. Z. der Raum $\emptyset$.

Hiernach kommen wir zur *linearen Hülle*.

1. 2. 4 Definition. Sei $\mathfrak{A} \subseteq \mathfrak{V}$ und $\mathfrak{U}_i \ (i \in I)$ die Familie aller abgeschlossenen Teilmengen die $\mathfrak{A}$ enthalten. Dann bezeichnen wir den Durchschnitt $\bigcap \mathfrak{U}_i \ (i \in I) =: [\,\mathfrak{A}\,]$ als **die lineare Hülle** $[\,\mathfrak{A}\,]$ von $\mathfrak{A}$.

Insbesondere ist damit $[\,\emptyset\,] = \{\mathfrak{o}\}$ und, wie man leicht sieht, im Falle $\mathfrak{A} \neq \emptyset$

$$[\,\mathfrak{A}\,] = \{\mathfrak{x} \mid \mathfrak{x} \ = \ \sum x_i \mathfrak{a}_i \ \ (\mathfrak{a}_i \in \mathfrak{A})\}.$$

Die große Bedeutung der linearen Hülle liegt in ihrer definierenden Rolle im Blick auf **die lineare Abhängigkeit**.

1. 2. 5 Definition. Sei **V** ein Vektorraum. Dann setzen wir

$$\mathfrak{x} \propto \mathfrak{A} \ \ :\Longleftrightarrow \ \ \mathfrak{x} \in [\,\mathfrak{A}\,]$$

und sagen im Falle $\mathfrak{x} \propto \mathfrak{A}$, der Vektor $\mathfrak{x}$ sei in **V linear abhängig** von der Vektormenge $\mathfrak{A}$.

Offenbar haben wir:

$$\mathfrak{x} \propto \mathfrak{A} \quad :\Longleftrightarrow \quad \mathfrak{x} = \mathfrak{o} \quad \text{V} \quad \mathfrak{x} = \sum x_i \ \ \mathfrak{a}_i \ \ (\mathfrak{a}_\mathfrak{i} \in \mathfrak{A}).$$

1. 2. 6 Proposition. *In jedem Vektorraum gilt*

(LA1) $\quad \mathfrak{x} \in \mathfrak{A} \Longrightarrow \mathfrak{x} \propto \mathfrak{A}$

(LA2) $\quad \mathfrak{x} \propto \mathfrak{A} \ \ \& \ \ \mathfrak{a} \propto \mathfrak{B} \ \ (\forall \mathfrak{a} \in \mathfrak{A}) \Longrightarrow \mathfrak{x} \propto \mathfrak{B}$

(LA3) $\mathfrak{x} \propto \mathfrak{A} \Longrightarrow \mathfrak{x} \propto \mathfrak{E} \subseteq \mathfrak{A}$ ($\mathfrak{E}$ endlich)

(LA4) $\mathfrak{x} \not\propto \mathfrak{B}$ & $\mathfrak{x} \propto (\mathfrak{B}, \mathfrak{y}) \Longrightarrow \mathfrak{y} \not\propto \mathfrak{B}$ & $\mathfrak{y} \propto (\mathfrak{B}, \mathfrak{x})$.

BEWEIS.

(LA1): $$\mathfrak{x} \in \mathfrak{A} \subseteq [\,\mathfrak{A}\,] \;\rightsquigarrow\; \mathfrak{x} \in [\,\mathfrak{A}\,] \rightsquigarrow \mathfrak{x} \propto \mathfrak{A}.$$

(LA2): $$\mathfrak{x} \in [\,\mathfrak{A}\,] \;\&\; \mathfrak{A} \subseteq [\,\mathfrak{B}\,] \;\Longrightarrow\; \mathfrak{x} \in [\,\mathfrak{A}\,] \subseteq [\,\mathfrak{B}\,] \Longrightarrow \mathfrak{x} \propto \mathfrak{B}\,.$$

(LA3): ist offenbar nichts zu zeigen.

(LA4): Wäre $\mathfrak{y} \propto \mathfrak{B}$ erfüllt, so würde folgen: $\mathfrak{x} \in [\,\mathfrak{B}, \mathfrak{y}\,] = [\,\mathfrak{B}\,] \rightsquigarrow \mathfrak{x} \propto \mathfrak{B}$ mit Widerspruch. Also gilt

$$\mathfrak{x} \not\propto \mathfrak{B} \;\&\; \mathfrak{x} \propto (\mathfrak{B}, \mathfrak{y}) \;\Longrightarrow\; \mathfrak{y} \not\propto \mathfrak{B}\,.$$

Weiter haben wir $\mathfrak{x} \not\propto \mathfrak{B} \Longrightarrow \mathfrak{x} \neq \mathfrak{o}$. Folglich ist $\mathfrak{x}$ wegen $\mathfrak{x} \propto (\mathfrak{B}, \mathfrak{y})$ von der Form

$$\mathfrak{x} = s\mathfrak{y} + \sum x_i \mathfrak{b}_i \;\; (s \neq 0),$$

woraus sich

$$\mathfrak{y} = \frac{1}{s}\mathfrak{x} - \sum \frac{1}{s}\, x_i \mathfrak{b}_i$$

ergibt, also

$$y \propto (\mathfrak{B}, \mathfrak{x}).$$

□

1.3 Basis und Dimension

1. 3. 1 Definition. Sei $\mathbf{V}$ ein Vektorraum über $\mathcal{K}$. Wir nennen $\mathfrak{A} \subseteq \mathfrak{V}$ **linear unabhängig**, i. Z. ℓu, wenn es keine nicht triviale Darstellung des Nullvektors $\mathfrak{o}$ über $\mathfrak{A}$ gibt, d. h., wenn gilt:

(LU) $$\mathfrak{o} = \sum x_i \mathfrak{a}_i \;\; (\mathfrak{a}_i \in \mathfrak{A}) \;\Longrightarrow\; x_i = 0 \;\; (\forall i)\,.$$

Dementsprechend nennen wir $\mathfrak{A}$ **linear abhängig**, i.Z ℓa, wenn $\mathfrak{A}$ nicht ℓu ist. Schließlich nennen wir $\mathfrak{B}$ eine **Basis** zu $\mathbf{V}$, wenn $\mathfrak{B}$ linear unabhängig und $[\,\mathfrak{B}\,] = \mathfrak{V}$ erfüllt ist.

Nach 1.3.1 ist die leere Menge $\emptyset$ offenbar ℓu, man beachte, dass es überhaupt keine Darstellung des Nullvektors über $\emptyset$ gibt. Daher können wir auch formulieren:

$\mathfrak{A} \subseteq \mathfrak{V}$ ist ℓa genau dann, wenn $\mathfrak{A} \neq \emptyset$ ist und mindestens ein Vektor $\mathfrak{a}$ aus $\mathfrak{A}$ ℓa ist von $\mathfrak{A} - \{\mathfrak{a}\}$.

Im weiteren werden wir einen Vektorraum **endlich erzeugt** nennen, wenn es eine endliche Teilmenge $\mathfrak{E} \subseteq \mathfrak{V}$ gibt mit $[\,\mathfrak{E}\,] = \mathfrak{V}$.

1. 3. 2 Der Basissatz. *Jeder endlich erzeugte Vektorraum* $\mathbf{V}$ *besitzt eine Basis.*

BEWEIS. Ist $\mathfrak{V} = [\,\mathfrak{E}\,]$ und zusätzlich $\mathfrak{E}$ ℓu, so ist nichts zu zeigen.

Sonst aber existiert ein $\mathfrak{x} \in \mathfrak{E}$ mit

$$\mathfrak{V} = [\,\mathfrak{E}\,] \;=\; [\,\mathfrak{E} - \{\mathfrak{x}\}\,] =: [\,\mathfrak{E}_1\,],$$

man beachte (LA1, LA2).

Ist nun $\mathfrak{E}_1$ ℓu, so sind wir fertig, sonst aber setzen wir das Verfahren fort, bis es spätestens bei der leeren Menge $\emptyset$ abbricht. □

Der soeben bewiesene Sachverhalt ist auch eine fast unmittelbare Folge des nachfolgenden Hilfssatzes:

1. 3. 3 Das Unabhängigkeitslemma.

$$\mathfrak{A}\ \ell u \ \ \&\ \ \mathfrak{x} \not\propto \mathfrak{A} \Longrightarrow (\mathfrak{A}, \mathfrak{x})\ \ell u\,.$$

BEWEIS. Wäre $(\mathfrak{A}, \mathfrak{x})$ unter den gegebenen Voraussetzungen ℓa, so hätten wir für ein $\mathfrak{y} \in \mathfrak{A} \cup \{\mathfrak{x}\} =: \mathfrak{A}_1$

$$\mathfrak{y} \;\propto\; \mathfrak{A}_1 - \{\mathfrak{y}\}.$$

Dieses $\mathfrak{y}$ wäre aber verschieden von $\mathfrak{x}$, weshalb wir auf

$$\mathfrak{y} \propto ((\mathfrak{A} - \{\mathfrak{y}\}), \mathfrak{x}) \quad \& \quad \mathfrak{y} \not\propto (\mathfrak{A} - \{\mathfrak{y}\})$$

schließen könnte, also nach (LA4) – man setze $(\mathfrak{A} - \{\mathfrak{y}\}) =: \mathfrak{B}$ – auch auf $\mathfrak{x} \propto \mathfrak{A}$. □

Der oben bewiesene Basissatz liefert die Grundlage für eine spätere Einführung von **Koordinaten**. Vorab ist jedoch zu beweisen:

1. 3. 4 Der Dimensionssatz. *Ist* $\mathbf{V}$ *endlich erzeugt, so haben alle Basen gleiche Länge.*

BEWEIS. Ist $\mathfrak{V} = \{\mathfrak{o}\}$, also $\mathbf{V} = \mathbf{O}$, so ist $\emptyset$ die einzige Basis, und es ist nichts zu zeigen. Sei hiernach $\mathbf{V} \neq \mathbf{O}$ und

$$\begin{aligned} \mathfrak{B} &= (\mathfrak{b}_1, \ldots, \mathfrak{b}_n) \\ \mathfrak{A} &= (\mathfrak{a}_i \,|\, i \in I) \end{aligned}$$

eine endliche sowie
eine beliebige Basis zu $\mathbf{V}$. Wir werden zeigen, dass $\mathfrak{A}$ genau n viele Elemente besitzt. Hierzu beachten wir zunächst, dass in $\mathfrak{A}$ ein $\mathfrak{a}_1$ existieren muss mit

$$\begin{aligned} \mathfrak{a}_1 &\not\propto (\mathfrak{b}_2, \ldots, \mathfrak{b}_n), \\ \mathfrak{b}_1 &\in [\,\mathfrak{A}\,] \subseteq [\,\mathfrak{b}_2, \ldots, \mathfrak{b}_n\,], \end{aligned}$$

da andernfalls

$$\mathfrak{b}_1 \propto (\mathfrak{b}_2, \ldots, \mathfrak{b}_n)$$

also
erfüllt wäre. Daher haben wir

$$\begin{aligned} \mathfrak{a}_1 \not\propto (\mathfrak{b}_2, \ldots, \mathfrak{b}_n) \quad \& \quad & \mathfrak{a}_1 \propto (\mathfrak{b}_1, \ldots, \mathfrak{b}_n) \\ \rightsquigarrow \quad & \mathfrak{b}_1 \propto (\mathfrak{a}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_n) \\ \rightsquigarrow \quad & \mathfrak{b}_i \propto (\mathfrak{a}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_n) \\ & \qquad (1 \leq i \leq n) \\ \rightsquigarrow \quad & [\,\mathfrak{a}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_n\,] = \mathfrak{V}. \end{aligned}$$

Nun ist aber $\mathfrak{B}_1 := (\mathfrak{a}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_n)$ ℓu – man vergleiche 1.3.3 – und folglich (ebenfalls) eine Basis zu $\mathbf{V}$. Demzufolge können wir unser Verfahren fortsetzen mit

$$\mathfrak{B}_1 := (\mathfrak{a}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_n) \text{ in der Rolle von } \mathfrak{B}$$

$$\text{und} \qquad \mathfrak{B}_2 := (\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{b}_n) \text{ in der Rolle von } \mathfrak{B}_1.$$

Damit ist das ausgewählte $\mathfrak{a}_2$ notwendig verschieden von $\mathfrak{a}_1$, und wir gelangen so zu einer Basis $\mathfrak{B}_2 = (\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{b}_3, \ldots, \mathfrak{b}_n)$.

Insgesamt bedeutet dies aber, dass wir fortfahren können, bis schließlich auch $\mathfrak{b}_n$ ersetzt ist. Somit besitzt $\mathfrak{A}$ mindestens n-Elemente.

Da $\mathfrak{A}$ als Basis, insbesondere also ℓu vorausgesetzt war, besitzt $\mathfrak{A}$ aber auch nur die Elemente $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, da jedes weitere $\mathfrak{a} \in \mathfrak{A}$ müsste ja $\mathfrak{a} \propto (\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \subseteq \mathfrak{A} - \{\mathfrak{a}\}$ erfüllen müsste. □

1. 3. 5 Definition. Sei $\mathfrak{V}$ endlich erzeugt. Dann bezeichnen wir die eindeutig bestimmte, allen Basen gemeinsame **Länge** als die **Dimension** von $\mathfrak{V}$, i. Z. $\dim(\mathbf{V})$.

Analog sprechen wir von der Dimension einer Hülle, etwa von $\dim([\mathfrak{A}])$.

Es ist also nach den beiden letzten Sätzen jeder endlich erzeugte Vektorraum (auch) endlich-dimensional und jeder endlich-dimensionale Vektorraum (natürlich auch) endlich erzeugt.

Die große Bedeutung der Existenz einer Basis $\mathfrak{B}$ zu $\mathbf{V}$ liegt darin, dass sie für jeden Vektor $\mathfrak{x}$ aus $\mathfrak{V}$ eine eindeutig bestimmte Darstellung

$$\mathfrak{x} = x_1\mathfrak{b}_1 + \cdots + x_n\mathfrak{b}_n \qquad (b_i \in \mathfrak{B})$$

sichert. Denn es gilt:

1. 3. 6 Lemma. *Sei* $\mathbf{V}$ *ein* $\mathcal{K}$*-Vektorraum. Dann ist* $\mathfrak{A}$ *genau dann* ℓu*, wenn gilt*

$$\mathfrak{A} = \emptyset \ \vee \ \sum x_i\mathfrak{a}_i = \sum y_i\mathfrak{a}_i \Longrightarrow x_i = y_i \quad (x_i, y_i \in K,\ \mathfrak{a}_i \in \mathfrak{A},\ 1 \leq i \leq n).$$

BEWEIS. (a) Sei $\mathfrak{A}$ ℓu und sei $\mathfrak{A} \neq \emptyset$. Dann gilt:

$$\begin{aligned} \sum x_i\mathfrak{a}_i = \sum y_i\mathfrak{a}_i \ &\Longrightarrow \ \sum (x_i - y_i)\mathfrak{a}_i = \mathfrak{o} \\ &\rightsquigarrow \ x_i - y_i = 0 \ \ (1 \leq i \leq n) \\ &\rightsquigarrow \ x_i = y_i. \end{aligned}$$

(b) Sei hiernach die Bedingung des Satzes erfüllt. Ist $\mathfrak{A} = \emptyset$, so ist nichts zu zeigen. Ist $\mathfrak{A}$ hingegen nicht leer, so erhalten wir insbesondere

$$\mathfrak{o} = \sum x_i\mathfrak{a}_i = \sum 0\mathfrak{a}_i \Longrightarrow x_i = 0 \quad (1 \leq i \leq n)$$

und damit die lineare Unabhängigkeit von $\mathfrak{A}$. □

Hiernach lässt sich formulieren:

1. 3. 7 Der Darstellungssatz. *Sei* $\mathbf{V}$ *ein endlich erzeugter Vektorraum. Dann ist die Struktur von* $\mathbf{V}$ *eindeutig festgelegt durch die Dimension von* $\mathbf{V}$ *und die Struktur des Körpers der Skalare.*

Insbesondere hat sich ergeben: Ist $\mathfrak{B}$ *eine Basis von* $\mathbf{V}$*, so können wir die einzelnen Vektoren aus* $\mathbf{V}$ *„kodieren" vermöge*

$$\mathfrak{x} = \sum x_i\mathfrak{b}_i \ \ (b_i \in B) =: \langle x_1, \ldots, x_n \rangle$$

d.h. so lassen sich die Vektoren aus $\mathbf{V}$ *auch auffassen als* n*-tupel von Skalaren, die wir bei vorgegebener Basis auch bezeichnen als* **Koordinaten**.

Theorie der endlich erzeugten Vektorräume ist also nichts anderes als Theorie der n**-tupel-Vektorräume**

mit

$$\begin{aligned} \langle x_1, \ldots, x_n \rangle \oplus \langle y_1, \ldots, y_n \rangle &= \langle x_1 + y_1, \ldots, x_n + y_n \rangle \\ \text{und} \qquad s \odot \langle y_1, \ldots, y_n \rangle &= \langle s \cdot y_1, \ldots, s \cdot y_n \rangle. \end{aligned}$$

Sie sollen im folgenden symbolisiert werden mittels $\mathcal{K}^n$.

Hinweis für den Anfänger: Man beachte, dass nach dem Darstellungssatz ein erfreulicher Anschluss an die Linal der Oberstufe gwonnen ist.

1.4 Austausch und Ausdehnung

Wir fahren fort mit einigen wichtigen Fakten über endlich erzeugte Vektorräume.

Zunächst:

1. 4. 1 Der Steinitz**sche Austauschsatz.** *Sei* $\mathbf{V}$ *ein Vektorraum, u. a. mit der Basis* $\mathfrak{B} = (\mathfrak{b}_1, \ldots, \mathfrak{b}_n)$ *und sei* $\mathfrak{A} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_m)$ *ℓu. Dann gibt es eine Basis*

$$(\mathfrak{a}_1, \ldots, \mathfrak{a}_m, \mathfrak{c}_1, \ldots, \mathfrak{c}_{n-m})$$

mit $\mathfrak{c}_i \in \mathfrak{B}\,(1 \leq i \leq n-m)$*, also anschaulich: dann lässt sich ein Teil der Vektormenge* $\mathfrak{B}$ *austauschen gegen die Vektormenge* $(\mathfrak{a}_1, \ldots, \mathfrak{a}_m)$.

BEWEIS. Sind alle $\mathfrak{b}_i\,(1 \leq i \leq n)$ linear abhängig von $(\mathfrak{a}_1, \ldots, \mathfrak{a}_m)$, so ist $(\mathfrak{a}_1, \ldots, \mathfrak{a}_m)$ eine Basis, und wir sind am Ziel.

Sonst aber haben wir zunächst ein $\mathfrak{c}_1 \in \mathfrak{B}$ mit $\mathfrak{c}_1 \not\propto (\mathfrak{a}_1, \ldots, \mathfrak{a}_m)$, so dass nach dem Unabhängigkeitslemma die Menge $(\mathfrak{a}_1, \ldots, \mathfrak{a}_m, \mathfrak{c}_1)$ ℓu ist, und wir sind fertig, wenn $[\,\mathfrak{a}_1, \ldots, \mathfrak{a}_m, \mathfrak{c}_1\,] = \mathfrak{V}$ erfüllt ist. Andernfalls aber können wir fortfahren ... □

Insbesondere hat sich ergeben, dass keine ℓu Teilmenge mehr als n Elemente besitzen kann, und es gilt mit 1.4.1 in schwächerer Version auch

1. 4. 2 Der Ausdehnungssatz. *Jedes ℓu $\mathfrak{A}$ eines endlich erzeugten Vektorraumes lässt sich ausdehnen zu einer Basis.*

Ferner resultiert aus den beiden letzten Sätzen der wichtige Sachverhalt:

1. 4. 3 Proposition. *Ist* $\mathbf{U}$ *ein Unterraum des endlich-dimensionalen Vektorraums* $\mathbf{V}$ *und gilt* $\dim \mathbf{U} = \dim \mathbf{V}$*, so folgt* $\mathbf{U} = \mathbf{V}$*.*

DENN: ist $\mathfrak{B}_u$ eine Basis zu $\mathbf{U}$, so lässt sich $\mathfrak{B}_u$ ausdehnen zu einer Basis von $\mathbf{V}$. Also ist $\mathfrak{B}_u$ auch Basis zu $\mathbf{V}$. □

1.5 Zerlegungsaspekte

1. 5. 1 Definition. Seien $\mathfrak{U}$ und $\mathfrak{W}$ nicht leer und abgeschlossen in $\mathbf{V}$. Dann verstehen wir unter der Summe von $\mathfrak{U}$ und $\mathfrak{W}$ die Menge

$$\mathfrak{U} + \mathfrak{W} \;:=\; \{\mathfrak{x} \,|\, \mathfrak{x} = \mathfrak{u} + \mathfrak{w},\ \mathfrak{u} \in \mathfrak{U} \ \&\ \mathfrak{w} \in \mathfrak{W}\}.$$

1. 5. 2 Proposition. *Seien* $\mathbf{U}, \mathbf{W}$ *Unterräume von* $\mathbf{V}$*. Dann ist* $\mathfrak{U} + \mathfrak{W}$ *operativ abgeschlossen, weshalb wir auch vom Summenraum* $\mathbf{U} + \mathbf{W}$ *sprechen dürfen.*

BEWEIS. Wir haben

$$\begin{aligned} (\mathfrak{u}_1 + \mathfrak{w}_1) + (\mathfrak{u}_2 + \mathfrak{w}_2) &= (\mathfrak{u}_1 + \mathfrak{u}_2) + (\mathfrak{w}_1 + \mathfrak{w}_2), \\ s(\mathfrak{u} + \mathfrak{w}) &= s\mathfrak{u} + s\mathfrak{w}. \end{aligned}$$

□

Für den Summenraum gilt

1. 5. 3 Die 1. Dimensionsformel. *Sind* $\mathbf{U}$ *und* $\mathbf{W}$ *Unterräume von* $\mathbf{V}$*, so haben wir:*

$$\dim \mathbf{U} + \dim \mathbf{W} \;=\; \dim (\mathbf{U} + \mathbf{W}) + \dim (\mathbf{U} \cap \mathbf{W}).$$

Gilt $\mathfrak{U} \subseteq \mathfrak{W}$ oder $\mathfrak{W} \subseteq \mathfrak{U}$, so ist nichts zu zeigen, sonst aber schließen wir wie folgt:

BEWEIS. Wir wählen eine Basis $\mathfrak{B}$ zu $\mathbf{D} = \mathbf{U} \cap \mathbf{W}$ und verlängern $\mathfrak{B}$ das eine Mal zu einer Basis $\mathfrak{B}_U$ von $\mathbf{U}$, das andere Mal zu einer Basis $\mathfrak{B}_W$ von $\mathbf{W}$. Dann haben wir:

$$\begin{aligned} \mathfrak{B}_U \cap \mathfrak{B}_W &= \mathfrak{B} \\ \text{und es ist} \quad \mathfrak{B}_U \cup \mathfrak{B}_W &=: \mathfrak{C} \text{ Basis zu } \mathbf{U} + \mathbf{W}\,. \end{aligned}$$

Gehört nämlich $\mathfrak{x}$ zu $\mathfrak{B}_U \cap \mathfrak{B}_W$ so auch zu $\mathfrak{U} \cap \mathfrak{W} = \mathfrak{D}$, und folglich ist $\mathfrak{x}$ in diesem Falle ℓa von $\mathfrak{B}$. $\mathfrak{B}_U$ und $\mathfrak{B}_W$ sind aber ℓu. Folglich liegt $\mathfrak{x}$ sogar in $\mathfrak{B}$, was $\mathfrak{B}_U \cap \mathfrak{B}_W \subseteq \mathfrak{B} \subseteq \mathfrak{B}_U \cap \mathfrak{B}_W$ bedeutet. Also gilt die erste Behauptung.

Bleibt zu zeigen, dass $\mathfrak{C}$ Basis ist zu $\mathbf{U} + \mathbf{W}$. Hierzu genügt aber wegen $[\,\mathfrak{B}_U \cup \mathfrak{B}_W\,] = \mathfrak{U} + \mathfrak{W}$ der Nachweis der linearen Unabhängigkeit von $\mathfrak{C}$.

Sei also

$$\sum x_i \mathfrak{c}_i \;=\; \mathfrak{o} \;\; (\mathfrak{c} \in \mathfrak{C})$$

und sei ferner diese Darstellung nicht trivial. Dann muss sowohl ein Element $\mathfrak{c}_u$ aus $\mathfrak{U} - \mathfrak{D}$ als auch ein Element $\mathfrak{c}_w$ aus $\mathfrak{W} - \mathfrak{D}$ effektiv (d.h. mit nicht verschwindendem Koeffizienten) in die Darstellung von $\mathfrak{o}$ eingehen, da andernfalls $\mathfrak{B}_W$ bzw. $\mathfrak{B}_U$ nicht ℓu wäre. Das führt aber zum Widerspruch.

Denn fasst man die Glieder aus $\mathfrak{U} - \mathfrak{D}$ zusammen zu $\mathfrak{u}$ und bringt $\mathfrak{u}$ auf die eine Seite, alle übrigen Summanden hingegen auf die andere Seite, so wird klar, dass $\mathfrak{u}$ in $\mathfrak{U}$ und auch in $\mathfrak{W}$, also in $\mathfrak{D}$ liegen müsste, was bedeuten würde, dass $\mathfrak{u}$ eine Darstellung über $\mathfrak{B}$ und auch eine Darstellung über $\mathfrak{B}_U - \mathfrak{B}$ besäße. □

Weiter zeigen wir:

1. 5. 4 Proposition. *Ist* $\mathbf{V}$ *endlich-dimensional, so existiert zu jedem Unterraum* $\mathbf{U}$ *von* $\mathbf{V}$ *ein Unterraum* $\overline{\mathbf{U}}$ *von* $\mathbf{V}$ *mit*

$$\mathfrak{U} \cap \overline{\mathfrak{U}} = \mathfrak{O} \quad \textit{und} \quad \mathfrak{U} + \overline{\mathfrak{U}} = \mathfrak{V}\,.$$

BEWEIS. Sei $\mathfrak{B}_U$ Basis zu $\mathbf{U}$ und $\mathfrak{B}_V \supseteq \mathfrak{B}_U$ Basis zu $\mathbf{V}$. Dann leistet der Unterraum $\overline{\mathbf{U}} := ([\,\mathfrak{B}_V - \mathfrak{B}_U\,]\,, \oplus\,, \odot)$ das Gewünschte. □

Die besondere Bedeutung von 1.5.4 liegt darin, dass die Struktur von $\mathbf{V}$ durch diesen Satz zurückgeführt wird auf die Struktur der Unterräume

U und **W**. Dies ist im endlich-dimensionalen Fall evident, gilt aber auch allgemien in folgendem Sinne:

1. 5. 5 Proposition. *Sei* **V** *ein beliebiger Vektorraum. Dann gilt genau dann*

$$\mathfrak{U} \cap \mathfrak{W} = \mathfrak{O} \quad \textit{und} \quad \mathfrak{U} + \mathfrak{W} = \mathfrak{V},$$

wenn sich jedes $\mathfrak{x} \in \mathfrak{V}$ *eindeutig darstellen lässt als Summe* $\mathfrak{u}+\mathfrak{w}$ *mit* $\mathfrak{u} \in \mathfrak{U}$ *und* $\mathfrak{w} \in \mathfrak{W}$.

BEWEIS. (a) Gelte $\mathfrak{U} \cap \mathfrak{W} = \mathfrak{O}$ und $\mathfrak{U} + \mathfrak{W} = \mathfrak{V}$. Dann folgt zunächst mit geeigneten Vektoren $\mathfrak{u} \in \mathfrak{U}$, $\mathfrak{w} \in \mathfrak{W}$:

$$\begin{array}{rcl} \mathfrak{x} & \in & \mathfrak{V} \\ & \Longrightarrow & \\ \mathfrak{x} & = & \mathfrak{u} + \mathfrak{w} \end{array}$$

Sei nun zusätzlich $\mathfrak{x} = \mathfrak{u}_1 + \mathfrak{w}_1$.

Dann erhalten wir

$$\begin{array}{rcl} \mathfrak{u}_1 - \mathfrak{u} & = & \mathfrak{w}_1 - \mathfrak{w} \\ & \in & \mathfrak{U} \cap \mathfrak{W} = \mathfrak{O}. \\ & \rightsquigarrow & \\ \mathfrak{u}_1 - \mathfrak{u} = \mathfrak{o} & & = \mathfrak{w}_1 - \mathfrak{w} \\ & \rightsquigarrow & \\ \mathfrak{u}_1 = \mathfrak{u} & \& & \mathfrak{w}_1 = \mathfrak{w} \end{array}$$

(b) Gelte hiernach umgekehrt die Bedingung des Satzes. Dann ist $\mathfrak{U} + \mathfrak{W} = \mathfrak{V}$ evident, und es folgt:

$$\begin{array}{rcl} \mathfrak{x} \in \mathfrak{U} \cap \mathfrak{W} \Longrightarrow \mathfrak{x} & = & \mathfrak{x} + \mathfrak{o} \ \ (\mathfrak{x} \in \mathfrak{U},\ \mathfrak{o} \in \mathfrak{W}) \\ & = & \mathfrak{o} + \mathfrak{x} \ \ (\mathfrak{o} \in \mathfrak{U},\ \mathfrak{x} \in \mathfrak{W}) \\ \Longrightarrow \mathfrak{x} & = & \mathfrak{o}. \end{array}$$

□

Mit anderen Worten haben wir damit erhalten:

Ist $\mathfrak{U} \cap \mathfrak{W} = \mathfrak{O}$ und $\mathfrak{U} + \mathfrak{W} = \mathfrak{V}$, so können wir die Vektoren aus $\mathfrak{V}$ kodieren durch Paare $(\mathfrak{u}, \mathfrak{w})$ $(\mathfrak{u} \in \mathfrak{U},\ \mathfrak{w} \in \mathfrak{W})$.

Wir schreiben dann auch statt $\mathbf{U} + \mathbf{W}$ etwa $\mathbf{U} \oplus \mathbf{W}$ und sagen:

V lässt sich **direkt zerlegen** in **U** und **W**.

bzw. **V** ist **direkte Summe** von **U** und **W** .

Wir beenden diesen Abschnitt mit einem Gesetz für den **Verband** aller Unterräume, betrachtet bezüglich + und ∩.

1. 5. 6 Proposition. *Sind* $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$ *Unterräume eines endlich-dimensionalen Vektorraumes* $\mathbf{V}$*, so gilt das Verbands-Gesetz der* **Modularität** [2)]

(M) $$\mathfrak{X} \supseteq \mathfrak{Z} \implies \mathfrak{X} \cap (\mathfrak{Y} + \mathfrak{Z}) = (\mathfrak{X} \cap \mathfrak{Y}) + \mathfrak{Z}.$$

BEWEIS. Wegen $\mathfrak{X} \supseteq \mathfrak{Z}$ folgt unmittelbar

$$\mathfrak{X} \cap (\mathfrak{Y} + \mathfrak{Z}) \supseteq (\mathfrak{X} \cap \mathfrak{Y}) + \mathfrak{Z}.$$

Sei nun $\mathfrak{v} \in \mathfrak{X} \cap (\mathfrak{Y} + \mathfrak{Z})$. Dann besitzt $\mathfrak{v}$ eine Darstellung

$$\mathfrak{v} = \mathfrak{y} + \mathfrak{z} \quad \text{mit} \quad \mathfrak{z} \in \mathfrak{X},\ \mathfrak{y} \in \mathfrak{Y},$$

also auch mit $\mathfrak{y} = \mathfrak{v} - \mathfrak{z} \in \mathfrak{X}$ und folglich eine Darstellung

$$\mathfrak{v} = \mathfrak{y} + \mathfrak{z} \quad \text{mit} \quad \mathfrak{y} \in \mathfrak{X} \cap \mathfrak{Y},\ \mathfrak{z} \in \mathfrak{Z}.$$

Das bedeutet aber

(M) $$\mathfrak{X} \cap (\mathfrak{Y} + \mathfrak{Z}) \subseteq (\mathfrak{X} \cap \mathfrak{Y}) + \mathfrak{Z}$$

und damit die Behauptung. □

Hinweis für Liebhaber: In der **Verbandstheorie** wird gezeigt, dass die oben bewiesene Dimensionsformel eine Folge des Gesetzes (M) der **Modularität** ist – siehe hierzu das Skriptum über Geordnetes – also weniger ein Gesetz der linearen Algebra als ein solches der **Ordnungstheorie** ist.

1.6 Abstrakte Abhängigkeit *

In unsere bisherigen Betrachtungen ging ganz wesentlich ein, dass $\mathbf{V}$ endlich erzeugt sein sollte. Wollen wir auf diese Voraussetzung verzichten, kommen wir natürlich ohne einen Ersatz für diese Voraussetzung nicht sehr weit. Wir finden aber – in der Tat – einen angemessenen Ersatz im

[2)] Man beachte, dass dieses Gesetz Der Modularität durch einfaches Umschreiben übergeht in das Gesetz: $\mathfrak{X} \subseteq \mathfrak{Z} \Longrightarrow \mathfrak{X} + (\mathfrak{Y} \cap \mathfrak{Z}) = (\mathfrak{X} + \mathfrak{Y}) \cap Z$, d. h. dass es selbstdual ist ! Man vertausche X und Z und lese die beiden Seiten der Implikation jeweils von rechts nach links.

ZORNschen Lemma. Dieses „Lemma" ist äquivalent zu der Annahme, dass es zu jeder Familie nicht leerer **paarweise disjunkter Mengen** mindestens eine Auswahlmenge gibt, d. h. eine Menge, die aus jeder der vorgegebenen Mengen genau ein Element enthält, und es darf als optimaler „Endlichkeitsersatz" der Strukturmathematik angesehen werden. Es wurde benannt nach dem deutschen Mathematiker MAX ZORN, der dieses Lemma in den Dreißigern für den Sonderfall der *Ideale eines Ringes mit 1* formulierte.

1. 6. 1 Das Zorn'sche Lemma. *Sei* $\mathfrak{S} = S_i \;\; i \in I$ *eine Familie von Teilmengen der Menge* M*, derart, dass mit jeder* **Kette** *– d. h. mit jedem Teilsystem* $A_i \;\; (i \in I)$ *aus* $\mathfrak{S}$*, dessen Mengen paarweise vergleichbar sind – auch die* **Vereinigungsmenge** $\bigcup A_i \;\; (i \in I)$ *zu* $\mathfrak{S}$ *gehört. Dann gibt es in* $\mathfrak{S}$ *mindestens eine* **maximale Menge***, d. h. eine Menge, die in keiner anderen Menge der Familie echt enthalten ist.*

Im folgenden wird das ZORNsche Lemma an zwei Stellen zum Tragen kommen, und zwar zum einen bei der Konstruktion einer Basis, zum anderen beim Nachweis der eindeutigen Bestimmtheit der Basislänge.

Wie oben gezeigt wurde, erfüllt die lineare Abhängigkeitsrelation in $\mathbf{V}$ die vier Gesetze (LA1),..., (LA4), und wie der aufmerksame Leser schon dort beobachten konnte, lässt sich im Falle endlich erzeugter Vektorräume der Basissatz rein formal herleiten – beachte 1.15, 1.16. Das hat seinen Grund darin, dass die spezielle Abhängigkeitsrelation in Vektorräumen zwar in der Sprache der Vektorräume erklärt wurde, dass die Regeln (LA1),..., (LA4) aber keinen Bezug auf die Struktur des Vektorraums nehmen.

Deshalb ist es möglich, den Basissatz aus den Regeln (LA1),...,(LA4) unter ausschließlicher Bezugnahme auf die abstrakte Relation $\propto$ herzuleiten.

Hierzu starten wir von einer beliebigen Menge M, auf der eine „Relation" $\propto$ zwischen den Elementen von M und den Teilmengen von M so erklärt sei, dass die Regeln (LA1),...,(LA4) erfüllt sind.

Ein Beispiel für eine solche Relation wäre die vertraute lineare Abhängigkeit in Vektorräumen, ein weiters Beispiel wäre die Beziehung $a \in A$, und wieder ein anderes Beispiel liefert uns die Beziehung $a \propto A \;\; (\forall A \subseteq M)$.

Wir definieren nun als erstes die Hülle $[\,A\,]$ von A mittels:

$$[\,A\,] \;:=\; \{x \,|\, x \propto A\}.$$

Mittels $[\,A\,]$ können wir $a \propto A$ dann auch „synonym" notieren vermöge:

$$a \propto A \iff a \in [\,A\,].$$

und es gilt nach (LA2) – offenbar –

$$a \propto [\,A\,] \implies a \in [\,A\,],$$

in Worten $[\,A\,]$ ist **abgeschlossen**. Definieren wir abgeschlossen im Sinne der Implikation $a \propto A \Longrightarrow a \in A$, so folgt offenbar $[\,A\,] = \bigcap A_i$ $(A \subseteq A_i \;\&\; A_i$ abgeschlossen$)$.

Hiernach erklären wir völlig analog zum Sonderfall.

1. 6. 2 Definition. $B \subseteq M$ heiße unabhängig, wenn es in B kein b gibt mit $b \propto B - \{b\}$. $A \subseteq M$ heiße abhängig, wenn A nicht unabhängig ist. $B \subseteq M$ heiße eine Basis, wenn $[\,B\,] = M$ und B unabhängig ist.

Dies liefert sukzessive:

1. 6. 3 Lemma. *Ist $A \subseteq M$ abhängig, so gibt es ein endliches $E \subseteq A$, das ebenfalls abhängig ist.*

BEWEIS. Übung □

1. 6. 4 Lemma. *$B \subseteq M$ ist unabhängig gdw. jede endliche Teilmenge von B unabhängig ist.*

BEWEIS. Übung □

1. 6. 5 Lemma. *Ist B unabhängig und gilt $a \propto B$, so ist auch $(B, a) := B \cup \{a\}$ unabhängig.*

BEWEIS. Übung □

Damit sind die Voraussetzungen für den allgemeinen Basissatz gegeben.

1. 6. 6 Der Allgemeine Basissatz. *Sei $\propto$ eine Abhängigkeitsrelation zwischen M und seiner* **Potenzmenge** $\mathfrak{P}(M)$ *(der Menge aller Teilmengen von M). Dann besitzt M eine Basis bezüglich $\propto$.*

BEWEIS. Sei B_i $(i \in I)$ eine Kette von unabhängigen Teilmengen aus M. Dann ist auch $\bigcup B_i$ $(i \in I)$ unabhängig. Denn im andern Fall gäbe es eine endliche abhängige Teilmenge von B, etwa $\{b_1, \ldots, b_n\} =: E$ und daher mindestens ein B_i, das E enthält, also abhängig wäre.

Somit existiert nach dem ZORNschen Lemma eine maximale unabhängige Teilmenge B in M.

Wir zeigen: B ist Basis.

Da B unabhängig ist, bleibt nur nachzuweisen, dass $M = [\, B\,]$ erfüllt ist.

Wir führen diesen Beweis indirekt und nehmen an, es gäbe ein $a \in M$ mit $a \not\propto B$. Dann wäre nach Lemma 1.6.5 auch $\{B, a\}$ (noch) unabhängig, mit Widerspruch zur Maximalität von B. Folglich muss a abhängig sein von B. □

Anmerkung. Der soeben geführte Beweis basiert u.a. auf der Tatsache, dass die leere Menge zwangsläufig unabhängig ist.

Ganz analog hätte man jedoch auch ausgehen können von einer Kette B_i mit $B_i \supseteq C$ $(\forall i)$ und unabhängigem C.

Somit gilt

1. 6. 7 Der Ausdehnungssatz. *Ist $\propto$ eine Abhängigkeitsrelation in M, so lässt sich jedes unabhängige C ausdehnen zu einer Basis.*

Wir haben mit Hilfe des ZORNschen Lemmas „einen allgemeinen Basissatz" bewiesen. Tatsächlich bedeutet dies aber nur den Nachweis eines zum ZORNschen Lemma äquivalenten Sachverhalts. Denn, es gilt in der Tat:

1. 6. 8 Proposition. *Sei A_i $(i \in I)$ eine Familie paarweise disjunkter nicht leerer Mengen. Bilden wir dann $M = \bigcup A_i$ und setzen*

$$x \propto A \;:\Longleftrightarrow\; \exists a \in A : \{x, a\} \subseteq A_i \;\; (\exists i \in I),$$

so liefert dies eine Abhängigkeitsrelation, und die Existenz einer Basis ist gleichbedeutend mit der Existenz einer Auswahlmenge.

BEWEIS. Übung □

Das bedeutet dann

1. 6. 9 Theorem. *Das* ZORN*sche Lemma ist äquivalent zum Allgemeinen Basissatz.*

Im endlichen Fall war die Länge der Basen eindeutig bestimmt und konnte deshalb als $\dim V$ definiert werden.

Wir zeigen nun

1. 6. 10 Der Dimensionssatz. *Sei $\propto$ eine Abhängigkeitsrelation auf M. Dann haben alle Basen gleiche Länge.*

BEWEIS. Existiert eine endliche Basis so schließen wir wie oben. Existiert hingegen keine endliche Basis B, so hängt jedes a einer vorgegebenen Basis A von einem endlichen $B_a \subseteq B$ ab, wenn B die oben konstruierte Basis bedeutet. Daher folgt:

$$|A| = |A||A| \;\geq\; |A||N| \geq |\bigcup B_a| \geq |B|$$

vgl. HALMOS: Naive Mengelehre. □

Nachbemerkung: Wie wir gesehen haben, sichert das ZORNsche Lemma für jeden Vektorraum eine Basis. Doch, wie wir ebenfalls sahen, ist der allgemeine Basissatz äquivalent zum ZORNschen Lemma. Das bedeutet im letzten, dass wir ebensogut an den Basissatz glauben könnten, wie an das ZORNsche Lemma.

Die Frage stellt sich, ob schon der Basissatz für Vektorräume äquivalent ist zum ZORNschen Lemma. Hier gilt zumindest nach HALPERN, Proc. AMS, 1968:

$$ZL \Longleftrightarrow (\mathfrak{V} = [\,\mathfrak{A}\,] \Rightarrow \mathfrak{A} \text{ enthält eine Basis}).$$

Ob hingegen auch der Basissatz für Vektorräume schon das ZORNsche Lemma impliziert, scheint bislang offen. Mit anderen Worten:

Der Basissatz für Vektorräume könnte schwächer sein als das ZORNsche Lemma. Daher scheint es klüger, den Basissatz für beliebige Vektorräume zu glauben als ihn zu beweisen.

1.7 Zornsches Lemma und Auswahlaxiom

Wir stellen im folgenden die Äquivalenz von Zornschem Lemma und Auswahlaxiom vor.

AUSWAHLAXIOM $\Rightarrow$ ZORN

Wir schließen indirekt und nehmen an, H sei eine nichtleere **Partialordnung** *ohne* **maximales Element**, in der jede nichtleere **Kette** K **nach oben begrenzt** ist. Die somit existierende obere Grenze einer Kette K bezeichnen wir mit $g(K)$. Jedem $x \in H$ ordnen wir nun die nichtleere Menge $S(x)$ derjenigen Elemente y zu, die x echt übertreffen. M sei die Menge aller Mengen $S(x)$. Nach dem Auswahlaxiom gibt es zu M eine **Funktion** φ, die aus jeder Menge $S(x)$ ein Element $\varphi(S(x)) \in S(x)$ auswählt. Wir setzen zur Abkürzung $\varphi(S(x)) =: f(x)$ und haben

$$x < f(x) \, .$$

H ist nach Voraussetzung nicht leer. Wir halten im folgenden ein Element a_0 von H fest.

Es soll nun eine Teilmenge Z von H eine **ZORNsche Menge** heißen, falls die drei folgenden Bedingungen erfüllt sind:

- (*i*) $a_0 \in Z$
- (*ii*) Mit jedem x liegt auch $f(x)$ in Z
- (*iii*) Mit jeder nicht leeren Kette K liegt auch deren obere Grenze $g(K)$ in Z.

Triviale Beispiele für ZORNsche Mengen sind etwa H selbst oder das **Ordnungsideal** $[a_0)$. Weiterhin ist natürlich der Durchschnitt Z_0 aller ZORNschen Mengen eine ZORNsche Menge, was unmittelbar daraus folgt, dass der Mengendurchschnitt Implikationen *mitnimmt*.

Somit ist Z_0 die *engste* ZORNsche Menge, und es liegt jedes Element aus Z_0 oberhalb von a_0.

Wir werden zeigen, dass Z_0 sogar eine Kette ist. Damit sind wir dann am Ziel, da mit $g(Z_0)$ auch $f(g(Z_0)) > g(Z_0)$ zu Z_0, was der Annahme, kein Element sei maximal, widerspricht.

Herleitung: Im folgenden verstehen wir unter z stets ein Element aus Z_0. Wir wollen ein Element a aus Z_0 **ausgezeichnet** nennen, wenn aus $z < a$ stets $f(z) \leq a$ folgt.

Natürlich ist a_0 ausgezeichnet, da es kein $z < a_0$ gibt.

Jedem ausgezeichneten Element a ordnen wir als Menge zu:

$$B(a) := \{z \leq a \vee f(a) \leq z\} \, .$$

Wir betrachten nun ein beliebiges ausgezeichnetes Element a:

(a) Wegen $a_0 \leq a$ ist $a_0 \in B(a)$.

(b) Ist $z \in B(a)$, so gilt einer der drei Fälle: $z \leq a, z = a$ oder $f(a) \leq z$.

Im ersten Falle schließen wir $f(z) \leq a$, da a ausgezeichnet ist. In den beiden anderen Fällen schließen wir unmittelbar $f(a) \leq f(z)$. Somit folgt in jedem der drei Fälle $f(z) \in B(a)$.

(c) K sei eine nichtleere Kette von Elementen aus $B(a)$. Wir unterscheiden zwei Fälle:

Liegen alle Elemente von K unterhalb a, so gilt auch $g(K) \leq a$, also wegen $g(K) \in Z_0$ auch $g(K) \in B(a)$.

Wenn es aber ein $k \in K$ mit $k \not\leq a$ gibt, so folgt $f(a) \leq k \leq g(K)$, also wieder $g(K) \in B(a)$.

Zusammenfassend zeigen (a), (b), (c), dass $B(a)$ für jedes ausgezeichnete Element a eine ZORNsche Menge bildet. Das bedeutet aber, dass jedes Element der kleinsten ZORNschen Menge Z_0 zu $B(a)$ gehört. Somit ist für jedes ausgezeichnete Element a die Menge $B(a)$ gleich Z_0, und es ist insbesondere jedes ausgezeichnete Element mit jedem anderen Element aus K vergleichbar.

Wir zeigen, dass die Menge A aller ausgezeichneten Elemente selbst eine ZORNsche Menge bildet und also gleich Z_o ist.

(a) Dass a_0 ausgezeichnet ist, haben wir schon oben gesehen.

(b) Mit a ist auch $f(a)$ ausgezeichnet. Dazu betrachten wir ein $z < f(a)$. Nach der soeben abgeschlossenen Überlegung gehört z zu $B(a)$, so dass entweder $z \leq a$ oder $f(a) \leq z$ erfüllt ist. Im vorliegenden Falle muss $z \leq a$ gelten. Ist hier nun zu, so ist nichts zu zeigen. Ist aber $z < a$, so folgt $f(z) \leq a$, da a ausgezeichnet ist.

(c) Sei hiernach K sei eine nichtleere Kette von ausgezeichneten Elementen. Wir haben noch zu zeigen, dass $g(K)$ ausgezeichnet ist. Sicher gehört $g(K)$ zu Z_0. Wir betrachten ein $z < g(K)$ und unterscheiden wieder zwei Fälle:

Gibt es ein $k \in K$ mit $z < k$, so ist $f(z) \leq k$, da k ausgezeichnet ist, und es folgt $f(z) \leq g(K)$.

Sonst aber folgt $k < z$ für alle $k \in K$, also $g(K) \leq z$ mit Widerspruch zu der Annahme $z < g(K)$.

Damit sind wir am Ziel.

Wir kommen nun zum Kehrsatz:

ZORN $\Rightarrow$ AUSWAHLAXIOM

Wir betrachten eine Familie A_i $(i \in I)$ paarweise disjunkter nicht leerer Mengen und definieren als partial geordnete Menge H die Menge aller Mengen, die aus jedem A_i höchstens ein Element enthalten.

H ist bezüglich $\subseteq$ partial geordnet, und es ist die Zornsche Bedingung erfüllt, wie der Leser sich klarmachen möge. Also existiert ein maximales Element in $(H, \subseteq)$, etwa A. Dieses A enthält dann aus jedem A_i $(i \in I)$ höchstens ein Element, und es enthält A aus jedem A_i auch mindestens ein Element. Denn, andernfalls könnten wir A *verlängern*.

Somit gilt unsere Behauptung im Falle paarweise disjunkter Mengen.

Sei hiernach A_i $(i \in I)$ nicht notwendig paarweise disjunkt. Dann lässt sich die Familie A_i $(i \in I)$ **verfremden**, indem man die Elemente aus A_i ersetzt durch die Paare (a, i).

Kapitel 2

Lineare Gleichungssysteme

2.1 Matrixaspekte

Sei $\mathcal{K}$ ein Körper. Dann bezeichnen wir als $m \times n$-**Matrix** über $\mathcal{K}$ jedes rechteckige Schema

$$\begin{pmatrix} a_{11} & \ldots\ldots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \ldots\ldots & a_{m,n} \end{pmatrix} =: (a_{i,k})$$

mit Elementen aus K, und wir bezeichnen ganz allgemein Matrizen über $\mathcal{K}$ mit großen lateinischen Buchstaben, hier etwa mit A.

Ist A eine $m \times n$-Matrix, so lassen sich die Zeilen $a_{i,1}, \ldots, a_{i,n}$ $(1 \leq i \leq m)$ auffassen als Elemente des $\mathcal{K}^n$ und analog die Spalten $a_{1,k}, \ldots, a_{m,k}$ $(1 \leq k \leq n)$ als Elemente des $\mathcal{K}^m$.

Seien nun $\mathfrak{a}$ und $\mathfrak{b}$ Vektoren aus $\mathbf{V} := \mathbf{K}^n$. Dann setzen wir

$$\mathfrak{a} \cdot \mathfrak{b} := a_1 b_1 + \cdots + a_n b_n$$

und nennen $\mathfrak{a}\,\mathfrak{b} := \mathfrak{a} \cdot \mathfrak{b}$ das **skalare Produkt** von $\mathfrak{a}$ und $\mathfrak{b}$ – im Gegensatz zum S-Produkt $s \cdot \mathfrak{a}$. [1)]

Offenbar erfüllt das skalare Produkt die Gesetze:

2. 1. 1 Lemma. $$s(\mathfrak{a} \cdot \mathfrak{b}) = (s\mathfrak{a}) \cdot \mathfrak{b}$$

und $$\mathfrak{a} \cdot (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cdot \mathfrak{b} + \mathfrak{a} \cdot \mathfrak{c}.$$

[1)] Im weiteren werden wir das Symbol $\cdot$ großzügig simultan für die Multiplikation von Skalaren, für die S-Multiplikation und auch für das skalare Produkt verwenden.

Sei A eine $m \times n$-Matrix mit den **Zeilenvektoren** $\mathfrak{a}_i$ $(1 \leq i \leq m)$. Dann verstehen wir unter $A \cdot \mathfrak{x}$ den Vektor $(\mathfrak{a}_1 \cdot \mathfrak{x}, \ldots, \mathfrak{a}_m \cdot \mathfrak{x})$, auch bezeichnet mit $A\,\mathfrak{x}$. Daher lässt sich die Gleichungsforderung

$$\begin{aligned} a_{11}x_1 \,+\, a_{12}x_2 \,+\cdots+\, a_{1,n}\,x_n \quad &\doteq b_1 \\ \vdots& \\ a_{m,1}x_1 +\, a_{m,2}x_2 +\cdots+\, a_{m,n}x_n &\doteq b_m \end{aligned}$$

abkürzen zu

$$\text{LGS}: \quad A\mathfrak{x} \doteq \mathfrak{b} \quad \text{mit} \quad \mathfrak{b} = (b_1, \ldots, b_m),$$

und es kommt LGS dem *Auftrag* gleich, einen Vektor $\mathfrak{u} \in \mathcal{K}^n$ zu finden, der bei *Anwendung* von A auf $\mathfrak{u}$ den Vektor $\mathfrak{b}$ *als Bild erhält.*

Ist ein LGS gegeben, so bezeichnen wir A als die Matrix dieses Systems und $(A, \mathfrak{b})$, d. h. die um den **Spaltenvektor** $\mathfrak{b}$ *verlängerte* Matrix, als die **erweiterte Matrix** dieses LGS.

Sei (erneut) A eine $m \times n$-Matrix. Dann verstehen wir unter dem **Rang der Matrix** A die Dimension des von den Spaltenvektoren von A aufgespannten Unterraumes des $\mathbf{K}^m$. Da sich (zumindest) eine Basis dieses Unterraumes aus der Menge der Spaltenvektoren auswählen lässt , ist demzufolge der Rang von A – symbolisiert vermöge $\operatorname{rg} A$ – nichts anderes als die allen maximalen linear unabhängigen Teilmengen der Menge der Spaltenvektoren von A gemeinsame Anzahl.

Insbesondere bedeutet dies, dass wir beim Studium eines LGS im Falle $\operatorname{rg} A = r$ annehmen dürfen, dass die Spaltenvektoren $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ eine Basis des **Spaltenraumes** bilden, da Vertauschungen von Spalten in diesem Falle keine wesentliche Veränderung bedeuten.

Eine erste Antwort auf die Frage, wann ein LGS eine Lösung besitzt, erhalten wir gewissermaßen als *verbale Translation:*

2. 1. 2 Das Rangkriterium. *Die Forderung* $A\mathfrak{x} \doteq \mathfrak{b}$ *ist genau dann erfüllbar, wenn gilt:*

$$\operatorname{rg}(A) = \operatorname{rg}(A, \mathfrak{b}).$$

Offenbar ist $A\mathfrak{u} = \mathfrak{b} = A\mathfrak{v}$ äquivalent mit $A\mathfrak{u} = \mathfrak{b} \;\;\&\;\; A(\mathfrak{v} - \mathfrak{u}) = \mathfrak{o}$. Demzufolge beherrschen wir alle Lösungen zu $A\mathfrak{x} \doteq \mathfrak{b}$, wenn wir wenigstens

eine Lösung $\mathfrak{u}$ zu $A\mathfrak{x} \doteq \mathfrak{b}$ und alle Lösungen zu $A\mathfrak{x} \doteq \mathfrak{o}$ kennen – schreibe $\mathfrak{v} = \mathfrak{u} + (\mathfrak{v} - \mathfrak{u})$.

Aus diesem Grund schicken wir dem Studium von $A\mathfrak{x} \doteq \mathfrak{b}$, das wir im nächsten Abschnitt mittels des Gaußschen Algorithmus angehen werden, ein Studium von $A\mathfrak{x} \doteq \mathfrak{o}$ voraus.

2. 1. 3 Definition. Ein LGS $A\mathfrak{x} \doteq \mathfrak{b}$ heißt **homogen** im Falle $\mathfrak{b} = \mathfrak{o}$, andernfalls **inhomogen**.

2. 1. 4 Lemma. *Die Lösungsgesamtheit eines homogenen* LGS *bildet einen Unterraum des* $\mathbf{K}^n$*, genannt der* **Lösungsraum***, kurz der* **(LR)**.

DENN: Es ist $A\mathfrak{o} = \mathfrak{o}$, also $\mathfrak{o}$ ein **Lösungsvektor**, und es liegt mit $\mathfrak{y}$ auch $s\mathfrak{y}$ und mit $\mathfrak{u}$ und $\mathfrak{v}$ auch $\mathfrak{u} + \mathfrak{v}$ (bzw. $\mathfrak{u} - \mathfrak{v}$) im **LR** (LGS). □

$\operatorname{rg} A$ ist zwangsläufig nicht größer als n. Gilt sogar $\operatorname{rg} A =: r \leq n-1$, so hat das zu A korrespondierende LGS mindestens eine nichttriviale Lösung, da in diesem Falle wegen des Unabhängigkeitslemmas je $r+1$ Spaltenvektoren ℓa sind.

Wir interessieren uns für die Lösungsgesamtheit $\mathfrak{LR}$. Ist LGS homogen, so wissen wir schon, dass die Lösungsmenge von LGS einen Unterraum des $\mathbf{K}^n$ bildet, hingegen wissen wir noch nichts über dessen Dimension. Auskunft hierüber gibt

2. 1. 5 Proposition. *Sei* $A\mathfrak{x} \doteq \mathfrak{o}$ *ein* LGS *und* A *eine* $m \times n$*-Matrix* A *und* $\operatorname{rg} A = r$*. Dann hat der Lösungsraum* $\mathbf{LR} := \{\mathfrak{u} \mid A\mathfrak{u} = \mathfrak{o}\}$ *die Dimension* $n - r$*.*

BEWEIS. Ist der Rang von A gleich n, so existiert nur die triviale Lösung $\mathfrak{o}$ und $\mathfrak{O}$ hat die Dimension 0, da in diesem Falle die leere Menge $\emptyset$ Basis ist. Folglich gilt für $r = n$ die Formel $\dim(\mathbf{LR}) = 0 = n - r$.

Ist der Rang von A kleiner als n, so dürfen wir annehmen, dass die Menge der Spaltenvektoren $(\mathfrak{a}_1, \ldots, \mathfrak{a}_r)$ ℓu ist, hingegen alle $(\mathfrak{a}_1, \ldots, \mathfrak{a}_r, \mathfrak{a}_{r+i})$ ℓa sind $(1 \leq i \leq n - r)$. Dies führt mit geeigneten Koeffizienten $y_{\cdot,\cdot}$ zu

$$\begin{array}{rcrcccrcrcl}
y_{r+1,1} \cdot \mathfrak{a}_1 & + & y_{r+1,2} \cdot \mathfrak{a}_2 & + & \cdots & + & y_{r+1,r} \cdot \mathfrak{a}_r & + & 1 \cdot \mathfrak{a}_{r+1} & = & \mathfrak{o} \\
y_{r+2,1} \cdot \mathfrak{a}_1 & + & y_{r+2,2} \cdot \mathfrak{a}_2 & + & \cdots & + & y_{r+2,r} \cdot \mathfrak{a}_r & + & 1 \cdot \mathfrak{a}_{r+2} & = & \mathfrak{o} \\
\vdots & & & & & & & & & & \\
y_{n,1} \cdot \mathfrak{a}_1 & + & y_{n,2} \cdot \mathfrak{a}_2 & + & \cdots & + & y_{n,r} \cdot \mathfrak{a}_r & + & 1 \cdot \mathfrak{a}_n & = & \mathfrak{o}.
\end{array}$$

Somit sind die Vektoren

$$\mathfrak{y}_i := (y_{r+i,1}, \ldots, y_{r+i,r}, 0, \ldots, \underset{r+i}{1}, \ldots, 0),$$

mit 1 an der Stelle $r+i$, Lösungen zu LGS, und es ist

$$(\mathfrak{y}_1, \ldots, \mathfrak{y}_{n-r})$$

ℓu, so dass wir $\dim(\mathbf{LR}) \geq n-r$ erhalten.

Wir zeigen nun, dass auch $\dim(\mathbf{LR}) \leq n-r$ erfüllt ist. Dies wird sich daraus ergeben, dass jeder Lösungsvektor $\mathfrak{z}$ Linearkombination der $\mathfrak{y}_i$ $(1 \leq i \leq n-k)$ ist, was sich wie folgt herleitet:

Sei $A\mathfrak{z} = \mathfrak{o}$. Wir bilden zunächst den Vektor:

$$\mathfrak{u} := z_{r+1} \cdot \mathfrak{y}_1 + \cdots + z_n \cdot \mathfrak{y}_{n-r}$$

und hiernach den Vektor: $\mathfrak{w} := \mathfrak{z} - \mathfrak{u}$.

Dann stimmen $\mathfrak{u}$ und $\mathfrak{z}$ an den Stellen $r+1$ bis n überein, weshalb $\mathfrak{w}$ an diesen Stellen verschwindet. Es ist aber $\mathfrak{w}$ ein Lösungsvektor zu $A\mathfrak{x} \doteq \mathfrak{o}$. Deshalb ist

$$w_1 \cdot \mathfrak{a}_1 + w_2 \cdot \mathfrak{a}_2 + \ldots + w_r \cdot \mathfrak{a}_r = \mathfrak{o}$$

erfüllt und damit $w_1 = w_2 = \cdots = w_r = 0$, also insgesamt $\mathfrak{w} = \mathfrak{o}$ und folglich

$$\mathfrak{z} = \mathfrak{u} = \textstyle\sum_{k=1}^{n-r} z_{r+k} \cdot \mathfrak{y}_k\,,$$

bzw. $\mathfrak{z} \in [\,\mathfrak{y}_k\,] \quad (1 \leq k \leq n-r)$. □

Aus 2.1.4 und 2.1.5 ergibt sich als Zusammenfassung

2. 1. 6 Das homogene Lösungstheorem. *Ist* LGS *ein homogenes lineares Gleichungssystem mit einer $m \times n$-Matrix A vom Range r, so bildet die Lösungsmenge von* LGS *einen Lösungsraum* **LR** *der Dimension $n-r$.*

In 2.1.6 ging der Rang der Matrix A wesentlich ein. Er wurde definiert über die Spalten von A. Wir zeigen nun, dass $\operatorname{rg} A$ invariant ist gegenüber **Spiegelungen** von A an den **Diagonalen**. Genauer werden wir beweisen:

2. 1. 7 Proposition. *Sei A eine $m \times n$-Matrix über $\mathcal{K}$. Dann sind der zu A korrespondierende* **Spaltenraum** *und der zu A korrespondierende* **Zeilenraum** *von gleicher Dimension.*

BEWEIS. Offenbar sind die genannten Dimensionen invariant gegenüber Zeilen- bzw. Spaltenvertauschungen. Deshalb dürfen wir annehmen, dass die ersten r Spalten eine Basis des Spaltenraumes und die ersten s Zeilen eine Basis des Zeilenraumes bilden. Wir zeigen $r = s$. Hierzu genügt es, $r \leq s$ zu beweisen, man beachte: Spiegelung überführt Zeilen in Spalten (und Spalten in Zeilen).

Zum Zwecke des Beweises löschen wir alle Zeilen vom Index $s+1$ an und gelangen so zu A_s. Hierdurch ändert sich die Lösungsgesamtheit nicht, wegen $\mathbf{LR}(A_s) = \mathbf{LR}(A)$, weshalb auch $\operatorname{rg} A_s = \operatorname{rg} A$ erfüllt ist, man beachte 2.1.6

Nun hat aber A_s nur s Zeilen. Folglich haben die Spalten von A_s die Länge s, was

$$r = \operatorname{rg} A = \operatorname{rg} A_s \leq s$$

bedeutet, da im $\mathbf{K}^s$ je $s+1$ Vektoren ℓa sind. □

Ist $A = (a_{i,k})$ eine $m \times n$-Matrix, so versteht man unter $A^\top$ die transponierte $n \times m$-Matrix $(b_{k,i})$ mit $b_{k,i} = a_{i,k}$, also diejenige Matrix, die im Falle $n = m$ aus A durch Spiegelung an der Diagonalen $(11, 22, \ldots)$ hervorgeht.

2. 1. 8 Korollar. $\operatorname{rg} A = \operatorname{rg} A^\top$.

Wir wissen schon, dass die Lösungsgesamtheit eines LGS einen Unterraum des $\mathbf{K}^n$ bildet. Wir zeigen nun, dass auch umgekehrt jeder Unterraum des $\mathbf{K}^n$ als Lösungsraum eines LGS aufgefasst werden kann. [2]

2. 1. 9 Proposition. *Gilt $\mathfrak{U} \subseteq K^n$, so ist die Menge aller $\mathfrak{y}$ mit $\mathfrak{u} \cdot \mathfrak{y} = 0$ $(\forall \mathfrak{u} \in \mathfrak{U})$ abgeschlossen, und ist zudem auch $\mathfrak{U}$ selbst abgeschlossen, so folgt $\mathbf{U} = \mathbf{U}^{\perp\perp}$ $(:= (\mathbf{U}^\perp)^\perp)$. Dies bedeutet insbesondere, dass $\mathbf{U}$ für jede Basis $(\mathfrak{b}_1, \ldots, \mathfrak{b}_s)$ von $\mathbf{U}^\perp$ den Bedingungen genügt:*

$$\begin{aligned} \mathfrak{b}_1 \cdot \mathfrak{x} &\doteq 0 \\ &\vdots \\ \mathfrak{b}_s \cdot \mathfrak{x} &\doteq 0 \end{aligned}$$

[2] Der Leser beachte beim Repetieren an dieser Stelle auch die späteren Ausführungen zur Orthogonalität in Kapitel 10.

BEWEIS. Sei $(\mathfrak{a}_1, \ldots, \mathfrak{a}_p)$ Basis zu $\mathfrak{U} \subseteq K^n$. Dann ist $\mathfrak{y}$ Lösung zu

$$\begin{aligned} \mathfrak{a}_1 \cdot \mathfrak{x} &\doteq 0 \\ &\vdots \\ \mathfrak{a}_p \cdot \mathfrak{x} &\doteq 0 \end{aligned}$$

gdw. $$s_1 \cdot \mathfrak{a}_1\mathfrak{y} + \cdots + s_p \cdot \mathfrak{a}_p\mathfrak{y} = \mathfrak{o}$$

für alle $(s_1, \ldots, s_p)$ erfüllt ist, also genau dann, wenn $\mathfrak{y}$ **orthogonal** ist zu allen Vektoren

$$s_1 \cdot \mathfrak{a}_1 + \cdots + s_p \cdot \mathfrak{a}_p,$$

d. h. zu allen Vektoren aus $[\,\mathfrak{a}_1, \ldots, \mathfrak{a}_p\,] = \mathfrak{U}$.

Sei nun $[\,\mathfrak{b}_1, \ldots, \mathfrak{b}_{n-p}\,]$ eine Basis zu $\mathbf{U}^\perp$. Dann können wir analog $(\mathbf{U}^\perp)^\perp$ konstruieren, und es gilt $\mathbf{U} \subseteq (\mathbf{U}^\perp)^\perp$.

Nun ist aber $\dim \mathbf{U} = p$ und $\dim (\mathbf{U}^\perp)^\perp \leq n - (n-p) = p$. Das bedeutet dann

$$\dim \mathbf{U} = \dim (\mathbf{U}^\perp)^\perp \rightsquigarrow \mathbf{U} = (\mathbf{U}^\perp)^\perp .$$

□

2.2 Der Gauss'sche Algorithmus

Bislang fehlt uns ein praktisches Lösungsverfahren zu $A\mathfrak{x} \doteq \mathfrak{b}$. Um ein solches herzuleiten, beachten wir, dass Vertauschungen von Zeilen mit Zeilen und von Spalten mit Spalten natürlich keinen Einfluss auf die Lösungsgesamtheit nehmen. Deshalb dürfen wir von $a_{11} \neq 0$ ausgehen, falls $A \neq O$ erfüllt ist. Ferner ist die Lösungsgesamtheit von $A\mathfrak{x} \doteq \mathfrak{o}$ gleich der Lösungsgesamtheit von

$$\begin{aligned} \mathfrak{a}_1 \cdot \mathfrak{x} &\doteq 0 \\ (\mathfrak{a}_i - s\mathfrak{a}_1) \cdot \mathfrak{x} &\doteq 0 \qquad (2 \leq i \leq m), \end{aligned}$$

denn dies ergibt sich aus

$$\begin{aligned} \mathfrak{a}_i \cdot \mathfrak{x} - s\mathfrak{a}_1 \cdot \mathfrak{x} &= 0 \;\&\; \mathfrak{a}_i \cdot \mathfrak{x} = 0 \\ \Longrightarrow \mathfrak{a}_i \cdot \mathfrak{x} &= s\mathfrak{a}_1 \cdot \mathfrak{x} = 0 \end{aligned}$$

Daher gelangen wir ausgehend von $A\mathfrak{x} \doteq \mathfrak{o}$ zu einem

$$B\mathfrak{x} \doteq \mathfrak{o} \quad \text{mit} \quad b_{11} \neq 0 \ \ \& \ \ b_{i,1} = 0 \ \ (2 \leq i \leq m)$$

und bei Fortsetzung des Verfahrens sukzessive zu einem System

$$\begin{aligned} b_{11}\,x_1 + b_{12}\,x_2 + \ \cdots\cdots\cdots + b_{1,m}\,x_m + \ldots + b_{1,n}\,x_n &\doteq 0 \\ b_{22}\,x_2 + \ \cdots\cdots\cdots + b_{2,m}\,x_m + \ldots + b_{2,n}\,x_n &\doteq 0 \\ b_{33}\,x_3 + \cdots + b_{3,m}\,x_m + \ldots + b_{3,n}\,x_n &\doteq 0 \\ \ddots & \\ b_{m,m}\,x_m + \ldots + b_{m,n}\,x_n &\doteq 0. \end{aligned}$$

Somit gewinnen wir Lösungen zu dem LGS $A\mathfrak{x} \doteq \mathfrak{o}$, indem wir $x_{m-1}, \ldots, x_n$ beliebig wählen und durch *Aufrollen* des Systems $B\mathfrak{x} \doteq \mathfrak{o}$ von unten nach oben die Werte von $x_m, \ldots, x_1$ bestimmen.

Insbesondere erhalten wir eine Basis zum **LR** , indem wir sukzessive $x_j = 1$ und $x_k = 0$ setzen für $j = m+1, \ldots, n$, $j \neq k = m+1, \ldots, n$.

Sei nun $A\mathfrak{x} \doteq \mathfrak{b}$ gefordert und $\operatorname{rg} A = \operatorname{rg}(A, \mathfrak{b})$. Dann können wir analog verfahren, da die Lösungsgesamtheit zu $A\mathfrak{x} \doteq \mathfrak{b}$ und zu

$$\mathfrak{a}_1\mathfrak{x} \doteq b_1, \qquad (\mathfrak{a}_i - s\mathfrak{a}_1) \cdot \mathfrak{x} \doteq b_i - s\,b_1$$

übereinstimmen.

Weist das umgeformte Gleichungssystem n viele Gleichungen auf, so lassen sich die linken Seiten durch weitere **elementare Umformungen** jeweils nach x_i überführen, so dass der Vektor $\mathfrak{b}$ übergeht in den Lösungsvektor. Dies liefert u. a. eine Methode, zu einer $n \times n$-Matrix vom Rang n die **inverse Matrix** zu bestimmen, d. h. die Matrix A^{-1} mit $A \cdot A^{-1} = E = A^{-1} \cdot A$. Vergleiche hierzu die Schlussbemerkungen im Kapitel über Lineare Abbildungen

Wie sich ein vorgegebenes LGS **rechnerökonomisch** und möglichst genau *bewältigen* lässt, ist ein Problem der numerischen Mathematik und soll hier nicht näher diskutiert werden.

Leser, die an einer technik-orientierten Darstellung der LA interessiert sind, seien an dieser Stelle vor allem hingewiesen auf das Buch der Kollegen Burg/Haf/Wille, Höhere Mathematik für Ingenieure, Band 2, B. G. Teubner, Stuttgart, (Bibliothek der GhK).

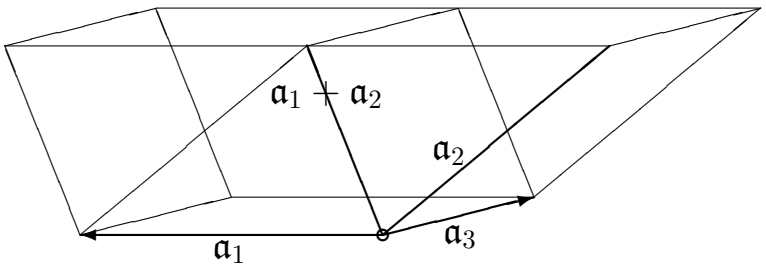
Leser, die an einer wirtschafts-orientierten Darstellung der LA interessiert sind, seien hingewiesen auf das Buch von TOUTENBURG, Lineare Modelle, Physica Verlag, Würzburg - Heidelberg, (Bibliothek der GhK).

Kapitel 3

Determinanten

3.1 Zum Volumenaspekt

Betrachten wir im $\mathbf{R}^3$ das von den Vektoren $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ aufgespannte **Parallelotop**



so gilt für dessen Volumen $V(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ offenbar:

$$
\begin{array}{lrcl}
(0) & V \text{ ist eine Funktion } (\mathbf{R}^n)^n & \longmapsto & \mathbf{R} \ \ (n = 3) \\
(1) & V(\mathfrak{a}_1, \ldots, \mathfrak{a}_i + \mathfrak{a}_k, \ldots, \mathfrak{a}_n) & = & V(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \ \ (i \neq k) \\
(2) & V(\mathfrak{a}_1, \ldots, s\,\mathfrak{a}_i, \ldots, \mathfrak{a}_n) & = & |\,s\,| \cdot V(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \\
(3) & V(\mathfrak{e}_1, \ldots, \mathfrak{e}_n) & = & 1 \\
(4) & V(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) & \geq & 0
\end{array}
$$

Demzufolge ist $(0), \ldots, (4)$ zu beachten, soll die **Volumenfunktion** soweit wie möglich in die Theorie der beliebigen n-dimensionalen Vektorräume $\mathbf{V}$ *herüber geholt* werden.

Indes, $||$ und $\geq$ machen in beliebigen Vektorräumen keinen Sinn, so dass wir uns mit weniger begnügen müssen, soll die Volumenfunktion in allgemeinen Vektorräumen *nachempfunden* werden. Deshalb schauen wir nach Funktionen, die im $\mathbf{R^n}$ aufs engste mit der Volumenfunktion assoziiert und zudem einer algebraischen Charakterisierung zugänglich sind.

Hierzu starten wir von einem beliebigen $\mathbf{K}^n =: \mathbf{V}$ oder, was dasselbe ist, von einem n-dimensionalen Vektorraum $\mathbf{V}$ bei vorgegebener **geordneter Basis** $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$. Auf diese Weise werden die Einheitsvektoren (des $\mathbf{R}^n$) erfasst, und wir kommen der Volumenfunktion sehr nahe mittels einer jeden Funktion $D: \mathfrak{V}^n \longmapsto K$, die den drei Bedingungen genügt:

$$\text{(D1)} \qquad D(\mathfrak{a}_1, \ldots, \mathfrak{a}_i + \mathfrak{a}_k, \ldots, \mathfrak{a}_n) = D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \ (i \neq k)$$

$$\text{(D2)} \qquad D(\mathfrak{a}_1, \ldots, s\,\mathfrak{a}_i, \ldots, \mathfrak{a}_n) = s \cdot D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$$

$$\text{(D3)} \qquad D(\mathfrak{e}_1, \ldots, \mathfrak{e}_n) = 1,$$

denn eine jede solche Funktion liefert – wie wir sehen werden – im Falle $\mathbf{V} = \mathbf{R^n}$ via $|D|$ eine Volumenfunktion.

Sei also $\mathbf{V}$ im folgenden ein $\mathbf{K}^n$ mit Basis $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$

3. 1. 1 Definition. Als **Determinantenfunktion** in $\mathbf{V} := \mathbf{K}^n$ bezeichnen wir jede Funktion $D: \mathfrak{V}^n \longmapsto K$, die den Bedingungen (D1), ..., (D3) genügt.

D ordnet also jedem n-tupel aus $\mathbf{V}$ einen Skalar aus K zu, den wir – wie üblich – mit $\det(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ oder auch mit $D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ notieren und als die **Determinante** (auch als den Determinantenwert) der Vektoren $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ bezeichnen.

Statt $D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ schreiben wir gelegentlich auch $D\begin{pmatrix} \mathfrak{a}_1 \\ \vdots \\ \mathfrak{a}_n \end{pmatrix}$. Daher ist zusätzlich auch

$$D\begin{pmatrix} a_{11}, \ldots, a_{1,n} \\ \vdots \\ a_{n,1}, \ldots, a_{n,n} \end{pmatrix}$$

eine mögliche Schreibweise. Verhältnismäßig leicht ergeben sich als erste Determinantenformeln:

(3.4) $$D(\mathfrak{a}_1, \ldots, \mathfrak{a}_i + s\,\mathfrak{a}_k, \ldots, \mathfrak{a}_n) = D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \;\; (i \neq k).$$

DENN:

$$\begin{aligned} & D(\mathfrak{a}_1, \ldots, \mathfrak{a}_i + s\,\mathfrak{a}_k, \ldots, \mathfrak{a}_k, \ldots, \mathfrak{a}_n) \\ = \;& -\tfrac{1}{s} \cdot D(\mathfrak{a}_1, \ldots, \mathfrak{a}_i + s\,\mathfrak{a}_k, \ldots, -s\mathfrak{a}_k, \ldots, \mathfrak{a}_n) \\ = \;& -\tfrac{1}{s} \cdot D(\mathfrak{a}_1, \ldots, \mathfrak{a}_i, \ldots\ldots, -s\,\mathfrak{a}_k, \ldots, \mathfrak{a}_n) \\ = \;& D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n). \end{aligned}$$

□

(3.5) $$D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) = D(\mathfrak{a}_1, \ldots, \mathfrak{a}_i + \sum_{i \neq k} s_k\,\mathfrak{a}_k, \ldots, \mathfrak{a}_n),$$

DENN: beachte (3.4). □

(3.6) $$D(\mathfrak{a}_1, \ldots, \mathfrak{o}, \ldots, \mathfrak{a}_n) = 0\,.$$

DENN: beachte (D2). □

3. 1. 2 Das Additionstheorem.

$$\begin{aligned} & D(\mathfrak{a}_1, \ldots, \mathfrak{b}_i, \quad \ldots, \mathfrak{a}_n) \\ + \;& D(\mathfrak{a}_1, \ldots\ldots, \quad \mathfrak{c}_i, \ldots, \mathfrak{a}_n) \\ = \;& D(\mathfrak{a}_1, \ldots, \mathfrak{b}_i + \mathfrak{c}_i, \ldots, \mathfrak{a}_n)\,. \end{aligned}$$

BEWEIS. Wir wählen o.B.d.A. $i = 1$.

Sei nun zunächst $\{\mathfrak{a}_2, \ldots, \mathfrak{a}_n\}$ ℓa, dann ist nach (3.5) und (3.6) nichts zu zeigen, da alle drei aufgeführten Determinanten verschwinden.

Ist aber $\{\mathfrak{a}_2, \ldots, \mathfrak{a}_n\}$ ℓu, so gibt es eine Basis $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$, die ihrerseits Darstellungen der Art

$$\begin{aligned} \mathfrak{b}_1 &= s_1\,\mathfrak{a}_1 + \cdots + s_n\,\mathfrak{a}_n \\ \mathfrak{c}_1 &= t_1\,\mathfrak{a}_1 + \cdots + t_n\,\mathfrak{a}_n \end{aligned}$$

gewährleistet, die zu den Gleichungen

$$\begin{aligned} D(\mathfrak{b}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n) &= s_1 \cdot D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \\ D(\mathfrak{c}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n) &= t_1 \cdot D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \\ D(\mathfrak{b}_1 + \mathfrak{c}_1, \ldots, \mathfrak{a}_n) &= (s_1 + t_1) \cdot D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \end{aligned}$$

führen. □

3. 1. 3 Das Vertauschungslemma. *Vertauscht man zwei Zeilen, so springt das Vorzeichen um, formal: ist $i \neq k$, so gilt:*

$$D(\mathfrak{a}_1, \ldots, \mathfrak{a}_i, \ldots, \mathfrak{a}_k, \ldots, \mathfrak{a}_n) = -D(\mathfrak{a}_1, \ldots, \mathfrak{a}_k, \ldots, \mathfrak{a}_i, \ldots, \mathfrak{a}_n)$$

DENN: man überführe nacheinander

$$\mathfrak{a}_i \longrightarrow \mathfrak{a}_i + \mathfrak{a}_k \;\; ; \;\; \mathfrak{a}_k \longrightarrow \mathfrak{a}_k - \mathfrak{a}_i - \mathfrak{a}_k \;\; ; \;\; \mathfrak{a}_i + \mathfrak{a}_k \longrightarrow \mathfrak{a}_k$$

und wende (D2) an. □

Schließlich folgt:

3. 1. 4 Das Determinantenkriterium. *Ist A eine Matrix mit den Zeilenvektoren $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$, so gilt:*

$$(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \;\; \ell a \Longleftrightarrow D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) = 0 \Longleftrightarrow rg\, A \leq n-1.$$

BEWEIS. (a) Ist $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ ℓa, so gilt – wie wir schon oben gesehen haben – $D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) = 0$. Denn, es lässt sich ja in diesem Falle o.B.d.A. etwa der Vektor $\mathfrak{a}_1$ als $\sum_{i \neq 1} s_i\, \mathfrak{a}_i$ kombinieren.

(b) Sei $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ hiernach ℓu. Da $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ eine Basis bildet, lassen sich die Vektoren $\mathfrak{e}_1, \ldots, \mathfrak{e}_n$ linear über $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ kombinieren, und es muss darüber hinaus zumindest ein $(\mathfrak{e}_k, \mathfrak{a}_2, \ldots, \mathfrak{a}_n)$ ℓu sein, da sonst schon $(\mathfrak{a}_2, \ldots, \mathfrak{a}_n)$ eine Basis wäre. Das liefert aber:

$$\mathfrak{e}_k = s_1\, \mathfrak{a}_1 + \sum_2^n s_i\, \mathfrak{a}_i \text{ mit } s_1 \neq 0\,,$$

woraus dann

$$D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) = \frac{1}{s_1} \cdot D\Big(\underset{\pi(1)}{\mathfrak{e}_k}, \; \mathfrak{a}_2, \ldots, \mathfrak{a}_n\Big)$$

resultiert.

Nun ist aber $(\mathfrak{e}_{\pi(1)}, \mathfrak{a}_2, \ldots, \mathfrak{a}_n)$ ℓu. Deshalb können wir das Verfahren fortsetzen, bis wir nach n Schritten zu

$$D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) = \frac{1}{s_1 \cdot \ldots \cdot s_n} \cdot D(\mathfrak{e}_{\pi(1)}, \ldots, \mathfrak{e}_{\pi(n)}) \neq 0$$

gelangen. □

Wir wissen bislang noch nicht, ob es überhaupt eine Determinantenfunktion gibt. Wir können aber aufgrund der bisherigen Sätze zumindest herleiten, wie ein solches D *aussähe*.

Seien hierzu $\mathfrak{a}_i = a_{i,1}\,\mathfrak{e}_1 + \ldots + a_{i,n}\,\mathfrak{e}_n$ $(1 \leq i \leq n)$ die Darstellungen der Vektoren $\mathfrak{a}_i$ über $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$. Dann geht

$$D\begin{pmatrix} \mathfrak{a}_1 \\ \vdots \\ \mathfrak{a}_n \end{pmatrix} = D\begin{pmatrix} a_{11}\,\mathfrak{e}_1 + a_{12}\,\mathfrak{e}_2 + \ldots + a_{1,n}\,\mathfrak{e}_n \\ \vdots \\ a_{n,1}\,\mathfrak{e}_1 + a_{n,2}\,\mathfrak{e}_2 + \ldots + a_{n,n}\,\mathfrak{e}_n \end{pmatrix}$$

nach dem Additionstheorem und dem Determinantenkriterium auf dem Wege sukzessiver *Spaltung* von Zeile zu Zeile über in eine Summe von Determinanten des Typs

$$D\begin{pmatrix} a_{1,\pi(1)}\,\mathfrak{e}_{\pi(1)} \\ \vdots \\ a_{n,\pi(n)}\,\mathfrak{e}_{\pi(n)} \end{pmatrix} = D\left(a_{1,\pi(1)}\,\mathfrak{e}_{\pi(1)}, \ldots, a_{n,\pi(n)}\,\mathfrak{e}_{\pi(n)}\right),$$

wobei π alle **Permutationen** [1] von $\{1, \ldots, n\}$ durchläuft. Das bedeutet aber formal nichts anderes als

$$\begin{aligned} D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) &= \sum_{\pi\,\text{eine}}^{\text{Perm.}} D(a_{1,\pi(1)}\,\mathfrak{e}_{\pi(1)}, \ldots, a_{n,\pi(n)}\,\mathfrak{e}_{\pi(n)}) \\ &= \sum_{\pi\,\text{eine}}^{\text{Perm.}} a_{1,\pi(1)} \cdot \ldots \cdot a_{n,\pi(n)} \cdot D(\mathfrak{e}_{\pi(1)}, \ldots, \mathfrak{e}_{\pi(n)}). \end{aligned}$$

Nach dem Vertauschungslemma ist $D(\mathfrak{e}_{\pi(1)}, \ldots, \mathfrak{e}_{\pi(n)})$ aber gleich $+1$ oder gleich -1, da wir durch sukzessives Vertauschen schließlich zu $D(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ gelangen (bringe $\mathfrak{e}_1$ auf Platz 1, $\mathfrak{e}_2$ auf Platz 2 usf.). Demzufolge bleibt zu studieren, wie die Anordnung $\pi(i)$ $(1 \leq i \leq n)$ in das Ergebnis des entsprechenden Summanden eingeht. Hierzu bedarf es einer Zwischenbetrachtung:

Schreiben wir n natürliche Zahlen in irgendeiner Reihenfolge hin, so kann es sein, dass k vor i kommt, obwohl $i < k$ gilt. Wir sagen in diesem Falle

[1] bijektiven Abbildungen

(k, i) sei ein vertauschtes Paar und bezeichnen die eindeutig bestimmte Zahl der vertauschten Paare als die **Vertauschungszahl** der betrachteten Anordnung π, i. Z. (als) $VZ(\pi)$.

Für diese Vertauschungszahl gelten nun zwei Fakten, die uns weiterführen werden, nämlich:

1. Vertauscht man $\pi(i)$ und $\pi(i+1)$, also zwei benachbarte Elemente, so springt $(-1)^{VZ}$ um.
2. Auch wenn man zwei beliebige Elemente vertauscht, springt $(-1)^{VZ}$ um.

DENN: Vertauscht man zwei benachbarte Elemente miteinander, so nimmt VZ um *eins* zu oder um *eins* ab, und man kann zwei beliebige verschiedene Elemente a und b miteinander vertauschen, indem man zunächst das links liegende Element sukzessive mit allen x zwischen a und b vertauscht, hiernach a und b vertauscht und schließlich das ursprünglich rechts liegende Element sukzessive mit allen x vertauscht, die ursprünglich zwischen a und b lagen. Und das bedeutet, dass die Parität (gerade, ungerade) der Vertauschungszahl umspringt.

Ein Beispiel: In 8, 6, 7, 5, 2, 1, 4, 3 sollen 7 und 4 in einer Serie von Einzelschritten vertauscht werden.

LÖSUNG:

$$\begin{array}{cccccccc} 7\ 5 & 7\ 2 & 7\ 1 & 7\ 4 & 1\ 4 & 2\ 4 & 5\ 4 \\ \vee & \vee & \vee & \vee & \vee & \vee & \vee \end{array}$$

Es kann also nach dem bisherigen die Konstellation $\mathfrak{e}_{\pi(1)}, \ldots, \mathfrak{e}_{\pi(n)}$ im Falle $\langle VZ$ gerade$\rangle$ nur über eine gerade Anzahl von paarweisen Vertauschungen und im Falle $\langle VZ$ ungerade$\rangle$ nur über eine ungerade Anzahl von Vertauschungen $\mathfrak{e}_{\pi(i)}, \mathfrak{e}_{\pi(j)} \longrightarrow \mathfrak{e}_{\pi(j)}, \mathfrak{e}_{\pi(i)}$ erreicht werden. Dies bedeutet aber

$$D\left(\mathfrak{e}_{\pi(1)}, \ldots, \mathfrak{e}_{\pi(n)}\right) = (-1)^{VZ(\pi)} =: \operatorname{sg}(\pi).$$

Somit ergibt sich als ein erstes Zwischenresultat:

3. 1. 5 Der Eindeutigkeitssatz. *Sei* $\mathbf{V}$ *ein endlich dimensionaler Vektorraum mit vorgegebener geordneter Basis* $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$. *Dann gibt es in bezug auf diese Basis höchstens eine Determinantenfunktion, nämlich*

$$D\left(\mathfrak{a}_1, \ldots, \mathfrak{a}_n\right) = \sum_{\pi \in \text{Perm.}} \operatorname{sg}(\pi) \cdot a_{1,\pi(1)} \cdot \ldots \cdot a_{n,\pi(n)}.$$

Andererseits stellt sich leicht ein:

3. 1. 6 Der Existenzsatz. *Sei* $\mathbf{V}$ *ein endlich-dimensionaler Vektorraum und* $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ *eine geordnete Basis zu* $\mathbf{V}$*. Dann liefert die unter* 3.1.5 *erklärte Funktion* D *eine Determinantenfunktion.*

BEWEIS. Offenbar gilt das Additionstheorem, und man sieht leicht ein, dass $D(\mathfrak{a}_1, \ldots, \mathfrak{a}_i, \ldots, \mathfrak{a}_i, \ldots, \mathfrak{a}_n)$ verschwindet. Denn im letzten Fall tritt jedes Produkt $a_{1,\pi(1)} \cdot \ldots \cdot a_{n,\pi(n)}$ zweimal auf, jedoch aufgrund der Regeln für *sg* mit verschiedenen Vorzeichen, da eine der betreffenden Permutationen eine gerade, die andere eine ungerade Vertauschungszahl aufweist. Daraus ergibt sich aber

$$\begin{aligned} D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) &= D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) + 0 \\ &= D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) + D(\mathfrak{a}_1, \ldots, \mathfrak{a}_k, \ldots, \mathfrak{a}_k, \ldots, \mathfrak{a}_n) \\ &= D(\mathfrak{a}_1, \ldots, \mathfrak{a}_i + \mathfrak{a}_k, \ldots, \mathfrak{a}_n). \end{aligned}$$

Somit gilt Axiom (D1). Weiter sieht man unmittelbar, dass D auch die Axiome (D2) und (D3) erfüllt. □

Nachdem wir nun wissen, dass zu jedem endlich erzeugten Vektorraum **bei vorgegebener geordneter Basis genau eine Determinantenfunktion bezüglich dieser Basis** existiert und dass diese von den Komponenten der Vektoren $\mathfrak{a}_i$ im Blick auf die Einheitsvektoren bestimmt wird, bietet sich als natürliche Notation die Schreibweise

$$\begin{aligned} D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) &=: |\, \mathfrak{a}_1, \ldots\ldots, \mathfrak{a}_n \,| \\ &=: \begin{vmatrix} a_{11}, \ldots, a_{1,n} \\ \vdots \\ a_{n,1}, \ldots, a_{n,n} \end{vmatrix} =: |\, A \,| \end{aligned}$$

an, so wie sie häufig *per definitionem* mittels

$$\det(A) := \sum_{\pi \in \text{Perm.}} \operatorname{sg}(\pi) \cdot a_{1,\pi(1)} \cdot \ldots \cdot a_{n,\pi(n)}$$

eingeführt wird.

Auf diese Weise wird dann zusätzlich deutlich, dass zu jeder $n \times n$-Matrix A eines $\mathbf{K}$ eine eindeutig bestimmte Determinante aus $\mathbf{K}^n$ gehört, nämlich $|\, A \,|$.

Hiernach setzen wir unsere Bemühungen um Determinantengesetze fort. Als ein wesentlicher Hilfssatz wird sich dabei erweisen:

3. 1. 7 Das Eindeutigkeitslemma. *Sei* $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ *eine geordnete Basis zu* $\mathbf{V}$ *und* $F : \mathfrak{V}^n \longmapsto K$ *eine* **schwache Determinantenfunktion**, *d. h. eine Funktion, die – lediglich – den Axiomen* (D1) *und* (D2) *genügt. Dann ermittelt sich* F *vermöge der zu* $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ *gehörenden Determinantenfunktion* D via:

$$F\,(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) = F\,(\mathfrak{e}_1, \ldots, \mathfrak{e}_n) \cdot D\,(\mathfrak{a}_1, \ldots, \mathfrak{a}_n).$$

DENN: Ist $F\,(\mathfrak{e}_1, \ldots, \mathfrak{e}_n) = 1$, so sind wir nach 3.1.5 am Ziel. Sonst aber haben wir $F\,(\mathfrak{e}_1, \ldots, \mathfrak{e}_n) - 1 \neq 0$, und es folgt

$$\frac{F(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) - D\,(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)}{F(\mathfrak{e}_1, \ldots, \mathfrak{e}_n) - 1} = D\,(\mathfrak{a}_1, \ldots, \mathfrak{a}_n),$$

da die linke Seite die Axiome (D1),. . . ,(D3) erfüllt, und damit die Behauptung:

$$F(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) = F(\mathfrak{e}_1, \ldots, \mathfrak{e}_n) \cdot D\,(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \qquad \square$$

Mit Hilfe des letzten Lemmas lässt sich nun zeigen, dass es im $\mathbf{R}^n$ im wesentlichen keine anderen **Inhaltsfunktionen** gibt als die Determinantenfunktion. Genauer gilt:

3. 1. 8 Der Volumensatz. *Ist* $V : (\mathbf{R}^n)^n \longmapsto \mathbf{R}$ *eine Volumenfunktion im Sinne von* $(0), \ldots, (4)$, *so gilt:*

$$V(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \;=\; |\, D\,(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \,|.$$

BEWEIS. Zu zeigen ist: $D = \operatorname{sg}(D) \cdot V =: I$. Nun erfüllt aber I die Axiome (D1) und (D3) evidenterweise, und es gilt wegen $\operatorname{sg}(ab) = \operatorname{sg}(a) \cdot \operatorname{sg}(b)$:

$$\begin{aligned}
& I\,(\mathfrak{a}_1, \ldots, s\,\mathfrak{a}_i, \ldots, \mathfrak{a}_n) \\
= \;& V\,(\mathfrak{a}_1, \ldots, s\,\mathfrak{a}_i, \ldots, \mathfrak{a}_n) \cdot \operatorname{sg}\,(D\,(\mathfrak{a}_1, \ldots, s\,\mathfrak{a}_i, \ldots, \mathfrak{a}_n)) \\
= \;& |s| \cdot V\,(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \cdot \operatorname{sg}(s) \cdot \operatorname{sg}\,(D\,(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)) \\
= \;& s \cdot V\,(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \cdot \operatorname{sg}\,(D\,(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)) \\
= \;& s \cdot (V \cdot \operatorname{sg}(D))(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \\
= \;& s \cdot I(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)\,,
\end{aligned}$$

weshalb die Funktion I auch (D2) erfüllt, woraus die Gleichheit $D = I$ resultiert. □

Als ein weiteres wichtiges Resultat liefert 3.1.7:

3. 1. 9 Das Multiplikationstheorem. *Definiert man $A \cdot B$ als $(\mathfrak{a}_i \cdot \downarrow b_k)$, also als diejenige Matrix, in der am Platz i, k das Skalarprodukt des i-ten Zeilenvektors von A mit dem k-ten Spaltenvektor $\downarrow b_k$ von B steht, so gilt:*

$$|A \cdot B| \;=\; |A| \cdot |B|.$$

BEWEIS. Wir bezeichnen die Matrix $A \cdot B$ mit $(c_{i,k})$. Dann ist $|A \cdot B|$ einerseits gleich $D(\mathfrak{c}_1, \ldots, \mathfrak{c}_n)$, andererseits aber bei festgehaltenem B (und variablem A) ein $F(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$, und es gelten fast unmittelbar:

$$\begin{aligned} F(\mathfrak{a}_1, \ldots, \mathfrak{a}_i + \mathfrak{a}_k, \ldots, \mathfrak{a}_n) &= D(\mathfrak{c}_1, \ldots, \mathfrak{c}_i + \mathfrak{c}_k, \ldots, \mathfrak{c}_n) \\ \text{und} \qquad F(\mathfrak{a}_1, \ldots, s \cdot \mathfrak{a}_i, \ldots, \mathfrak{a}_n) &= D(\mathfrak{c}_1, \ldots, s \cdot \mathfrak{c}_i, \ldots, \mathfrak{c}_n). \end{aligned}$$

Somit erfüllt F die Axiome (D1) und (D2), woraus die Behauptung

$$\begin{aligned} |A| \cdot |B| &= D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \cdot D(\mathfrak{b}_1, \ldots, \mathfrak{b}_n) \\ &= D(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \cdot F(\mathfrak{e}_1, \ldots, \mathfrak{e}_n) \\ &= F(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \\ &= D(\mathfrak{c}_1, \ldots, \mathfrak{c}_n) = |A \cdot B| \end{aligned}$$

resultiert. □

Schließlich gilt noch

3. 1. 10 Der Spiegelungssatz. $\quad |A^\top| = |A|.$

DENN: transformiert man die Matrix A zu $A^\top$, so gehen die einzelnen Produkte $a_{1,\pi(1)} \cdot \ldots \cdot a_{n,\pi(n)}$ über in sich selbst, und es geht π über in π^{-1}, also $\operatorname{sg}(\pi)$ über in $\operatorname{sg}(\pi^{-1}) = \operatorname{sg}(\pi)$. □

3.2 Zum linearen Gleichungsaspekt

In diesem Abschnitt wenden wir uns Determinantentheoremen im Blick auf lineare Gleichungssysteme zu.

3. 2. 1 Der Laplace'sche Entwicklungssatz. *Bezeichnet man die aus A durch Streichung der i-ten Zeile und k-ten Spalte hervorgehende Matrix mit $A_{i,k}$, so gilt bei festem i*

$$|\,A\,| \;=\; \sum_{k=1}^{n}\;(-1)^{i+k}\cdot a_{i,k}\cdot|\,A_{i,k}\,|\,.$$

BEWEIS. Wir entwickeln zunächst nach der 1. Zeile, d. h., wir klammern a_{11} bis $a_{1,n}$ vor. Dies liefert:

$$|\,A\,| \;=\; \sum_{k=1}^{n}\;a_{1,k}\,P_{1,k}\,.$$

Hiernach betrachten wir ein $a_{1,k}\cdot a_{2,\pi(2)}\cdot\ldots\cdot a_{n,\pi(n)}$. Offenbar hat das n-tupel $k,\pi(2),\ldots,\pi(n)$ $k-1$ vertauschte Paare mehr als $\pi(2),\ldots,\pi(n)$. Somit gelten die Gleichungen

$$\begin{aligned}
\operatorname{sg}(\pi) &= (-1)^{k-1}\cdot\operatorname{sg}(\pi(2),\ldots,\pi(n))\\
\text{bzw.}\qquad P_{1,k} &= (-1)^{k-1}\cdot|\,A_{1,k}\,|\\
\text{also:}\qquad A &= \sum_{k=1}^{n}\;(-1)^{k-1}\cdot a_{1,k}\cdot|\,A_{1,k}\,|\,.
\end{aligned}$$

Damit ist, wegen $(-1)^{k-1}=(-1)^{k+1}$, unsere Behauptung für $i=1$ bewiesen. Wir führen nun den allgemeinen Fall auf diesen Sonderfall zurück vermöge:

$$\begin{aligned}
|\,A\,| &= |\,\mathfrak{a}_1,\ldots,\mathfrak{a}_n\,|\\
&= (-1)^{i-1}\cdot|\,\mathfrak{a}_i,\mathfrak{a}_1,\ldots,\mathfrak{a}_{i-1},\mathfrak{a}_{i+1},\ldots,\mathfrak{a}_n\,|\\
&= (-1)^{i-1}\sum_{k=1}^{n}\;(-1)^{k-1}\cdot a_{i,k}\cdot|\,A_{i,k}\,|\\
&= \textstyle\sum_{k=1}^{n}(-1)^{i+k}\cdot a_{i,k}\cdot|\,A_{i,k}\,|,
\end{aligned}$$

da die $A_{i,k}$ von dem Vertauschungsprozess nicht betroffen sind. □

Der Entwicklung von A nach der i-ten Zeile entspricht natürlich eine Entwicklung nach der k-ten Spalte (beachte den Spiegelungssatz!). Somit gilt auch:

$$|\,A\,|=\sum_{i=1}^{n}\;(-1)^{i+k}a_{i,k}\cdot|\,A_{i,k}\,|\,.$$

Weiter erhalten wir als eine für die Gleichungslehre fundamentale Formel

3. 2. 2 Das Anullierungslemma. *Ist $i \neq j$, so gilt:*

$$\sum_{k=1}^{n} (-1)^{i+k} \cdot a_{i,k} \cdot |\, A_{j,k} \,| = 0.$$

DENN: die notierte Summe zur Linken ist nichts anderes als die Entwicklung derjenigen Determinante, die man erhält, wenn man in A den Zeilenvektor $\mathfrak{a}_j$ durch den Zeilenvektor $\mathfrak{a}_i$ ersetzt. □

Ganz entsprechend können wir auch hier wieder – wie oben – die angeführte Gleichung unter 3.2.2 auf die Spalten von A beziehen.

Damit sind wir in der Lage, 3.2.1 und 3.2.2 zusammenzufassen zu dem

3. 2. 3 Korollar. *Für Matrizen $(a_{i,k})$ gilt allgemein:*

$$\begin{aligned} & (a_{i,k}) \cdot ((-1)^{i+k} |\, A_{i,k} \,|)^{\top} &&= |\, A \,| \cdot E \\ \text{und} \qquad & ((-1)^{i+k} |\, A_{i,k} \,|)^{\top} \cdot (a_{i,k}) &&= E \cdot |\, A \,|\,. \end{aligned}$$

Wie man leicht sieht, beinhaltet 3.2.3 als Sonderfall:

3. 2. 4 Das Invertierbarkeitskriterium. *Genau dann ist die $n \times n$-Matrix A invertierbar, wenn ihre Determinante nicht verschwindet bzw. äquivalent hierzu, wenn sie den Rang n hat.*

DENN: man beachte 3.2.3 und $A \cdot X = E \Longrightarrow |\, A \,| \cdot |\, X \,| = 1$. □

Abschließend kommen wir zum Zusammenhang zwischen Determinanten und linearen Gleichungssystemen. Hauptergebnis wird dabei ein Sachverhalt sein, über den sich die Lösung eines LGS rein determinantentheoretisch formulieren lässt .

Hierzu bezeichne $A_{k,\mathfrak{b}}$ diejenige Matrix, in die A übergeht, wenn die k-te Spalte ersetzt wird durch den Vektor $\mathfrak{b}$. Dann folgt:

3. 2. 5 Die Cramer'sche Regel.

$$A \cdot (|\, A_{1,\mathfrak{b}} \,|, \ldots, |\, A_{n,\mathfrak{b}} \,|)^{\top} = \mathfrak{b}\, |\, A \,|$$

BEWEIS. Wir können uns auf den Beweis für die erste Zeile beschränken, da Vertauschung der ersten mit der i-ten Zeile sowohl in $|\,A\,|$ als auch in jedem $|\,A_{k,\mathfrak{b}}\,|\,(1 \leq k \leq n)$ das Vorzeichen umpolt. Und dies liefert:

$$\begin{array}{lll}
a_{11} \cdot |\,A_{1,\mathfrak{b}}\,| & + a_{11} \cdot b_1 \cdot |\,A_{11}\,| \; - \; a_{11} \cdot b_2 \cdot |\,A_{21}\,| \ldots \\
\quad + & \\
a_{12} \cdot |\,A_{2,\mathfrak{b}}\,| & - a_{12} \cdot b_1 \cdot |\,A_{12}\,| \; + \; a_{12} \cdot b_2 \cdot |\,A_{22}\,| \ldots \\
\quad + \qquad = & \\
a_{13} \cdot |\,A_{3,\mathfrak{b}}\,| & + a_{13} \cdot b_1 \cdot |\,A_{13}\,| \; - \; a_{13} \cdot b_2 \cdot |\,A_{23}\,| \ldots \\
\quad + & \\
a_{14} \cdot |\,A_{4,\mathfrak{b}}\,| & - a_{14} \cdot b_1 \cdot |\,A_{14}\,| \; + \; a_{14} \cdot b_2 \cdot |\,A_{24}\,| \ldots \\
\quad + & \vdots \qquad\qquad\qquad \vdots
\end{array}$$

$$\begin{aligned}
&= \quad b_1 \sum_{k=1}^{n} (-1)^{1+k} \cdot a_{1,k} \cdot |\,A_{1,k}\,| \; + \; 0 \; + \; 0 \ldots \\
&= \quad b_1 \cdot |\,A\,| \;,
\end{aligned}$$

was zu beweisen war. □

3. 2. 6 Korollar. *Sei* $|\,A\,| \neq 0$. *Dann wird* $A\mathfrak{x} \doteq \mathfrak{b}$ *eindeutig gelöst durch den Vektor* $\left(\frac{|\,A_{1,\mathfrak{b}}\,|}{|\,A\,|} \;,\; \frac{|\,A_{2,\mathfrak{b}}\,|}{|\,A\,|} \;,\; \ldots\ldots\ldots \;,\; \frac{|\,A_{n,\mathfrak{b}}\,|}{|\,A\,|} \right)$.

Kapitel 4

Lineare Abbildungen

4.1 Lineare Abbildungen

Seien im folgenden $\mathbf{V}$ und $\mathbf{W}$ Vektorräume über demselben Körper $\mathcal{K}$, also $\mathcal{K}$-Vektorräume.

4. 1. 1 Definition. $\alpha : \mathbf{V} \longmapsto \mathbf{W}$ heißt eine **lineare Abbildung** auch **linearer Operator** von $\mathbf{V}$ nach $\mathbf{W}$, wenn gilt

$$\text{(L)} \qquad \alpha\,(s\mathfrak{x} + t\mathfrak{y}) \;=\; s(\alpha\,(\mathfrak{x})) + t(\alpha\,(\mathfrak{y})).$$

Offenbar ist α genau dann linear, wenn gilt:

$$(i) \quad \alpha\,(\mathfrak{x} + \mathfrak{y}) = \alpha\,(\mathfrak{x}) + \alpha\,(\mathfrak{y})$$
$$(ii) \quad \alpha\,(s\mathfrak{x}) = s(\alpha\,(\mathfrak{x}))\,,$$

bzw. wenn gilt:

$$\text{(L}^*\text{)} \qquad \alpha\,(\,\textstyle\sum s_i\,\mathfrak{x}_i\,) \;=\; \sum s_i\,(\alpha\,(\mathfrak{x}_i))\,.$$

Statt $\alpha\,(\mathfrak{x})$ schreiben wir auch $\alpha\,\mathfrak{x}$. Spezialisierung liefert u.a.

$$\alpha\,\mathfrak{o} = \alpha\,(0\mathfrak{o}) \;=\; 0\cdot(\alpha\,\mathfrak{o}) = \mathfrak{o}$$
$$\text{und} \quad \alpha\,(-\mathfrak{x}) = \alpha\,((-1)\mathfrak{x}) \;=\; (-1)(\alpha\,\mathfrak{x}) = -(\alpha\,\mathfrak{x}).$$

Weitere unmittelbare Konsequenzen sind

4. 1. 2 Proposition. *Ist $\alpha : \mathbf{V} \longmapsto \mathbf{W}$ linear und $\mathfrak{U}$ abgeschlossen in $\mathbf{V}$, so ist $\alpha\,\mathfrak{U}$ abgeschlossen in $\mathbf{W}$, und es gilt*

$$\dim\,(\alpha\,\mathbf{U}) \le \dim\,(\mathbf{U})\,.$$

BEWEIS. Sind $\mathfrak{y}_1$ und $\mathfrak{y}_2$ aus $\alpha\,\mathfrak{U}$, so gilt für geeignete $\mathfrak{x}_1, \mathfrak{x}_2 \in \mathfrak{U}$

$$\begin{aligned} \mathfrak{y}_1 &= \alpha\,\mathfrak{x}_1 \\ &\qquad \rightsquigarrow \mathfrak{y}_1 + \mathfrak{y}_2 = \alpha\,(\,\mathfrak{x}_1 + \mathfrak{x}_2) \in \alpha\,\mathfrak{U}\,, \\ \mathfrak{y}_2 &= \alpha\,\mathfrak{x}_2 \end{aligned}$$

und es folgt analog $\mathfrak{y} \in \alpha\,\mathfrak{U} \Longrightarrow s\,\mathfrak{y} \in \alpha\,\mathfrak{U}$.

Und ist weiter $\sum_1^n s_i\,\mathfrak{x}_i = \mathfrak{o}$, so folgt $\sum s_i\,(\alpha\,\mathfrak{x}_i) = \mathfrak{o}$, weshalb $(\,\mathfrak{y}_1, \ldots, \mathfrak{y}_m\,) \subseteq \alpha\,\mathfrak{U}$ höchstens dann ℓu ist, wenn jedes Urbild-m-tupel zu $(\,\mathfrak{y}_1, \ldots, \mathfrak{y}_m\,)$ ℓu ist. □

4. 1. 3 Proposition. *Sei* $(\,\mathfrak{x}_1, \ldots, \mathfrak{x}_n\,)$ *eine Basis aus* $\mathbf{V}$ *und* $(\,\mathfrak{y}_1, \ldots, \mathfrak{y}_n\,)$ *beliebig aus* $\mathbf{W}$ *. Dann gibt es eine und nur eine lineare Abbildung* α *mit* $\alpha\,(\mathfrak{x}_i) = \mathfrak{y}_i$ *.*

BEWEIS. Setze $\alpha\,(\sum s_i\,\mathfrak{x}_i\,) := \sum s_i\,\mathfrak{y}_i$. Dies ist eine lineare Abbildung $\mathbf{V} \longmapsto \mathbf{W}$, da jedes $\mathfrak{x}$ aus $\mathbf{V}$ genau eine Darstellung über $(\,\mathfrak{x}_1, \ldots, \mathfrak{x}_n\,)$ besitzt, so dass jedem $\mathfrak{x} \in \mathfrak{V}$ exakt ein Bild zugeordnet wird, und es ist α *per definitionem* linear. □

Insbesondere hat sich damit ergeben:

4. 1. 4 Korollar. *Eine lineare Abbildung* $\alpha : \mathbf{V} \longmapsto \mathbf{W}$ *ist schon durch das Bild einer jeden beliebigen Basis, kurz durch ihre Basiswerte festgelegt.*

4. 1. 5 Definition. Sei $\alpha : \mathbf{V} \longmapsto \mathbf{W}$ linear. Wir erklären:

Der **Kern** von α soll sein: $\ker(\alpha) := \{\mathfrak{x} \in \mathfrak{V} \mid \alpha\,\mathfrak{x} = \mathfrak{o}\}$

Das **Bild** von α soll sein: $\mathrm{im}\,(\alpha) := \{\mathfrak{y} \in \mathfrak{W} \mid \exists \mathfrak{x} : \alpha\,\mathfrak{x} = \mathfrak{y}\}$

Der **Rang** von α soll sein: $\mathrm{rg}\,(\alpha) := \dim(\alpha\,\mathbf{V})$.

Als eine erste unmittelbare Folgerung stellt sich ein:

4. 1. 6 Proposition. *Sei* $\alpha : \mathbf{V} \longmapsto \mathbf{W}$ *linear. Dann gelten die Gleichungen* $\ker(\alpha) = [\,\ker(\alpha)\,]$ *und* $\mathrm{im}\,(\alpha) = [\,\mathrm{im}\,(\alpha)\,]$.

DENN: die Abgeschlossenheit von $\mathrm{im}\,(\alpha)$ wurde schon gezeigt und die Abgeschlossenheit von $\ker(\alpha)$ folgt aus den Implikationen

$$\alpha\,\mathfrak{x}_1 = \mathfrak{o} = \alpha\,\mathfrak{x}_2 \Longrightarrow \alpha\,(\,\mathfrak{x}_1 + \mathfrak{x}_2\,) = \mathfrak{o} \text{ und } \alpha\,\mathfrak{x} = \mathfrak{o} \Longrightarrow \alpha\,(s\mathfrak{x}) = s(\alpha\,\mathfrak{x}) = \mathfrak{o}\,,$$

fertig. □

Hiernach lässt sich beweisen:

4. 1. 7 Die 2. Dimensionsformel. *Sei* $\alpha : \mathbf{V} \longmapsto \mathbf{W}$ *linear. Dann gilt*

$$\dim\,(\mathbf{Ker}\,(\alpha)) + \dim\,(\mathbf{Im}\,(\alpha)) = \dim\,(\mathbf{V}).$$

BEWEIS. Ist die Dimension von $\mathbf{V}$ unendlich, so ist nichts zu zeigen, und dies gilt auch im Falle $\mathbf{V} = \mathbf{O}$. Sei deshalb $\dim\,(\mathbf{V})$ endlich, aber verschieden von 0. Dann existiert eine nicht leere Basis

$$\begin{aligned} &(\,\mathfrak{x}_1, \mathfrak{x}_2, \ldots, \mathfrak{x}_m\,,\, \mathfrak{x}_{m+1}, \ldots, \mathfrak{x}_n\,) \\ &\text{mit} \qquad [\,\mathfrak{x}_1, \ldots, \mathfrak{x}_m\,] = \ker\,(\alpha), \end{aligned}$$

und es folgt:

(i) Jedes Element aus $\mathrm{im}\,(\alpha)$ lässt sich darstellen als

$$\textstyle\sum s_i\,(\alpha\,\mathfrak{x}_i\,) + \sum t_j(\alpha\,\mathfrak{x}_j) \;\; (1 \leq i \leq m\,,\; m+1 \leq j \leq n),$$

also, wegen Wegfalls des ersten Summanden als Linearkombination der $n-m$ Vektoren $\alpha\,(\mathfrak{x}_{m+1}), \ldots, \alpha\,(\mathfrak{x}_n)$. Somit gilt $\mathrm{im}\,(\alpha) = [\,\alpha\,\mathfrak{x}_{m+1}, \ldots, \alpha\,\mathfrak{x}_n\,]$.

(ii) Die Darstellung aus (i) ist eindeutig, denn

$$\begin{aligned} \textstyle\sum t_j(\alpha\,\mathfrak{x}_j) = \mathfrak{o} \;&\Longrightarrow\; \alpha\,\textstyle\sum t_j\mathfrak{x}_j = \mathfrak{o} \\ &\Longrightarrow\quad \textstyle\sum t_j\mathfrak{x}_j \in \ker\,(\alpha) \\ &\Longrightarrow\quad t_j = 0 \;\; (m+1 \leq j \leq n). \end{aligned}$$

Daher ist $(\alpha\,\mathfrak{x}_{m+1}, \ldots, \alpha\,\mathfrak{x}_n)$ sogar Basis zu $\mathbf{Im}\,(\alpha)$, und es gilt

$$\begin{array}{ccccc} \dim\,(\mathbf{Ker}\,(\alpha)) & + & \dim\,(\mathbf{Im}\,(\alpha)) & & \\ = \qquad m & + & (n-m) & = & n = \dim\,(\mathbf{V}). \end{array}$$ □

Schließlich halten wir fest:

4. 1. 8 Proposition. *Sei* $\mathbf{V}$ *endlich-dimensional und die Abbildung* $\alpha : \mathbf{V} \longmapsto \mathbf{W}$ *linear. Dann folgt:*

$$\alpha \;\textit{injektiv} \Longleftrightarrow \mathbf{Ker}\,(\alpha) = \mathbf{O} \Longleftrightarrow \textit{alle Basisbilder sind } \ell u.$$

BEWEIS.
$$\begin{aligned}
\alpha \text{ injektiv} &\rightsquigarrow \mathbf{Ker}\,(\alpha) = \mathbf{O} \\
&\rightsquigarrow \textstyle\sum s_i\,(\alpha\,\mathfrak{x}_i\,) = \mathfrak{o} \Longleftrightarrow \sum s_i\,\mathfrak{x}_i\; = \mathfrak{o} \\
&\qquad\qquad\qquad\qquad \Longleftrightarrow s_i\; = 0\;\; (1 \leq i \leq n) \\
&\rightsquigarrow (\alpha\,\mathfrak{x}_1, \ldots, \alpha\,\mathfrak{x}_n)\;\; \ell u
\end{aligned}$$

$$\begin{array}{rcl}
\text{und} \quad \mathfrak{B} \text{ Basis} & \Longrightarrow & \alpha\,\mathfrak{B}\;\; \ell u \\
& \Downarrow & \\
\mathfrak{x}' \neq \mathfrak{x}'' \;\;\&\;\; \mathfrak{x}'' = s\mathfrak{x}_1 & \rightsquigarrow & \alpha\,\mathfrak{x}' \neq s\alpha\,\mathfrak{x}' = \alpha\,\mathfrak{x}'' \\
& \mathrm{V} & \mathfrak{x}' \neq \mathfrak{x}'' \;\;\&\;\; (\mathfrak{x}_1, \mathfrak{x}'')\;\; \ell u \\
& \rightsquigarrow & (\alpha\,\mathfrak{x}', \alpha\,\mathfrak{x}'')\;\; \ell u \\
& \rightsquigarrow & \alpha\,\mathfrak{x}' \neq \alpha\,\mathfrak{x}''. \qquad \square
\end{array}$$

Als eine unmittelbare Anwendung des Dimensionssatzes folgt:

4. 1. 9 Proposition. *Sei* $\alpha : \mathbf{V} \longmapsto \mathbf{W}$ *linear, und sei weiter* $\dim \mathbf{V} = \dim \mathbf{W}$. *Dann ist* α *schon dann* **bijektiv**, *wenn* α **surjektiv** *oder* **injektiv** *ist.*

BEWEIS. Ist α surjektiv, so resultiert $\dim\,(\mathbf{Im}\,(\alpha)) = \dim\,(\mathbf{V})$, also $\dim\,(\mathbf{Ker}\,(\alpha)) = 0$ und damit α injektiv.

Ist α aber injektiv, so ist $\mathbf{Ker}\,(\alpha) = \mathbf{O}$, also $\dim\,(\mathbf{Im}\,(\alpha)) = \dim\,(\mathbf{V})$ und daher dann $\mathbf{Im}(\alpha) = \mathbf{W}$, d.h. α surjektiv. $\square$

4.2 Der lineare Abbildungsraum $\mathbf{L}\,(\mathbf{V} \longmapsto \mathbf{W})$

Seien im folgenden $\mathbf{V}$ und $\mathbf{W}$ festgewählte Vektorräume über $\mathcal{K}$. Dann können wir zu jedem $\alpha : \mathbf{V} \longmapsto \mathbf{W}$ das s-fache bilden vermöge

$$(s\alpha)\,(\mathfrak{x}) \;:=\; s(\alpha\,\mathfrak{x})$$

und zu je zwei linearen Operatoren α, β die Summe [1)]

$$(\alpha + \beta)\,(\mathfrak{x}) \;:=\; \alpha\,(\mathfrak{x}) + \beta\,(\mathfrak{x})\,.$$

Darüber hinaus gilt:

[1)] Offenbar lässt sich nach dieser Methode jede Gesamtheit von Abbildungen aus einer Menge in eine algebraische Struktur mit **abgeleiteten algebraischen Operationen** versorgen.

4. 2. 1 Proposition. *Sei* $L(\mathbf{V} \longmapsto \mathbf{W}) =: \mathfrak{L}$ *die Menge aller linearen Abbildungen von* $\mathbf{V}$ *nach* $\mathbf{W}$ *. Dann bildet* $\mathfrak{L}$ *bezüglich der soeben definierten Operationen* s *und* $+$ *einen Vektorraum.*

BEWEIS. Die einzelnen Verifikationen dürfen weitgehend dem Leser überlassen bleiben, weshalb wir uns exemplarisch beschränken auf

$$\begin{aligned} (s\alpha)(\mathfrak{x}_1 + \mathfrak{x}_2) &= s(\alpha(\mathfrak{x}_1 + \mathfrak{x}_2)) \\ &= s(\alpha\,\mathfrak{x}_1 + \alpha\,x_2) \\ &= s(\alpha\,\mathfrak{x}_1) + s(\alpha\,\mathfrak{x}_2) \\ &= (s\alpha)(\mathfrak{x}_1) + (s\alpha)(\mathfrak{x}_2) \\ \text{und} \qquad (s\alpha)(t\mathfrak{x}) &= s(\alpha(t\mathfrak{x})) \\ &= s(t(\alpha\,\mathfrak{x})) \\ &= t(s(\alpha\,\mathfrak{x})) \\ &= t\cdot((s\alpha)\,\mathfrak{x})\,. \end{aligned}$$

□

Wir zeigen nun

4. 2. 2 Proposition. *Ist* $(\mathfrak{x}_1, \ldots, \mathfrak{x}_n)$ *eine Basis zu* $\mathbf{V}$ *und ist* $(\mathfrak{y}_1, \ldots, \mathfrak{y}_m)$ *eine Basis zu* $\mathbf{W}$ *, so bilden die linearen Abbildungen* $\alpha_{i,k}$ *mit*

$$\begin{aligned} \alpha_{i,k}(\mathfrak{x}_k) &:= \mathfrak{y}_i \\ \textit{und} \quad \alpha_{i,k}(\mathfrak{x}_\ell) &:= \mathfrak{o} \quad \textit{(falls } k \neq \ell\textit{)} \end{aligned}$$

eine Basis des Vektorraums $\mathbf{L} := (L(\mathbf{V} \longmapsto \mathbf{W}), +, s\cdot)$.

BEWEIS. Die Abbildungen $\alpha_{i,k}$ sind ℓu. Ist nämlich

$$\begin{aligned} \alpha \;=\;& s_{11}\,\alpha_{11} + s_{12}\,\alpha_{12} + \cdots\cdots + s_{1,n}\,\alpha_{1,n} \\ +\;& s_{21}\,\alpha_{21} + s_{22}\,\alpha_{22} + \cdots\cdots + s_{2,n}\,\alpha_{2,n} \\ +\;& \cdots\cdot \\ & \vdots \\ +\;& s_{m,1}\,\alpha_{m,1} + s_{m,2}\,\alpha_{m,2} + \cdots\cdots + s_{m,n}\,\alpha_{m,n} \\ =\;& \mathfrak{o}, \end{aligned}$$

also α die **Nullabbildung** $\mathfrak{o} : \mathfrak{x} \longmapsto \mathfrak{o}$ $(\forall \mathfrak{x})$, so folgt $\alpha(\mathfrak{x}_k) = \sum_1^m s_{i,k}\,\mathfrak{y}_i = \mathfrak{o}$ und damit $s_{i,k} = 0$ für festes k, weshalb insgesamt alle $s_{i,k}$ verschwinden müssen.

Es gilt aber auch $[\alpha_{i,k}] = Ł$. Ist nämlich α irgendeine lineare Abbildung mit

$$\begin{array}{ccccc} \alpha(\mathfrak{x}_1) & , & \alpha(\mathfrak{x}_2) & , \ \dots \ , & \alpha(\mathfrak{x}_n) \\ \| & & \| & & \| \\ a_{11}\,\mathfrak{y}_1 & & a_{12}\,\mathfrak{y}_1 & & a_{1,n}\,\mathfrak{y}_1 \\ + & & + & & + \\ a_{21}\,\mathfrak{y}_2 & & a_{22}\,\mathfrak{y}_2 & & a_{2,n}\,\mathfrak{y}_2 \\ + & & + & & + \\ \vdots & & \vdots & & \vdots \\ + & & + & & + \\ a_{m,1}\,\mathfrak{y}_m & & a_{m,2}\,\mathfrak{y}_m & & a_{m,n}\,\mathfrak{y}_m\,, \end{array}$$

so folgt

$$\begin{aligned} \alpha(\mathfrak{x}_k) &= \sum_1^m a_{i,k}\,\mathfrak{y}_i \\ &= \Big(\sum_{i,k=1}^{m,n} a_{i,k}\,\alpha_{i,k}\Big)(\mathfrak{x}_k)\,, \end{aligned}$$

also

$$\alpha = \sum_{i,k=1}^{m,n} a_{i,k}\,\alpha_{i,k}\,. \qquad \square$$

Beachten wir nun, dass die Menge der Bildvektoren $\alpha(\mathfrak{x}_k)$ genau dann ℓa ist, wenn dies für die entsprechende Menge der Spaltenvektoren aus $(a_{i,k})$ gilt, so können wir zusammenfassend feststellen:

4. 2. 3 Proposition. *Ist α eine lineare Abbildung von $\mathbf{V}$ nach $\mathbf{W}$, und sind*

$$\begin{aligned} \mathfrak{B}_{\mathbf{V}} &= (\,\mathfrak{x}_1,\,\dots\,,\,\mathfrak{x}_n\,) \subseteq \mathfrak{V} \\ \text{und} \qquad \mathfrak{B}_{\mathbf{W}} &= (\,\mathfrak{y}_1,\,\dots\,,\,\mathfrak{y}_m\,) \subseteq \mathfrak{W} \end{aligned}$$

Basen zu $\mathbf{V}$ und $\mathbf{W}$, so entspricht α in bezug auf $\mathfrak{B}_{\mathbf{V}}, \mathfrak{B}_{\mathbf{W}}$ in umkehrbar eindeutiger Weise eine vermittelnde Matrix $A = (a_{i,k})$ vermöge der Zuordnung

$$A(\mathfrak{x}_k) = \sum_{i=1}^m a_{i,k}\,\mathfrak{y}_i\,,$$

und es gilt

$$\operatorname{rg}(A) = \operatorname{rg}(\alpha)\,.$$

Schließlich erwähnen wir den für die Praxis wichtigen Sachverhalt:

4. 2. 4 Proposition. *Wird der lineare Operator* $\alpha : \mathbf{V} \longmapsto \mathbf{W}$ *bezüglich der Basen*

$$\mathfrak{B}_{\mathbf{V}} = (\,\mathfrak{x}_1,\,\ldots\,,\,\mathfrak{x}_n\,) \qquad \mathfrak{B}_{\mathbf{W}} = (\,\mathfrak{y}_1,\,\ldots\,,\,\mathfrak{y}_m\,)$$

vermittelt durch die Matrix $A = (a_{i,k})$*, so gilt für jedes* $\mathfrak{c}$ *aus* $\mathfrak{V}$*, aufgefasst als n-tupel bezüglich* $\mathfrak{B}_{\mathbf{V}}$ *die Gleichung* $\alpha\,(\mathfrak{c}) = A\mathfrak{c}$*.*

DENN: setzt man $\mathfrak{c} = c_1\mathfrak{x}_1 + \ldots + c_n\mathfrak{x}_n$ in die lineare Abbildung

$$\alpha = \begin{array}{c} a_{11}\,\alpha_{11} \quad + \ldots + \quad a_{1,n}\,\alpha_{1n} \\ + \\ \vdots \\ + \\ a_{m,1}\,\alpha_{m,1} \quad + \ldots + \quad a_{m,n}\,\alpha_{m,n} \end{array}$$

ein, so wird von den einzelnen $\alpha_{i,k}$ wegen $\alpha_{i,k}\,\mathfrak{x}_j = \mathfrak{o}$ im Falle $i \neq j$ nur die k-te Komponente c_k berücksichtigt, was fast unmittelbar die Behauptung liefert. □

Die Abbildung α wird also nach dem oben angegebenen Verfahren durch die Matrix $(a_{i,k})$ genau dann vermittelt, wenn

$$\begin{array}{cccc} \alpha\,(\mathfrak{x}_1) & \alpha\,(\mathfrak{x}_2) & \cdots\cdots & \alpha\,(\mathfrak{x}_n) \\ \| & \| & & \| \\ a_{11}\,\mathfrak{y}_1 & a_{12}\,\mathfrak{y}_1 & \cdots\cdots & a_{1,n}\,\mathfrak{y}_1 \\ + & + & & + \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ + & + & & + \\ a_{m,1}\,\mathfrak{y}_m & a_{m,2}\,\mathfrak{y}_m & \cdots\cdots & a_{m,n}\,\mathfrak{y}_m \end{array}$$

erfüllt ist, was wir symbolisch auch in der Form

α	$\alpha(\mathfrak{x}_1)$	$\alpha(\mathfrak{x}_2)$	.....	$\alpha(\mathfrak{x}_n)$
$\mathfrak{y}_1$	a_{11}	a_{12}	.....	$a_{1,n}$
$\mathfrak{y}_2$	a_{21}	a_{22}	.....	$a_{2,n}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathfrak{y}_m$	$a_{m,1}$	$a_{m,2}$	.....	$a_{m,n}$

festhalten können. Dabei ist die natürlich die Anordnung der Basen zu berücksichtigen. Nur wenn die beiden Basen $(\mathfrak{x}_1, \ldots, \mathfrak{x}_n)$ und $(\mathfrak{y}_1, \ldots, \mathfrak{y}_m)$ in der aufgeführten Anordnung notiert werden, ist die Matrix A eindeutig bestimmt. Permutation von $\mathfrak{x}_1, \ldots, \mathfrak{x}_n$ oder $\mathfrak{y}_1, \ldots, \mathfrak{y}_m$ führt natürlich in der Regel zu einer von A verschiedenen Matrix. Wählt man aber die Basen von $\mathbf{V}$ und $\mathbf{W}$ als geordnete Basen, so gilt:

Die Aussage

die lineare Abbildung (der lineare Operator) $\alpha : \mathbf{V} \longmapsto \mathbf{W}$ *wird bezüglich der geordneten Basen* $\mathfrak{B}_\mathbf{V}$, $\mathfrak{B}_\mathbf{W}$ *durch die Matrix* A *vermittelt*

lässt sich schematisieren zu

$$\begin{array}{c} \mathbf{V} \overset{(\alpha)}{\longmapsto} \mathbf{W} \\ \mathfrak{B}_\mathbf{V}\,(A)\,\mathfrak{B}_\mathbf{W} \end{array}$$

4. 2. 5 Proposition. *Es gilt die Implikation*

$$\begin{array}{ccc} \mathbf{X} \overset{(\beta)}{\longmapsto} \mathbf{Y} & \& & \mathbf{Y} \overset{(\alpha)}{\longmapsto} \mathbf{Z} \\ \mathfrak{B}_X(B)\mathfrak{B}_Y & & \mathfrak{B}_Y(A)\mathfrak{B}_Z \\ & \Downarrow & \\ \mathbf{X} & \overset{(\alpha\circ\beta)}{\longmapsto} & \mathbf{Z} \\ \mathfrak{B}_X & (AB) & \mathfrak{B}_Z \end{array}$$

BEWEIS. Offenbar ist mit α und β auch $\alpha \circ \beta$ linear, denn $(\alpha \circ \beta)\mathfrak{x}$ ist ja definiert als $\alpha(\beta\,\mathfrak{x})$, woraus die Linearität fast unmittelbar folgt.

Bezeichnen wir nun mit $\downarrow b_k$ den k-ten Spaltenvektor der Matrix B, so haben wir

$$\begin{aligned}
(\alpha \circ \beta)\,(\mathfrak{x}_k) &= \alpha\,(\beta\,(\mathfrak{x}_k)) \\
&= \alpha\,(b_{1,k}\,\mathfrak{y}_1 + \ldots + b_{m,k}\,\mathfrak{y}_m) \\
&= b_{1,k}\,(\alpha\,\mathfrak{y}_1) + \ldots + b_{m,k}\,(\alpha\,\mathfrak{y}_m) \\
&= b_{1,k}\,(a_{11}\,\mathfrak{z}_1 + a_{21}\,\mathfrak{z}_2 + \ldots + a_{\ell,1}\,\mathfrak{z}_\ell) \\
&+ b_{2,k}\,(a_{12}\,\mathfrak{z}_1 + a_{22}\,\mathfrak{z}_2 + \ldots + a_{\ell,2}\,\mathfrak{z}_\ell) \\
&\quad\vdots \\
&+ b_{m,k}\,(a_{1,m}\,\mathfrak{z}_1 + a_{2,m}\,\mathfrak{z}_2 + \ldots + a_{\ell,m}\,\mathfrak{z}_\ell) \\
&= (\mathfrak{a}_1 \cdot \downarrow b_k)\,\mathfrak{z}_1 + (\mathfrak{a}_2 \cdot \downarrow b_k)\,\mathfrak{z}_2 + \ldots + (\mathfrak{a}_e \cdot \downarrow b_k)\,\mathfrak{z}_\ell\,.
\end{aligned}$$

□

Der Leser beachte im weiteren, dass die identische Abbildung ε dann, wenn eine erste Basis $(\,\mathfrak{x}_1{}^*, \ldots, \mathfrak{x}_n{}^*\,)$ zu $\mathbf{V}$ und eine zweite Basis $(\,\mathfrak{x}_1, \ldots, \mathfrak{x}_n\,)$ zu $\mathbf{V}$ in der Rolle von $(\,\mathfrak{y}_1, \ldots, \mathfrak{y}_m\,) \subseteq \mathfrak{V} = \mathfrak{W}$ fixiert sind, die lineare Abbildung $\varepsilon : \mathbf{V} \longmapsto \mathbf{V}$ bezüglich $(\,\mathfrak{x}_1{}^*, \ldots, \mathfrak{x}_n{}^*\,)$, $(\,\mathfrak{x}_1, \ldots, \mathfrak{x}_n\,)$ auch gesehen werden kann als Übergang vom $\mathfrak{x}^*$-System zum $\mathfrak{x}$-System, also in anderen Worten, dass die lineare Abbildung u.a. auch die Koordinatentransformation erfasst. Dabei steht dann die **Start-Basis** $(\,\mathfrak{x}_1{}^*, \ldots, \mathfrak{x}_n{}^*\,)$ in der **Kopf-Zeile** und die **Ziel-Basis** in der **Leit-Spalte.**

Hiernach lässt sich *geradeaus* beweisen:

4. 2. 6 Der Transformationssatz. *Seien* $\mathbf{V}$ *und* $\mathbf{W}$ $\mathcal{K}$*-Vektorräume mit jeweils (geordneten) Basen*

$$\begin{aligned}
&\mathfrak{B}_{\mathbf{V}} = (\,\mathfrak{x}_1, \ldots, \mathfrak{x}_n\,) \\
&\mathfrak{B}_{\mathbf{V}^*} = (\,\mathfrak{x}_1{}^*, \ldots, \mathfrak{x}_n{}^*\,)
\end{aligned} \qquad zu \quad \mathbf{V}$$

$$\begin{aligned}
\textit{und} \qquad &\mathfrak{B}_{\mathbf{W}} = (\,\mathfrak{y}_1, \ldots, \mathfrak{y}_m\,) \\
&\mathfrak{B}_{\mathbf{W}^*} = (\,\mathfrak{y}_1{}^*, \ldots, \mathfrak{y}_m{}^*\,)
\end{aligned} \qquad zu \quad \mathbf{W}$$

und werde der Übergang von $\mathfrak{B}_{\mathbf{V}^*}$ *zu* $\mathfrak{B}_{\mathbf{V}}$*, also die lineare Abbildung* $\varepsilon_{\mathrm{v}} : \mathbf{V} \longmapsto \mathbf{V}$ *bezüglich* $\mathfrak{B}_{\mathbf{V}^*}, \mathfrak{B}_{\mathbf{V}}$ *durch die Matrix* S *und der Übergang von* $\mathfrak{B}_{\mathbf{W}}$ *zu* $\mathfrak{B}_{\mathbf{W}^*}$*, also die lineare Abbildung* $\varepsilon_{\mathrm{w}} : \mathbf{W} \longmapsto \mathbf{W}$ *bezüglich* $\mathfrak{B}_{\mathbf{W}}, \mathfrak{B}_{\mathbf{W}^*}$

durch die Matrix T^* vermittelt. Dann folgt

$$\begin{array}{c}\mathbf{V} \overset{(\alpha)}{\longmapsto} \mathbf{W} \\ \mathfrak{B}_{\mathbf{V}}\,(A)\,\mathfrak{B}_{\mathbf{W}}\end{array} \quad \& \quad \begin{array}{c}\mathbf{V} \overset{(\alpha)}{\longmapsto} \mathbf{W} \\ \mathfrak{B}_{\mathbf{V}^*}\,(A^*)\,\mathfrak{B}_{\mathbf{W}^*}\end{array} \quad \Longrightarrow \quad A^* = T^*AS.$$

BEWEIS. Man beachte zunächst, dass die Verkettung von Abbildungen

$$\alpha : A \longmapsto B,\ \beta : B \longmapsto C,\ \gamma : C \longmapsto D$$

assoziativ ist, was fast *per definitionem* gilt. Das bedeutet aber, dass auch $(T^*A)S = T^*(AS)$ erfüllt ist. Wir betrachten nun

$$\begin{array}{ccc}\mathbf{V} \overset{(\varepsilon_v)}{\longmapsto} \mathbf{V} & \mathbf{V} \overset{(\alpha)}{\longmapsto} \mathbf{W} & \mathbf{W} \overset{(\varepsilon_w)}{\longmapsto} \mathbf{W} \\ \mathfrak{B}_{\mathbf{V}^*}\,(S)\,\mathfrak{B}_{\mathbf{V}} & \mathfrak{B}_{\mathbf{V}}\,(A)\,\mathfrak{B}_{\mathbf{W}} & \mathfrak{B}_{\mathbf{W}}\,(T^*)\,\mathfrak{B}_{\mathbf{W}^*}\end{array}$$

Dann folgt die Behauptung nach 4.2.5: aus

$$\alpha : \begin{array}{c}\mathbf{V} \longmapsto \mathbf{W} \\ \mathfrak{B}_{\mathbf{V}^*}\,(A^*)\,B_{\mathbf{W}^*}\end{array} = \varepsilon_{\mathrm{w}} \circ \alpha \circ \varepsilon_{\mathrm{v}} : \begin{array}{c}\mathbf{V} \longmapsto \mathbf{W} \\ \mathfrak{B}_{\mathbf{V}^*}\,(T^*AS)\,\mathfrak{B}_{\mathbf{W}}\,.\end{array}$$

□

4.3 Der Endomorphismenring $\mathbf{R}\,(\mathbf{V} \longmapsto \mathbf{V})$

Sei im weiteren stets $\mathbf{V} = \mathbf{W}$, also $L\,(\mathbf{V} \longmapsto \mathbf{W}) = E\,(\mathbf{V} \longmapsto \mathbf{V})$ die Menge aller **Endomorphismen** von $\mathbf{V}$ in $\mathbf{V}$. Dann gilt bei festem $\mathfrak{B}_{\mathbf{V}}$ mit

$$\begin{array}{lll} & A \cdot B := (c_{i,k}) & (c_{i,k} = \underset{\rightarrow}{\mathfrak{a}_i} \cdot \downarrow \mathfrak{b}_k) \\ \text{und} & A + B := (c_{i,k}) & (c_{i,k} = a_{i,k} + b_{i,k}) \end{array}$$

$$\text{die Implikation} \quad \begin{array}{c}\alpha \to A \\ \& \\ \beta \to B\end{array} \quad \Longrightarrow \quad \begin{array}{l}\alpha \circ \beta \to A \cdot B \\ \\ \alpha + \beta \to A + B,\end{array}$$

d.h. es entsprechen Endomorphismen und Matrizen bei vorgegebener Basis umkehrbar eindeutig einander unter Erhalt der Operationen. Insbesondere ist damit die Multiplikation von Matrizen assoziativ. Dies regt an zu dem folgenden

Einschub: Wegen des Multiplikationstheorems hat mit den Matrizen A und B auch die Matrix $A \cdot B$ eine nicht verschwindende Determinante, und wegen des Invertierbarkeitskriteriums existiert zu jedem A mit nicht verschwindender Determinante auch die Matrix A^{-1}. Schließlich folgt $A = A \cdot A^{-1} \cdot (A^{-1})^{-1} = (A^{-1})^{-1}$, also $A = (A^{-1})^{-1}$ und damit $A^{-1} \cdot A = E$.

Somit erfüllt die Menge der **regulären** Matrizen, d. h. der Matrizen mit nicht verschwindender Determinante, insgesamt die Gesetze der **Gruppe**, d. h. sie bilden eine Algebra $(G, \cdot, ^{-1})$, die den Regeln genügt:

(A) $A \cdot (B \cdot C) = (A \cdot B) \cdot C$

(E) Es existiert eine $E \in G$ mit $A \cdot E = a = E \cdot A$.

(I) Zu jedem $A \in G$ existiert ein $A^{-1} \in G$ mit $A \cdot A^{-1} = E = A^{-1} \cdot A$.

Wie wir schon wissen, bildet $E\,(\mathbf{V} \longmapsto \mathbf{V})$ einen Vektorraum. Es gilt aber noch mehr, nämlich

4. 3. 1 Proposition. *$(E\,(\mathbf{V} \longmapsto \mathbf{V}), \circ, +)$ bildet einen (natürlich nicht notwendig kommutativen) Ring mit der identischen Abbildung ε als Eins. Die Verifikation der einzelnen Gesetze ist Sache der Routine und darf dem Leser überlassen bleiben.*

Insbesondere ergibt sich aus 4.3.1 für Matrizen fast unmittelbar:

4. 3. 2 Proposition. *Die $n \times n$-Matrizen eines Körpers $\mathcal{K}$ bilden einen Ring mit der Einheitsmatrix E*

$$\begin{pmatrix} 1 & & \mathrm{O} \\ & \ddots & \\ \mathrm{O} & & 1 \end{pmatrix}$$

als Eins.

Hinweis: Weder die lineare Abbildung noch die Matrix basieren auf der Kommutativität von $\mathcal{K}$, und es existiert (sehr wohl) schon eine strukturreiche nicht kommutative lineare Algebra.

Wie wir sahen, hängt die Darstellung eines Endomorphismus $\phi : \mathbf{V} \longmapsto \mathbf{V}$ natürlich von der zugrunde gelegten Basis ab, doch besteht aufgrund des Transformationssatzes ein enger Zusammenhang zwischen den einen

vorgegebenen Endomorphismus ϕ vermittelnden Matrizen. Hinzu kommt, dass im Sonderfall $\mathbf{V} = \mathbf{W}$ und $\mathfrak{B}_{\mathbf{V}} = \mathfrak{B}_{\mathbf{W}}$, $\mathfrak{B}^*_{\mathbf{V}} = \mathfrak{B}^*_{\mathbf{W}}$ die Gleichung

$$ST^* = E = T^*S$$

und damit $T^* = S^{-1}$ erfüllt ist, wegen

$$SU = E = VS \Longrightarrow U = EU = VSU = VE = V\,.$$

Das bedeutet aber

4. 3. 3 Proposition. *Ist $\phi : \mathbf{V} \longmapsto \mathbf{V}$ ein Endomorphismus und A eine ϕ vermittelnde Matrix, so gewinnen wir alle übrigen ϕ vermittelnden Matrizen durch Transformation von A, d.h. als $A^* = S^{-1}AS$ mit invertierbarem S .*

BEWEIS. Vermitteln A und A^* bezüglich vorgegebener Basen $(\mathfrak{x}_1, \ldots, \mathfrak{x}_n)$ und $(\mathfrak{x}_1{}^*, \ldots, \mathfrak{x}_n{}^*)$ dasselbe ϕ, so gilt – wie wir soeben sahen – $A^* = S^{-1}AS$.

Und ist andererseits S invertierbar und $A^* = S^{-1}AS$, so hat S aufgrund von $\mid S \mid \cdot \mid S^{-1} \mid = \mid E \mid = 1$ eine nicht verschwindende Determinante, was $\operatorname{rg} S = n$ impliziert, also Unabhängigkeit der Spalten-Menge von S. Das liefert dann über den Ansatz

$*$			
$\mathfrak{x}_1$	s_{11}	$\cdots\cdots$	$s_{1,n}$
$\vdots$	$\vdots$	$s_{i,k}$	$\vdots$
$\mathfrak{x}_n$	$s_{n,1}$	$\cdots\cdots$	$s_{n,n}$

eine *ℓu Kopfzeile* von Vektoren $(\mathfrak{x}_1{}^*, \ldots, \mathfrak{x}_n{}^*)$ so, dass die Matrix $S^{-1}AS$ bezüglich der „gestirnten" Basis $(\mathfrak{x}_1{}^*, \ldots, \mathfrak{x}_n{}^*)$ denselben Endomorphismus vermittelt wie die Matrix A bezüglich der Basis $(\mathfrak{x}_1, \ldots, \mathfrak{x}_n)$. □

Es können also unendlich viele Matrizen ein und denselben Endomorphismus vermitteln. Es stimmen aber alle diese Matrizen nach dem Multiplikationstheorem in ihrer Determinante überein, wegen

$$\begin{aligned} \mid S^{-1}AS \mid &= \mid S^{-1} \mid \cdot \mid A \mid \cdot \mid S \mid \\ &= \mid A \mid \cdot \mid S^{-1} \mid \cdot \mid S \mid \\ &= \mid A \mid \cdot \mid S^{-1} \cdot S \mid \\ &= \mid A \mid \cdot \mid E \mid \\ &= \mid A \mid . \end{aligned}$$

4. 3. 4 Definition. Sei $\phi : \mathbf{V} \longmapsto \mathbf{V}$ ein Endomorphismus. Dann verstehen wir unter der **Determinante** $\det(\phi)$ **des Endomorphismus** ϕ , auch symbolisiert durch $|\phi|$ den allen ϕ vermittelnden Matrizen A gemeinsamen Wert $\mid A \mid$.

Gilt $A^* = S^{-1}AS$, so nennen wir A und A^* auch **ähnlich**, i. Z. $A \approx A^*$.

Wie man sich leicht klarmacht, hängt die Darstellung eines Endomorphismus von der Gestalt der vermittelnden Matrix ab, und es leuchtet ein, dass die vermittelnde Matrix besonders gut überschaubare Verhältnisse liefert, wenn sie $a_{i,k} = 0$ für alle $i \neq k$ erfüllt. Deshalb wenden wir uns nun der Frage zu, unter welchen Bedingungen sich eine Matrix als ähnlich zu einer **Diagonalmatrix** erweist, kurz unter welchen Bedingungen sich eine Matrix **diagonalisieren** lässt. Zum Zwecke eines ersten Kriteriums formulieren wir vorab das zentrale Begriffspaar der linearen Algebra:

4. 3. 5 Definition. Sei $\phi : \mathbf{V} \longmapsto \mathbf{V}$ ein Endomorphismus. Dann nennen wir $\mathfrak{x} \in \mathfrak{V}$ einen **Eigenvektor** (EV) von ϕ mit dem **Eigenwert** (EW) c, falls

$$\mathfrak{x} \neq \mathfrak{o} \quad \text{und} \quad \phi(\mathfrak{x}) = c\,\mathfrak{x}$$

erfüllt ist. Damit ergibt sich fast unmittelbar:

4. 3. 6 Das 1. Diagonalisierbarkeitskriterium. *Die Matrix A lässt sich genau dann* **diagonalisieren**, *d.h. mittels einer Matrix vom Rang n in eine* **Diagonalmatrix** $S^{-1}AS$ *überführen, wenn* $\mathbf{V}$ *zu jedem von A vermittelten* **Endomorphismus** *eine Basis aus lauter* EVn *besitzt.*

DENN: A liefert zu jeder Basis von $\mathbf{V}$ einen Endomorphismus, und: gibt es wenigstens einen Endomorphismus der genannten Art, so hat jeder Endomorphismus, der von A vermittelt wird, die geforderte Eigenschaft, da Diagonalisierbarkeit eine reine Matrizeneigenschaft ist. □

Das 1. Diagonalisierbarkeitskriterium ist sehr theoretisch. Wir bemühen uns deshalb um ein anwendungsorientiertes 2. Kriterium.

4. 3. 7 Proposition. *Sei $\phi : \mathbf{V} \longmapsto \mathbf{V}$ vermittelt durch A bezüglich der Basis $(\mathfrak{x}_1, \ldots, \mathfrak{x}_n)$. Dann ist $\mathfrak{x} \neq \mathfrak{o}$ Eigenvektor zu ϕ mit dem Eigenwert c gdw. gilt*

$$\begin{array}{rrrrcl} & c & \textit{ist Lösung zu} & \mid A - tE \mid & \doteq & 0 \\ \textit{und} & \mathfrak{x} & \textit{ist Lösung zu} & (A - cE)\mathfrak{u} & \doteq & \mathfrak{o} \end{array}$$

BEWEIS.
$$\begin{array}{rcrcl} \phi\,\mathfrak{x} = c\,\mathfrak{x} & \Longrightarrow & (\phi - c\,\varepsilon)\,\mathfrak{x} & = & \mathfrak{o} \\ & \Longrightarrow & (A - c\,E)\,\mathfrak{x} & = & \mathfrak{o} \\ & \& & \mid A - cE \mid & = & 0 \\ & \Longrightarrow & A\,\mathfrak{x} - c\,\mathfrak{x} & = & \mathfrak{o} \\ & \Longrightarrow & \phi\,\mathfrak{x} & = & c\,\mathfrak{x}. \end{array}$$
□

Ein Beispiel: Wir betrachten $\phi : \mathbf{R^4} \longmapsto \mathbf{R^4}$, vermittelt durch

$$A := \begin{pmatrix} 2 & 0 & 1 & 2 \\ 0 & 2 & -2 & -4 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

Dann folgt:
$$A - tE \quad = \quad \begin{vmatrix} 2-t & 0 & 1 & 2 \\ 0 & 2-t & -2 & -4 \\ 0 & 0 & -t & 1 \\ 0 & 0 & -1 & -t \end{vmatrix}$$

also
$$A - tE = (2-t)^2(t^2+1)\,.$$

Reeller Eigenwert ist demzufolge nur 2.

Um festzustellen, ob $\mathfrak{x}$ ein Eigenvektor ist, haben wir $(A - cE) \cdot \mathfrak{u}$ zu bilden und das Forderungssystem

$$\begin{array}{rcccl} (a_{11} - c) \cdot u_1 & + & \cdots\cdots & + & a_{1,n} \cdot u_n \doteq 0 \\ \vdots & & & & \vdots \\ a_{n,1} \cdot u_1 & + & \cdots\cdots & + & (a_{n,n} - c) \cdot u_n \doteq 0 \end{array}$$

zu untersuchen, in unserem Falle also das System

$$\begin{array}{rcrcrcrcl} (2-2) \cdot u_1 & + & 0 \cdot u_2 & + & 1 \cdot u_3 & + & 2 \cdot u_4 & \doteq & 0 \\ 0 \cdot u_1 & + & 0 \cdot u_2 & + & (-2) \cdot u_3 & + & (-4) \cdot u_4 & \doteq & 0 \\ 0 \cdot u_1 & + & 0 \cdot u_2 & + & (-2) \cdot u_3 & + & 1 \cdot u_4 & \doteq & 0 \\ 0 \cdot u_1 & + & 0 \cdot u_2 & + & (-1) \cdot u_3 & + & (-2) \cdot u_4 & \doteq & 0 \end{array}$$

zu lösen. Lösungen sind hier $(1,0,0,0)$ und $(0,1,0,0)$ sowie deren Linearkombinationen.

Beachte: Die 1., 2. und 4. Gleichung sind paarweise äquivalent.

Hiernach kommen wir zu einem weiteren zentralen Begriff der Endomorphismentheorie.

4. 3. 8 Definition. Sei A eine Matrix. Dann bezeichnen wir

$$\chi_\phi := \mid A - Et \mid$$

als das **charakteristische Polynom** von A. .

Die Berechtigung von „dem charakteristischen Polynom" zu sprechen wir deutlich durch den nun folgenden Satz.

4. 3. 9 Proposition. *Sei ϕ ein Endomorphismus des Vektorraums $\mathbf{V}$. Dann erzeugen alle ϕ vermittelnden Matrizen das gleiche charakteristische Polynom. In anderen Worten: Sind A und A^* ähnlich, so gilt $\mid A - tE \mid = \mid A^* - tE \mid$.*

BEWEIS. Sei $A^* = S^{-1}AS$. Wir betrachten die Elemente $a_{i,k}$ und $s_{i,k}$ sowie das Element t als Unbestimmte über $\mathcal{K}$. Dann gilt in dem von diesen Unbestimmten erzeugten Körper der rationalen Funktionen über $\mathcal{K}$

$$\begin{aligned} \mid A^* - tE \mid &= \mid S^{-1}AS - S^{-1}tES \mid \\ &= \mid S^{-1} \cdot (A - tE) \cdot S \mid \\ &= \mid S^{-1} \mid \cdot \mid A - tE \mid \cdot \mid S \mid \\ &= \mid A - tE \mid . \end{aligned}$$

Daher gilt unsere Behauptung erst recht, denn man fasse im Nachhinein die $a_{i,k}$ und $s_{i,k}$ wieder auf als Elemente aus $\mathcal{K}$. □

Der letzte Satz gibt Anlass zu der weiteren Erklärung

4. 3. 10 Definition. Sei ϕ ein Endomorphismus des n-dimensionalen Vektorraums $\mathbf{V}$. Dann verstehen wir unter dem **charakteristischen Polynom χ_ϕ von ϕ** das allen ϕ vermittelnden Matrizen A gemeinsame charakteristische Polynom χ_A .

Wir interessieren uns weiterhin für die Frage, wann sich ein Endomorphismus durch eine *Diagonalmatrix* vermitteln lässt, also für die Frage, wann eine Matrix A ähnlich ist zu einer Diagonalmatrix D. Hierzu geben wir vorab noch einen Hilfssatz sowie eine Definition.

4. 3. 11 Lemma. *Seien $\mathfrak{x}_1, \ldots, \mathfrak{x}_r$ Eigenvektoren zum Endomorphismus ϕ des Vektorraumes $\mathbf{V}$ mit paarweise verschiedenen Eigenwerten $c_1, \ldots, c_r$. Dann ist die Menge der Vektoren $\{\, \mathfrak{x}_1, \ldots, \mathfrak{x}_r \,\}$ linear unabhängig.*

BEWEIS. Wendet man den Endomorphismus $\phi - c_i\,\varepsilon$ auf den Vektor $\mathfrak{x}_j$ an, so erhält man

$$\begin{aligned}(\phi - c_i\,\varepsilon)\,\mathfrak{x}_j &= \phi\,\mathfrak{x}_j - c_i\,\mathfrak{x}_j \\ &= c_j\,\mathfrak{x}_j - c_i\,\mathfrak{x}_j = (c_j - c_i)\,\mathfrak{x}_j \ ,\end{aligned}$$

also den Nullvektor für $i = j$. Somit folgt aus

$$s_1\,\mathfrak{x}_1 + s_2\,\mathfrak{x}_2 + \cdots + s_r\,\mathfrak{x}_r = \mathfrak{o}$$

bei sukzessiver Anwendung der $\phi - c_i\,\varepsilon$ mit $i \neq j$

$$s_j \cdot (c_j - c_1)(c_j - c_2)\cdots(c_j - c_{j-1})(c_j - c_{j+1})\cdots(c_j - c_r)\,\mathfrak{x}_j = \mathfrak{o},$$

so dass $s_j = 0$ wegen $i \neq j \Longrightarrow c_i - c_j \neq 0$ verschwinden muss, da $\mathfrak{x}_j$ EV ist, also nicht der Nullvektor sein kann. □

Offenbar bildet die Menge aller $\mathfrak{x}$ mit $\phi\,\mathfrak{x} = c\mathfrak{x}$ stets einen Unterraum. Hierzu erklären wir:

4. 3. 12 Definition. Sei c ein Eigenwert zu ϕ. Dann nennen wir den Unterraum $(\,\{\mathfrak{x} \mid \phi\,\mathfrak{x} = c\,\mathfrak{x}\}\,,\,+\,,\,s\cdot\,)$ den zu c gehörenden **Eigenraum**, i. Z. $\mathbf{ER}\,(c)$.

Hiernach lässt sich beweisen

4. 3. 13 Das 2. Diagonalisierbarkeitskriterium. *Sei $\mathbf{V}$ ein n-dimensionaler Vektorraum und $\phi : \mathbf{V} \longmapsto \mathbf{V}$ bezüglich einer geeigneten Basis vermittelt durch die Matrix A. Dann sind die Aussagen äquivalent:*

(*i*) *ϕ lässt sich durch eine Diagonalmatrix $D = S^{-1}AS$ vermitteln.*

(*ii*) $\mid A - tE \mid$ *zerfällt in Linearfaktoren und die Ordnung eines jeden Eigenwertes* c_i *in* $\mid A - tE \mid$ *ist gleich der Dimension von* $\mathbf{ER}\,(c_i)$. [2)]

BEWEIS. $(i) \Longrightarrow (ii)$. Lässt sich ϕ durch eine Diagonalmatrix vermitteln und zwar so, dass die EW c_i in der Diagonalen jeweils k_i mal auftreten, so folgt:

$$\mid D - tE \mid = (c_1 - t)^{k_1} \cdot (c_2 - t)^{k_2} \cdot \ldots \cdot (c_r - t)^{k_r},$$

und es steht in der Matrix $(D - c_i\, E)$ an k_i vielen Stellen eine 0, also an $n - k_i$ vielen Stellen ein Wert $c_i - c_j \neq 0$. Das liefert aber

$$\begin{aligned} \dim\left(\mathbf{ER}\,(c_i\,)\right) &= \dim\left(\mathbf{Ker}\,(A - c_i\, E)\right) \\ &= n - \dim\left(\mathbf{Im}\,(A - c_i\, E)\right) \\ &= n - \mathrm{rg}\,(A - c_i\, E) \\ &= n - (n - k_i\,) = k_i\,. \end{aligned}$$

$(ii) \Longrightarrow (i)$. Seien $c_1, \ldots, c_r$ die verschiedenen EW von ϕ mit den entsprechenden Vielfachheiten $k_1, \ldots, k_r$. Dann zerfällt $\mid A - tE \mid$ genau dann in Linearfaktoren, wenn $\sum\limits_{1}^{r} k_i = n$ erfüllt ist. Gilt dies sowie zusätzlich

$$\dim\left(\mathbf{ER}(c_i\,)\right) = k_i \qquad (1 \leq i \leq r),$$

so besitzt jeder $\mathbf{ER}\ (c_i\,)$ eine Basis $(\mathfrak{a}_{i,1}, \ldots, \mathfrak{a}_{i,k_i})$.

Wir zeigen nun, dass die Menge dieser $\mathfrak{a}_{i,j}$ ℓu ist, also eine Basis aus lauter EVn bildet. Hierzu gehen wir aus von

$$\begin{array}{ccccccccc} & s_{11}\,\mathfrak{a}_{11} & + & s_{12}\,\mathfrak{a}_{12} & + & \cdots & + & s_{1,k_1}\,\mathfrak{a}_{1,k_1} \\ + & s_{21}\,\mathfrak{a}_{21} & + & s_{22}\,\mathfrak{a}_{22} & + & \cdots & + & s_{2,k_2}\,\mathfrak{a}_{2,k_2} \\ & + & & & & & & \\ & \vdots & & & & & & \\ + & s_{r,1}\,\mathfrak{a}_{r,1} & + & s_{r,2}\,\mathfrak{a}_{r,2} & & +\cdots+ & & s_{r,k_r}\,\mathfrak{a}_{r,k_r} \end{array} = \mathfrak{o}$$

und bezeichnen die Zeilen $\sum\limits_{1}^{k_i} s_{i,j}\,\mathfrak{a}_{i,j}$ mit $\mathfrak{b}_i$.

[2)] Hierfür sagt man auch kürzer: die **algebraische** und die **geometrischen Ordnung** eines jeden EW sind gleich.

Dann gilt $\sum \mathfrak{b}_i = \mathfrak{o}$, und es ist jeder Summand $\mathfrak{b}_i$ gleich $\mathfrak{o}$ oder ein EV mit dem EW c_i. Das bedeutet aber $\mathfrak{b}_i = \mathfrak{o}$ $(1 \leq i \leq r)$, da nach dem letzten Lemma eine Summe von EVn mit paarweise verschiedenen EWn nicht verschwinden kann. Somit haben wir $s_{i,k} = 0$ für alle i, j – man beachte die Basiseigenschaft der einzelnen $(\mathfrak{a}_{i,1}, \ldots, \mathfrak{a}_{i,k_i})$. □

Das soeben formulierte Kriterium wurde für beliebige Körper ausgesprochen. Legen wir hingegen den speziellen Körper $(\mathbf{C}, +, \cdot)$ zugrunde, so dürfen wir auf Besseres hoffen. Vergleiche hierzu Abschnitt 9.

Bei den Anwendungen der Diagonalisierung – etwa in der Theorie der Differentialgleichungen – interessiert nicht nur die Frage, *ob* sich eine Matrix A diagonalisieren lässt, sondern auch die Frage, *wie* dies möglich ist. Um dies allgemein zu klären, gehen wir aus von einer Basis $(\mathfrak{x}_1, \ldots, \mathfrak{x}_n)$ und betrachten den Endomorphismus ϕ_A.

Ist A diagonalisierbar, so existiert eine Basis von EVn $\mathfrak{e}_1, \ldots, \mathfrak{e}_n$ zu ϕ und umgekehrt, und wir finden eine Diagonalmatrix zu A, indem wir A nach dem Transformationssatz transformieren – wobei $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ die Rolle von $(\mathfrak{x}_1{}^*, \ldots, \mathfrak{x}_n{}^*)$ übernimmt.

Ist dann S diejenige Matrix, die die EVn $\mathfrak{e}_1, \ldots, \mathfrak{e}_n$ im $\mathfrak{x}$-System darstellt, also die lineare Abbildung $\varepsilon : \mathbf{V} \longmapsto \mathbf{V}$ bezüglich $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$, $(\mathfrak{x}_1, \ldots, \mathfrak{x}_n)$, so erhalten wir

ε	$\mathfrak{e}_1$	.....	$\mathfrak{e}_n$
$\mathfrak{x}_1$	e_{11}	.....	$e_{1,n}$
$\vdots$	$\vdots$	$e_{i,k}$	$\vdots$
$\mathfrak{x}_n$	$e_{n,1}$	.....	$e_{n,n}$.

Das bedeutet aber, dass sich A mit jeder Matrix transformieren lässt, deren Spalten von EVn gebildet werden.

Damit hat sich zusätzlich ergeben, dass unterschiedliche Matrizen S dieselbe Transformation zu bewirken vermögen.

Letztendlich ist natürlich die Frage interessant, wie man zu einer vorgegebenen invertierbaren Matrix S die inverse Matrix S^{-1} auf günstigem Wege findet. Hierzu verweisen wir auf den Abschnitt über den GAUSSschen Algorithmus. und betrachten $E \cdot A = A$.

Formen wir die rechte Seite elementar um durch Multiplikation der i-ten Zeile mit c, so entspricht dies einer Multiplikation von links mit derjenigen Matrix, die aus der Einheitsmatrix dadurch hervorgeht, dass man die Eins an der Stelle (i,i) ersetzt durch c, wir wollen diese Matrix bezeichnen mit $E_{i,c}$. Dies überführt $E \cdot A = A$ in $E_{i,c} \cdot E \cdot A = E_{i,c} \cdot A$.

Weiter entspricht der Addition der k-ten zur i-ten Zeile in B die Multiplikation von links mit derjenigen Matrix, die wir erhalten, wenn wir in$E$ die k-te zur i-ten Zeile addieren. Diese Matrix sei bezeichnet mit – man beachte die Reihenfolge – $E_{i,k}$. Dies überführt B nach $E_{i,k} \cdot B$.

Insgesamt können wir also, wenn wir unter E_i ganz allgemein eine *elementare Umformungsmatrix* verstehen, nach sukzessiver Multiplikation von links mit Matrizen E_i die rechte Seite von $E \cdot A = A$ überführen in $(E_n \circ E_{n-1} \circ \ldots \circ E_1) \circ A = E$, wobei die linke Seite übergeht in $(E_n \circ E_{n-1} \circ \ldots \circ E_1) \circ E) \circ A$. Hierbei ist dann $(E_n \circ E_{n-1} \circ \ldots \circ E_1) \circ E)$ die inverse Matrix zu A.

Damit erhalten wir das folgende Verfahren zur Inversenbestimmung einer Matrix A:

Schreibe A links neben die Matrix E und forme A und E simultan um, bis A in E überführt ist. Dann ist E überführt nach A^{-1}.

4.4 Eine Anwendung aus der Analysis.*

Viele Phänomene in der Physik, Chemie, Biologie und Ökonomie werden durch **Differentialgeichungen** beschrieben; das sind Gleichungen, die neben einer Funktion auch ihre Ableitungen enthalten. Wir werden jetzt sehen, wie sich bestimmte Differentialgleichungssysteme mit Mitteln der linearen Algebra lösen lassen. Dabei können wir das Gebiet nur oberflächlich behandeln. Es geht uns eher darum, die Anwendungsmöglichkeiten der linearen Algebra anzudeuten.

Zur Terminologie: Eine der einfachsten Differentialgleichungen ist

$$y' = ay \tag{4.3}$$

die die unbekannte Funktion $y = f(x)$ durch ihre Ableitung $y' = dy/dx$ und eine Konstante a beschreibt. Wie die meisten Differentialgleichungen

hat (4.3) unendlich viele Lösungen; diese haben die allgemeine Form

$$y = ce^{ax} \tag{4.4}$$

mit einer beliebigen Konstanten c. Jede dieser Funktionen erfüllt die Gleichung $y' = a$, denn

$$y' = ace^{ax} = ay.$$

Umgekehrt ist jede Lösung von $y' = a$ eine Funktion $c * a^a$ (Analysis). Wir nennen (4.4) dann die **allgemeine Lösung** von $y' = a$.

Oft erzeugt ein physikalisches Problem nicht nur eine Differentialgleichung, sondern liefert eine zusätzliche Bedingung, mit der wir eine Partikularlösung erhalten können. Verlangen wir etwa, dass die Lösung von $y' = a$ die Gleichung

$$y(0) = 3$$

erfüllt, so setzen wir in der allgemeinen Lösung $y = 3$ und $x = 0$ ein. Daraus erhalten wir die Konstante

$$c = ce^0 = 3\,,$$

weshalb sich unter der Zusatzforderung $y(0)$

$$y = 3e^{ax}$$

als eindeutig bestimmte Lösung von $y' = a$ ergibt. Eine Gleichung wie (3), die einen Funktionswert der Lösung festlegt, heißt eine **Anfangs-Bedingung;** eine Differentialgleichung mit vorgegebener Anfangsbedingung heißt ein **Anfangswert-Problem.**

Lineare Differentialgleichungssysteme erster Ordnung

Wir behandeln Differentialgleichungssysteme der Form

$$\begin{array}{rcccccccc}
y_1' & = & a_{11}\,y_1 & + & a_{12}\,y_2 & + & \cdots & + & a_{1,n}\,y_n \\
y_2' & = & a_{21}\,y_1 & + & a_{22}\,y_2 & + & \cdots & + & a_{2,n}\,y_n \\
\vdots & & \vdots & & \vdots & & \vdots & & \\
\vdots & & \vdots & & \vdots & & \vdots & & \\
y_n' & = & a_{n,1}\,y_1 & + & a_{n,2}\,y_2 & + & \cdots & + & a_{n,m}\,y_n
\end{array} \tag{4.5}$$

mit den zu bestimmenden Funktionen

$$y_1 = f(x),\ y_2 = f_2(x), \ldots,\ y_n = f_n(x)\ ,$$

wobei die a_{ij} Konstanten sind. In Matrixschreibweise ergibt sich aus (4)

$$\begin{bmatrix} y_1' \\ y_2' \\ \vdots \\ y_n' \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}$$

oder in Kurzform $$Y' = AY.$$

Beispiel 1 : (a) Man schreibe das folgende System als Matrixgleichung:

$$\begin{aligned} y_1' &= 3y_1 \\ y_2' &= -2y_2 \\ y_3' &= 5y_3. \end{aligned}$$

(b) Man löse das System.

(c) Welche Lösung erfüllt $y_1(0) = 1,\ y_2(0) = 4,\ y_3(0) = -2$?

Lösung a). Wir erhalten

$$\begin{bmatrix} y_1' \\ y_2' \\ y_3' \end{bmatrix} = \begin{bmatrix} 3 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 5 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} \tag{4.6}$$

oder

$$Y' = \begin{bmatrix} 3 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 5 \end{bmatrix} Y.$$

Lösung b). Da in jeder Gleichung nur eine der Unbekannten vorkommt, können wir sie unabhängig voneinander lösen. Nach (4.4) hat das System die allgemeine Lösung

$$\begin{aligned} y_1 &= c_1 e^{3x} \\ y_2 &= c_2 e^{-2x} \\ y_3 &= c_3 e^{5x} \end{aligned}$$

oder in Matrixschreibweise die Lösung:

$$Y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} c_1 e^{3x} \\ c_2 e^{-2x} \\ c_3 e^{5x} \end{bmatrix}.$$

Lösung c). Aus den Anfangsbedingungen ergeben sich

$$\begin{aligned} 1 &= y_1(0) = c_1 e^0 = c_1 \\ 4 &= y_2(0) = c_2 e^0 = c_2 \\ -2 &= y_3(0) = c_3 e^0 = c_3. \end{aligned}$$

Daraus erhalten wir die Partikularlösung

$$y_1 = e^{3x}, \quad y_2 = 4e^{-2x}, \quad y_3 = -2e^{5x}$$

oder

$$Y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} e^{3x} \\ 4e^{-2x} \\ -2e^{5x} \end{bmatrix}.$$

Das Differentialgleichungssystem des letzten Beispiels ist leicht zu lösen, da die einzelnen Gleichungen nur eine unbekannte Funktion enthalten. Das ist darauf zurückzuführen, dass die Koeffizeintenmatrix des Systems Diagonalgestalt hat. Diese Tatsache liefert einen Hinweis zur Lösung eines beliebigen Differentialgleichungssystems

$$Y' = AY.$$

Man versucht, durch eine geeignete Substitution für Y ein System mit diagonaler Koeffizientenmatrix zu erzeugen, dessen Lösung sich leichter bestimmen lässt. Aus dieser erhält man durch Rücksubstitution eine Lösung des ursprünglichen Systems. Wir betrachten die Substitution

$$\begin{array}{rcccccccc} y_1 &=& p_{11}\,u_1 &+& p_{12}\,u_2 &+& \cdots &+& p_{1,n}\,u_n \\ y_2 &=& p_{21}\,u_1 &+& p_{22}\,u_2 &+& \cdots &+& p_{2,n}\,u_n \\ \vdots && \vdots && \vdots && \vdots && \vdots \\ y_n &=& p_{n,1}\,u_1 &+& p_{n,2}\,u_2 &+& \cdots &+& p_{n,n}\,y_n \end{array} \tag{4.7}$$

die der Matrixgleichung

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \vdots & \vdots & & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix}$$

entspricht, bzw. in Kurzform erfüllt:

$$Y = PU$$

Die Konstanten p_{ij} sollen so beschaffen sein, dass die Koeffizientenmatrix des neuen Systems mit den unbekannten Funktionen $u_1, u_2, \ldots, u_n$ Diagonalgestalt hat. Es ist

$$Y' = PU'$$

(der Beweis bleibt dem Leser als Übungsaufgabe überlassen), wir können also in das gegebene System

$$Y' = AY$$

$Y = PU$ und $Y' = PU'$ einsetzen:

$$PU' = A(PU).$$

Unter der Annahme, dass P invertierbar ist, ergibt sich daraus

$$\begin{aligned} U' &= (P^{-1}AP)U, \\ U' &= DU \end{aligned}$$

also
mit $D = P^{-1}AP$. Hiernach versteht es sich, dass wir für P als eine Matrix wählen, die A diagonalisiert.

Ein Lösungsverfahren

Nach den oben angestellten Überlegungen erhalten wir als ein mögliches Lösungsverfahren für ein Differentialgleichungssystem

$$Y' = AY$$

mit diagonalisierbarer Koeffezientenmatrix A:

Schritt 1. Man bestimme eine Matrix P, die A diagonalisiert.

Schritt 2. Die Substitution $Y = PU$ und $Y' = PU'$ erzeugt ein neues System $U' = DU$ mit der Diagonalma
trix $D = P^{-1}AP$.

Schritt 3. Man löse das System $U' = DU$.

Schritt 4. Man berechne Y aus der Matrixgleichung $Y = PU$.

4.5 Das Minimalpolynom *

Mit Hilfe des charakteristischen Polynoms lassen sich theoretisch die EW eines Endomorphismus ermitteln. In der Praxis jedoch lassen sich die Nullstellen eines Polynoms natürlich nur angenähert berechnen – jedenfalls in der Regel –, und es hängt der Arbeitsaufwand ganz wesentlich auch am Grad des betrachteten Polynoms.

Deshalb soll in diesem Abschnitt ein weiteres Polynom betrachtet werden, das ebenso wie das charakteristische Polynom Auskunft über die Diagonalisierbarkeit einer Matrix gibt, in vielen Fällen jedoch von geringerem Grade ist.

Sei im folgenden $\mathbf{Z}$ ein komplexer Vektorraum der Dimension n. Dann gibt es bei vorgegebenem Endomorphismus ϕ eine Linearkombination

$$a_0 + a_1\,\phi + a_2\,\phi^2 + \cdots + a_{n^2-1}\,\phi^{n^2-1} + \phi^{n^2} = 0,$$

also ein $f(t)$ mit $f(\phi) = 0$. Denn, wir wissen ja, dass der Raum der Endomorphismen die Dimension n^2 hat.

Offenbar erzeugt jedes $g(t) \in \mathbf{C}(t)$ ein eindeutig bestimmtes $g(\phi)$, und es gelten die beiden Gleichungen:

$$\begin{aligned} (f+g)(\phi) &= f(\phi) + g(\phi) \quad \textit{per definitionem} \\ \text{und} \quad (f\cdot g)(\phi) &= f(\phi)\circ g(\phi) \quad \textit{per calculationem}. \end{aligned}$$

Sei nun $h_1(\phi) = 0 = h_2(\phi)$ erfüllt. Dann folgt $(h_1 - h_2)(\phi) = 0$. Somit gibt es nicht nur ein g mit $g(\phi) = 0$ von minimalem Grad, sondern wir dürfen dieses g sogar als **normiert** annehmen, d. h. als eindeutig bestimmt bei höchstem Koeffizienten 1.

4. 5. 1 Definition. Sei ϕ ein Endomorphismus von $\mathbf{Z}$. Dann nennen wir das eindeutig bestimmte Polynom g_ϕ mit den Eigenschaften

(i) g_ϕ ist normiert,

(ii) g_ϕ ist unter allen $h(t)$ mit $h(\phi) = 0$ von minimalem Grad,

das zu ϕ gehörende **Minimalpolynom** .

4. 5. 2 Lemma. *Das Minimalpolynom g_ϕ ist Teiler eines jeden h mit $h(\phi) = 0$.*

DENN: $h(\phi) = 0 \;\&\; h = g_\phi q + r \;\; (r = 0 \text{ V } \operatorname{grad}(r) < \operatorname{grad}(g_\phi))$ führt zu:

$$r(\phi) = h(\phi) - g_\phi(\phi)q(\phi) = 0 \rightsquigarrow r = 0.$$

□

Hiernach können wir zeigen:

4. 5. 3 Proposition. *Das Minimalpolynom $g_\phi =: g$ zu dem Endomorphismus $\phi : \mathbf{Z} \longmapsto \mathbf{Z}$ ist Teiler des charakteristischen Polynoms $f_\phi =: f$, und es hat g_ϕ dieselben Nullstellen wie f_ϕ.*

BEWEIS. Hat $\mathbf{Z}$ die Dimension 1 oder f den Grad 1, so ist nichts zu zeigen. Sei also der Satz schon bewiesen für

$$\dim \mathbf{Z} \leq k \;\text{ und }\; \operatorname{grad}(f) \leq m$$

und sei im weiteren

$$\dim \mathbf{Z} = k+1 \;\text{ und }\; \operatorname{grad}(f) = m+1.$$

Ist dann c ein Nullstelle von f, also ein EW zu ϕ, so gibt es einen EV $\mathfrak{a}$ mit

$$\phi\,\mathfrak{a} \;=\; c\,\mathfrak{a},$$

und es besitzt der Unterraum

$$\mathbf{U} \;:=\; (\phi - c\,\varepsilon)\,\mathbf{Z}$$

eine Dimension unterhalb von $\dim \mathbf{Z}$, wegen $\ker \phi - c\varepsilon \neq \mathfrak{O}$.

Ist nun $\mathbf{U} = \mathbf{O}$, so ist $g = t - c$ und $f = (c-t)^n$, womit in diesem Falle die Behauptung bewiesen ist.

Ist aber $\mathbf{U} \neq \mathbf{O}$, so können wir schließen:

$$\begin{aligned} \phi\,\mathfrak{U} &= \phi\,((\phi - c\varepsilon)\,\mathfrak{Z}) \\ &= (\phi - c\,\varepsilon)\;(\phi\,\mathfrak{Z}) \\ &\subseteq (\phi - c\varepsilon)\,\mathfrak{Z} \\ &= \mathfrak{U}, \end{aligned}$$

weshalb $\phi|_{\mathbf{U}} =: \phi_u$ einen Endomorphismus von $\mathbf{U}$ liefert.

Wir betrachten nun eine Basis $(\mathfrak{x}_1, \ldots, \mathfrak{x}_n)$ zu $\mathbf{Z}$ mit $[\mathfrak{x}_{k+1}, \ldots, \mathfrak{x}_n] = \mathfrak{U}$. Dann gilt

$$\begin{aligned} (\phi - c\varepsilon)\,\mathfrak{x}_i &=: \mathfrak{u}_i \in \mathfrak{U} \\ &\rightsquigarrow \\ \phi\,\mathfrak{x}_i &= c\,\mathfrak{x}_i + \mathfrak{u}_i \;\; (1 \leq i \leq k) \\ \&\;\; \phi\,\mathfrak{x}_j &\in \mathfrak{U} \quad (k+1 \leq j \leq n). \end{aligned}$$

Das liefert eine Abbildungsmatrix der Form

$$\left(\begin{array}{ccc|c} c & & & \\ & \ddots & & O \\ & & c & \\ \hline B & & & A_u \end{array}\right)$$

worin A_u eine der Abbildung ϕ_u zugeordnete Matrix ist. Damit folgt dann für ein geeignetes k

$$\begin{aligned} f(t) &= |A - t\,E| \\ &= (c-t)^k \cdot |A_u - t\,E| \\ &= (c-t)^k \cdot f_u(t) \end{aligned}$$

mit $g_u \,|\, f_u$ (man beachte: $\dim \mathbf{U} \leq k$, grad $f_u \leq m$). Ferner haben wir:

$$\begin{aligned} g_u(\phi)\,(\,(\phi - c\varepsilon)\,\mathbf{Z}) &= g_u(\phi)\,\mathbf{U} = \mathbf{O} \\ \text{und} \qquad (\phi - c\varepsilon)\,[\,\mathfrak{a}] &= \mathbf{O}. \end{aligned}$$

Das führt aber zu

$$g \,|\, g_u(t-c) \,|\, f\,, \quad \text{wegen} \quad (g_u(\phi)\cdot(\phi - c\varepsilon))\mathfrak{Z} = \mathfrak{O}$$

und zu

$$(t-c) \,|\, f\,, \quad \text{wegen} \quad g\,(\phi)\,[\,\mathfrak{a}\,] = \mathfrak{O}.$$

Damit sind wir am Ziel. □

4. 5. 4 Ein 3. Diagonalisierbarkeitskriterium. *Sei* $\mathbf{Z}$ *ein komplexer* n*–dimensionaler Vektorraum. Dann ist der Endomorphismus* $\phi : \mathbf{Z} \longmapsto \mathbf{Z}$ *genau dann diagonalisierbar, wenn das Minimalpolynom* g_ϕ *fremd ist zu seiner Ableitung (im Sinne der Analysis).*

BEWEIS. ϕ ist nach dem 2. Diagonalisierbarkeitskriterium genau dann diagonalisierbar, wenn für jeden Eigenwert c die Dimension des zugehörigen Eigenraumes $\mathbf{ER}$(c) gleich der Ordnung von c ist. Es war aber im Beweis des letzten Satzes $\dim\,(\mathrm{im}\,(\phi - c\varepsilon)) = \dim \mathbf{U} = n - k$. Wäre nun c ebenfalls Nullstele zu f_u, so erhielten wir zum einen $(t-c)^{k+1} \,|\, f(t)$ und zum andern

$$\begin{aligned} \dim\,(\mathbf{ER}(c)) &= \dim\,(\ker\,(\phi - c\varepsilon)) \\ &= n - \dim\,(\mathrm{im}\,(\phi - c\varepsilon)) \\ &= n - (n-k) = k \\ &< k+1, \end{aligned}$$

mit Widerspruch!

Daher ist Diagonalisierbarkeit von ϕ gleichbedeutend damit, dass kein EW c schon Nullstelle *seines* f_u, also *seines* g_u ist, und folglich damit, dass g_ϕ nur *einfache* Wurzeln hat.

Und das wiederum ist gleichbedeutend damit, dass g_ϕ und g'_ϕ keine gemeinsame Nullstelle haben, wegen;

$$\begin{aligned} & g_\phi(t) &=& (t-c)\cdot h(t) \\ \Longrightarrow \quad & g'_\phi(t) &=& h(t) + (t-c)\cdot h'(t). \end{aligned}$$

Damit ist unsere Behauptung bewiesen, da zwei Polynome über $\mathbf{C}$ wegen des Fundamentalsatzes der Algebra genau dann fremd sind, wenn sie keine gemeinsame Nullstelle haben. □

Hinweis: Der Wert von 4.5.4 liegt darin, dass sich der GGT zweier Polynome über $\mathbf{C}$ nach Euklid und das Minimalpolynom nach KOWALSKY, etwa 9. Auflage, S. 127, konstruktiv ermitteln lassen, was bedeutet, dass sich Diagonalisierbarkeit konstruktiv entscheiden lässt.

Insbesondere hat dieser Abschnitt zusätzlich geliefert:

4. 5. 5 Das Theorem von Caley/Hamilton. *Ist* $\phi : \mathbf{Z} \longmapsto \mathbf{Z}$ *ein Endomorphismus und* A *eine seiner vermittelnden Matrizen, so liefert die Matrix* A*, eingesetzt in* χ_ϕ *die Nullmatrix, also die Gleichung:* $\chi_\phi(A) = 0$.

Kapitel 5

Räume mit innerem Produkt

5.1 Skalare Produkte

Soll ein Algebra-Kalkül klassische geometrische Anwendungen ermöglichen, so ist als Minimalforderung zu stellen, dass sich Strecken sowohl als auch Winkel „messen" lassen. Dies gehört zum Schulstoff und wird dort gewährleistet über die Vektorrechnung. Grundlegend ist hier der Begriff des skalaren Produktes geometrischer Vektoren, definiert *Skalarprodukt* zu *via*

$$[\mathfrak{a}, \mathfrak{b}] = |\mathfrak{a}||\mathfrak{b}| \cos\theta\,,$$

wobei θ der von den beiden Vektoren eingeschlossene Winkel $\leq \pi$ ist.

Dieses Produkt gilt es algebraisch zu fassen, soll die Berechnung von Winkeln über die Koordinaten der Vektoren möglich werden.

Wiederholen wir deshalb zunächst den Kosinussatz. Er besagt:

5. 1. 1 Der Kosinussatz. *In jedem Dreieck ΔABC gilt*

(KS) $$c^2 \;=\; a^2 + b^2 - 2ab\cos\gamma$$

BEWEIS. Wir betrachten die Abbildung 5.1. Hier haben wir

$$\begin{aligned} c^2 &= y^2 + h^2 \\ &= (b-x)^2 + h^2 \\ &= b^2 - 2bx + x^2 + h^2 \\ &= b^2 - 2ba\cos\gamma + a^2 \\ &= a^2 + b^2 - 2ab\cos\gamma \end{aligned}$$

□

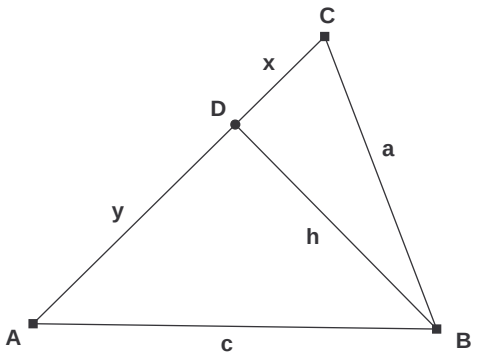


Abbildung 5.1: Zum Kosinussatz

Hiernach sind wir in der Lage, die gewünschte Algebraisierung zu realisieren:

5. 1. 2 Proposition. *Sind* $\mathfrak{u} = (u_1, u_2, u_3)$ *und* $\mathfrak{v} = (v_1, v_2, v_3)$ *zwei nicht verschwindende Vektoren des* $\mathbf{R}^3$*, so gilt:*

$$[\mathfrak{u}, \mathfrak{v}] = u_1v_1 + u_2v_2 + u_3v_3 \tag{5.2}$$

BEWEIS. Nach dem Kosinussatz gilt für den Vektor $\mathfrak{v} - \mathfrak{u}$

$$|\mathfrak{v} - \mathfrak{u}|^2 = |\mathfrak{u}|^2 + |\mathfrak{v}|^2 - 2|\mathfrak{u}||\mathfrak{v}| \cos\theta \tag{5.3}$$

also

$$\mathfrak{u}\mathfrak{v} = \frac{1}{2}\left(|\mathfrak{u}|^2 + |\mathfrak{v}|^2 - |\mathfrak{v} - \mathfrak{u}|^2\right) \tag{5.4}$$

Setzen wir nun

$$|\mathfrak{u}|^2 = u_1^2 + u_2^2 + u_3^2 \tag{5.5}$$

$$|\mathfrak{v}|^2 = v_1^2 + v_2^2 + v_3^2 \tag{5.6}$$

$$|\mathfrak{v} - \mathfrak{u})|^2 = (v_1 - u_1) + (v_2 - u_2) + (v_3 - u_3) \tag{5.7}$$

so erhalten wir nach Einsetzen in der Tat

$$\mathfrak{u}\mathfrak{v} = u_1v_1 + u_2v_2 + u_3v_3 \tag{5.8}$$

□

Diese Form des Skalarproduktes lässt sich auf jeden endlich dimensionalen Vektorraum übertragen, und das haben wir ja „oben" auch schon getan. Um jedoch eine möglichst starke „korrespondierende" Geometrie zu gewährleisten, bedarf es natürlich gewisser Einengungen der vorgegebenen

Vektorraums, und hier bietet sich die Forderung eines Körpers von Skalaren an, der einen *Vektorbetrag* ermöglicht.

Dies veranlasst uns von nun an grundsätzlich nur noch reelle bzw. komplexe Vektorräume zu betrachten. Hier haben wir ja zumindest im endlich dimensionalen Fall die Möglichkeit der Betragsdefinition

$$|(x_1, x_2, \ldots, x_n)| := \sqrt{\sum (x_i^2)}$$

Nach diesem Vorspann [1] sei noch einmal festgehalten:

Im folgenden befassen wir uns mit den „klassischen", das sind die **reellen** und **komplexen Vektorräumen**, denen eine zusätzliche Struktur aufgeprägt ist, und zwar nehmen wir an, dass ein **Skalares Produkt** [2] erklärt ist, wodurch **Längen-** und **Winkelmessung** möglich werden.

Es wird also darum gehen, den Begriff Skalares Produkt – auch kurz **Skalarprodukt** optimal auf den Sonderfall abzustimmen, in dem der zugrunde gelegte Körper gleich $\mathcal{R}$ oder $\mathcal{C}$ ist.

Skalare Produkte können auf mannigfache Weise erklärt werden, demzufolge sind die Begriffe Länge und Winkel(-größe) Relativbegriffe, die von der Wahl des Skalarproduktes abhängen.

Als wesentlich wird sich vor allem der Begriff der **Orthogonalität** erweisen.

Im Mittelpunkt unserer Betrachtungen werden im nächsten Kapitel lineare Abbildungen stehen, die besondere Forderungen an das Skalare Produkt berücksichtigen.

Unter ihnen werden sich die **selbstadjungierten**, die **normalen** und die **unitären** als besonders bedeutungsvoll erweisen.

5. 1. 3 Definition. Ein Vektorraum heißt **reell**, wenn $\mathcal{K}$ gleich $\mathcal{R}$ ist, er heißt **komplex**, wenn $\mathcal{K}$ gleich $\mathcal{C}$ ist.

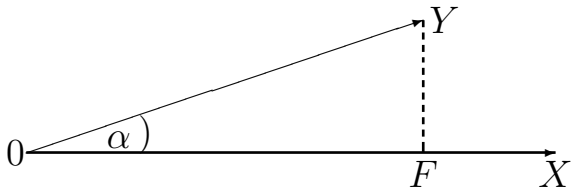
Wir erinnern erneut an die Oberstufe. Dort wurde das Skalarprodukt zweier Vektoren $[\mathfrak{x}, \mathfrak{y}]$ erklärt *via*

$$[\mathfrak{x}, \mathfrak{y}] := |\mathfrak{x}| \cdot |\mathfrak{y}| \cdot \cos(\mathfrak{x}, \mathfrak{y}) \,,$$

[1] Dieser Vorspann erscheint hier zum ersten Mal und war nicht Teil früherer Fassungen. Es ist aber wohl nicht mehr anzunehmen, dass der Zusammenhang zwischen geometrischem und algebraischem Skalarprodukt noch Teil eines jeden Leistungskurses ist.

[2] auch: inneres Produkt

in der nachfolgenden Abbildung also als $|OX| \cdot |OF|$, bzw. dual als $|OY| \cdot |OL|$, wenn man mit L den Fußpunkt des Lotes von X auf OY bezeichnet.



Schreibt man nun $[\mathfrak{x}, \mathfrak{y}]$ als $\mathfrak{x} \star y$ und ersetzt man zudem in der obigen Zeichnung $\mathfrak{x}$ durch $\mathfrak{u} + \mathfrak{v}$, so erhält man offenbar das rechtsseitige Distributiv-Gesetz $(\mathfrak{u} + \mathfrak{v}) = \mathfrak{u} \star \mathfrak{y} + \mathfrak{v} \star \mathfrak{y}$.

5. 1. 4 Definition. Sei $\mathbf{V}$ ein reeller Vektorraum und $\star$ eine Operation, die jedem Paar $\mathfrak{x}, \mathfrak{y}$ ein $\mathfrak{x} \star \mathfrak{y} \in \mathbf{R}$ zuordnet, dann heißt $\star$ ein **Skalares Produkt**, wenn gilt:

(S1) $$\mathfrak{x} \star \mathfrak{y} = \mathfrak{y} \star \mathfrak{x}$$

(S2) $$(c\,\mathfrak{x}) \star \mathfrak{y} = c\,(\mathfrak{x} \star \mathfrak{y})$$

(S3) $$(\mathfrak{x} + \mathfrak{y}) \star \mathfrak{z} = \mathfrak{x} \star \mathfrak{z} + \mathfrak{y} \star \mathfrak{z}$$

(S4) $$\mathfrak{x} \neq \mathfrak{o} \;\Rightarrow\; \mathfrak{x} \star \mathfrak{x} > 0$$

Diese vier Gesetze schließen also an den konkreten Vektorraum der Oberstufe an, wie wir oben sahen. Wegen (S1) heißt $\star$ auch symmetrisch, wegen (S4) positiv definit.

Beispiele:

1. Das für beliebige $\mathcal{K}^n$ bereits eingeführte Skalare Produkt im Falle $K = \mathbf{R}$.
2. $\mathbf{V} = \mathbf{R}^2, \quad \mathfrak{x} \star \mathfrak{y} = 4x_1y_1 - 2x_1y_2 - 2x_2y_1 + 3x_2y_2$
3. Der Raum aller steigen Funktionen $[\,a\,,\,b\,] \longmapsto \mathbf{R}$ mit

$$f \star g := \int_a^b h(t)\, f(t)\, g(t)\, dt \;\; (h(t) > 0 \;\; (a \leq t \leq b))\,.$$

5. 1. 5 Definition. Sei $\mathbf{V}$ ein reeller Vektorraum mit dem Skalaren Produkt $\star$. Dann nennen wir $(\mathbf{V}, \star)$ unter Einbeziehung von $\star$ einen **euklidischen Raum** .

Sei hiernach $\mathbf{V}$ komplex.

5. 1. 6 Definition. Ist $\mathbf{V}$ ein komplexer Vektorraum, so heißt eine Operation $\star$ ein Skalares Produkt, wenn gilt: $\mathfrak{x} \star \mathfrak{y} \in \mathbf{C}$ und

(S1') $\quad \mathfrak{x} \star \mathfrak{y} = \overline{\mathfrak{y} \star \mathfrak{x}}$

(S2') $\quad$ wie (S2)

(S3') $\quad$ wie (S3)

(S4) $\quad$ wie (S4) .

Anmerkung: Wegen $\mathfrak{x} \star \mathfrak{x} = \overline{\mathfrak{x} \star \mathfrak{x}}$ folgt, dass $\mathfrak{x} \star \mathfrak{x}$ in $\mathbf{R}$ liegt. Somit macht (S4) Sinn. Ferner haben wir aufgrund von (S1') bis (S3)

$$\begin{aligned} \mathfrak{x} \star (\mathfrak{y} + \mathfrak{z}) &= \overline{(\mathfrak{y} + \mathfrak{z}) \star \mathfrak{x}} \\ &= \overline{\mathfrak{y} \star \mathfrak{x}} + \overline{\mathfrak{z} \star \mathfrak{x}} \\ &= \mathfrak{x} \star \mathfrak{y} + \mathfrak{x} \star \mathfrak{z} \end{aligned}$$

also (auch) das linksseitige Distributivgesetz, und

$$\begin{aligned} \mathfrak{x} \star (c\,\mathfrak{y}) &= \overline{(c\,\mathfrak{y}) \star \mathfrak{x}} \\ &= \overline{c\,(\mathfrak{y} \star \mathfrak{x})} \\ &= \overline{c}\,(\mathfrak{x} \star \mathfrak{y}) \end{aligned}$$

Insbesondere ergibt sich damit

$$\begin{aligned} \mathfrak{x} \star \mathfrak{o} &= \mathfrak{x} \star (\mathfrak{y} + (-1\mathfrak{y}) \\ &= \mathfrak{x} \star \mathfrak{y} + \mathfrak{x} \star (-1\mathfrak{y}) \\ &= \mathfrak{x} \star \mathfrak{y} - \mathfrak{x} \star \mathfrak{y} = 0 \end{aligned}$$

und dual $\mathfrak{o} \star \mathfrak{x} = 0$.

Beispiele:

1. Definiere in $\mathbf{C}^n$ $\mathfrak{x} \star \mathfrak{y} := \sum x_i \overline{y_i} \quad (1 \leq i \leq n)$
2. Definiere in $\mathbf{C}^2$ $\mathfrak{x} \star \mathfrak{y} := 4x_1\overline{y_1} - 2x_1\overline{y_2} - 2x_2\overline{y_1} + 3x_2\overline{y_2}$

5. 1. 7 Definition. Sei $\mathbf{V}$ ein komplexer Vektorraum mit dem Skalaren Produkt $\star$. Dann hennen wir $(\mathbf{V}, \star)$ unter Einbeziehung von $\star$ einen **unitären Raum** .

Wir werden nun zeigen, dass sich jeder reelle Vektorraum ausdehnen lässt zu einem komplexen Vektorraum und jeder euklidische Vektorraum zu einem unitären Vektorraum.

5. 1. 8 Proposition. *Sei* $\mathbf{X}$ *ein reeller Vektorraum. Dann bildet die Menge aller Paare* $(\mathfrak{x}, \mathfrak{y})$ *bezüglich der Stellenaddition und der S-Multiplikation*

$$(a + bi)(\mathfrak{x}, \mathfrak{y}) := (a\mathfrak{x} - b\mathfrak{y} \mid a\mathfrak{y} + b\mathfrak{x})$$

einen komplexen Vektorraum $\mathbf{Z}$ *mit* $(\mathfrak{o}, \mathfrak{o})$ *als Nullvektor. Darüber hinaus ist der Raum* $\mathbf{X}$ *isomorph zu dem Unterraum aller* $(\mathfrak{x}, \mathfrak{o})$*, betrachtet bezüglich des Skalarenbereichs* $\mathbf{R}$*.*

BEWEIS. Übung. □

Identifizieren wir nun die Paare $(\mathfrak{x}, \mathfrak{o})$ mit $\mathfrak{x}$ und die Paare $(\mathfrak{o}, \mathfrak{y})$ mit $i\mathfrak{y}$ (es ist ja $i\mathfrak{y} = i(\mathfrak{y}, \mathfrak{o}) = (0, \mathfrak{y})$), so können wir die Paare $(\mathfrak{x}, \mathfrak{y})$ auch schreiben als Summe $\mathfrak{x} + i\mathfrak{y}$. Auf diese Weise gelangen wir zu einem Vektorraum $\mathbf{Z}$ von Vektoren $\mathfrak{z} = \mathfrak{x} + i\mathfrak{y}$ $(\mathfrak{x}, \mathfrak{y} \in \mathfrak{x})$ mit $(\mathbf{C}, +, \cdot)$ als zugehörigem Skalarenkörper.

5. 1. 9 Definition. Sei $\mathbf{X}$ ein reeller Vektorraum. Dann bezeichnen wir die soeben konstruierte Ausdehnung $\mathbf{Z}$ als die **komplexe Erweiterung** von $\mathbf{X}$.

Wie man sich leicht klarmacht, ist $\mathbf{Z}$ in folgendem Sinne eindeutig festgelegt:

Wäre auch $\mathbf{Z}'$ eine komplexe Erweiterung, so müssten sich die Paare $\mathfrak{x} + i\,\mathfrak{y}$ in $\mathbf{Z}'$ genau so verhalten, wie dies *per constructionem* für $\mathbf{Z}$ festgelegt wurde.

Es ist also gerechtfertigt, von *der* komplexen Erweiterung zu sprechen.

5. 1. 10 Proposition. *Sei* $\mathbf{Z}$ *komplexe Erweiterung zu* $\mathbf{X}$ *und* $\mathbf{Z}'$ *komplexe Erweiterung zu* $\mathbf{X}'$*. Dann lässt sich jede lineare Abbildung* $\phi : \mathbf{X} \longmapsto \mathbf{X}'$ *eindeutig ausdehnen zu einer linearen Abbildung* $\hat{\phi} : \mathbf{Z} \longmapsto \mathbf{Z}'$ *.*

BEWEIS. Setze: $\hat{\phi}\,(\mathfrak{x} + i\mathfrak{y}) := \phi\,(\mathfrak{x}) + i\phi\,(\mathfrak{y})$. □

5. 1. 11 Proposition. *Sei* $\mathbf{X}$ *ein euklidischer Raum und* $\mathbf{Z}$ *eine komplexe Erweiterung. Dann lässt sich das Skalare Produkt* $\star$ *von* $\mathbf{X}$ *eindeutig ausdehnen auf* $\mathbf{Z}$.

DENN: man setze:

$$(\mathfrak{x} + i\mathfrak{y}) \star_z (\mathfrak{u} + i\mathfrak{v}) = (\mathfrak{x} \star \mathfrak{u} - \mathfrak{y} \star \mathfrak{v}) + i(\mathfrak{y} \star \mathfrak{u} + \mathfrak{x} \star \mathfrak{v})\,. \qquad \square$$

5.2 Betrag – Linearität – Orthogonalität

Sei im folgenden $\mathbf{Z}$ stets ein euklidischer oder unitärer Vektorraum.

5. 2. 1 Definition. Sei $\mathfrak{x}$ aus $\mathbf{Z}$. Dann bezeichnen wir die reelle Zahl $\sqrt{\mathfrak{x} \star \mathfrak{x}} =: |\,\mathfrak{x}\,|$ als den **Betrag** bzw. als die **Länge** von $\mathfrak{x}$.

Es ist also *per definitionem* stets $|\,\mathfrak{x}\,|^2 = \mathfrak{x} \star \mathfrak{x}$ erfüllt. Als eine erste zentrale Regel erhalten wir: für Betrag und Skalarprodukt:

5. 2. 2 Die Schwarz**sche Ungleichung.**

(SU) $$|\,\mathfrak{x} \star \mathfrak{y}\,| \;\leq\; |\,\mathfrak{x}\,| \cdot |\,\mathfrak{y}\,|$$

BEWEIS. Ist $\mathfrak{x} = \mathfrak{o}$ oder $\mathfrak{y} = \mathfrak{o}$, so ist nichts zu zeigen. Sei deshalb $\mathfrak{y} \neq \mathfrak{o}$ und damit $\mathfrak{y} \star \mathfrak{y} > 0$. Dann folgt zunächst für jedes $c \in \mathbf{C}$

$$\begin{aligned} 0 \;&\leq\; (\mathfrak{x} - c\mathfrak{y}) \star (\mathfrak{x} - c\mathfrak{y}) \\ &=\; \mathfrak{x} \star \mathfrak{x} - \overline{c}(\mathfrak{x} \star \mathfrak{y}) - c\,(\mathfrak{y} \star \mathfrak{x}) + (c\,\overline{c})(\mathfrak{y} \star \mathfrak{y}) \\ &=\; \mathfrak{x} \star \mathfrak{x} - \overline{c}(\mathfrak{x} \star \mathfrak{y}) - c\,\overline{(\mathfrak{x} \star \mathfrak{y})} + (c\,\overline{c})(\mathfrak{y} \star \mathfrak{y}). \end{aligned}$$

Wählen wir nun c als $(\mathfrak{x} \star \mathfrak{y}) : (\mathfrak{y} \star \mathfrak{y})$, so folgt weiter:

$$0 \;\leq\; \mathfrak{x} \star \mathfrak{x} - \frac{\mathfrak{x} \star \mathfrak{y}}{\mathfrak{y} \star \mathfrak{y}}\,\overline{(\mathfrak{x} \star \mathfrak{y})},$$

also nach Multiplikation mit $\mathfrak{y} \star \mathfrak{y}$

$$0 \;\leq\; (\mathfrak{x} \star \mathfrak{x})(\mathfrak{y} \star \mathfrak{y}) - (\mathfrak{x} \star \mathfrak{y})\overline{(\mathfrak{x} \star \mathfrak{y})}.$$

Das liefert dann wegen

$$(\mathfrak{x} \star \mathfrak{y}) \cdot \overline{(\mathfrak{x} \star \mathfrak{y})} \;=\; |\,\mathfrak{x} \star \mathfrak{y}\,|^2$$

die obige Behauptung. □

Hiernach können wir weiter beweisen:

5. 2. 3 Vier Regeln zum Betrag.

(B1) $$|\,\mathfrak{x}\,| \;\geq\; 0$$

(B2) $$|\,\mathfrak{x}\,| = 0 \;\Leftrightarrow\; \mathfrak{x} = \mathfrak{o}$$

(B3) $$|\,c\mathfrak{x}\,| \;=\; |\,c\,|\,|\,\mathfrak{x}\,|$$

(B4) $$|\,\mathfrak{x} + \mathfrak{y}\,| \;\leq\; |\,\mathfrak{x}\,| + |\,\mathfrak{y}\,|$$

BEWEIS. (B1) und (B2) sind klar und (B3) folgt vermöge:

$$\begin{aligned} |\,c\mathfrak{x}\,| &= \sqrt{c\mathfrak{x} \star c\mathfrak{x}} \\ &= \sqrt{(c\,\overline{c})\,(\mathfrak{x} \star \mathfrak{x})} \\ &= \sqrt{(c\,\overline{c})}\,\sqrt{\mathfrak{x} \star \mathfrak{x}} \\ &= |\,c\,|\,|\,\mathfrak{x}\,|. \end{aligned}$$

Schließlich gilt:

$$\begin{aligned} |\,\mathfrak{x} + \mathfrak{y}\,|^2 &= (\mathfrak{x} + \mathfrak{y}) \star (\mathfrak{x} + \mathfrak{y}) \\ &= \mathfrak{x} \star \mathfrak{x} + \mathfrak{x} \star \mathfrak{y} + \mathfrak{y} \star \mathfrak{x} + \mathfrak{y} \star \mathfrak{y} \\ &= |\,\mathfrak{x}\,|^2 + |\,\mathfrak{y}\,|^2 + 2\mathrm{Re}\,(\mathfrak{x} \star \mathfrak{y})\,. \end{aligned}$$

Nun ist aber $\mathrm{Re}\,(c) \leq |\,c\,|$, und es folgt aus der SCHWARZschen Ungleichung $|\,\mathfrak{x} \star \mathfrak{y}\,| \leq |\,\mathfrak{x}\,|\,|\,\mathfrak{y}\,|$. Daher ergibt sich weiter:

$$\begin{aligned} |\,\mathfrak{x} + \mathfrak{y}\,|^2 &\leq |\,\mathfrak{x}\,|^2 + 2|\,\mathfrak{x}\,|\,|\,\mathfrak{y}\,| + |\,\mathfrak{y}\,|^2 \\ &= (|\,\mathfrak{x}\,| + |\,\mathfrak{y}\,|)^2, \end{aligned}$$

und somit (B4). □

Die Regel (B4) des letzten Satzes bezeichnet man üblicherweise als **Dreiecksungleichung** . Als Folgerung dieser Dreiecksungleichung erhalten wir

$$||\,\mathfrak{x}\,| - |\,\mathfrak{y}\,|| \;\leq\; |\,\mathfrak{x} - \mathfrak{y}\,|,$$

denn

$$\begin{array}{rcl} |\,\mathfrak{x}-\mathfrak{y}+\mathfrak{y}\,| & \leq & |\,\mathfrak{x}-\mathfrak{y}\,|+|\,\mathfrak{y}\,| \\ & \rightsquigarrow & \\ |\,\mathfrak{x}\,|-|\,\mathfrak{y}\,| & \leq & |\,\mathfrak{x}-\mathfrak{y}\,| \\ \&\ |\,\mathfrak{y}\,|-|\,\mathfrak{x}\,| & \leq & |\,\mathfrak{x}-\mathfrak{y}\,| \\ & \rightsquigarrow & \\ ||\,\mathfrak{x}\,|-|\,\mathfrak{y}\,|| & \leq & |\,\mathfrak{x}-\mathfrak{y}\,|. \end{array}$$

In der Längensymbolik gelten die beiden Abschätzungen:

$$\begin{array}{rcl} |\,\mathfrak{x}\star\mathfrak{y}\,| & \leq & |\,\mathfrak{x}\,|\cdot|\,\mathfrak{y}\,| \\ \text{und} \qquad |\,\mathfrak{x}+\mathfrak{y}\,| & \leq & |\,\mathfrak{x}\,|+|\,\mathfrak{y}\,|. \end{array}$$

Wir fragen, wann in diesen beiden Abschätzungen Gleichheit gilt.

5. 2. 4 Proposition. *Es gilt:*

$$|\,\mathfrak{x}\star\mathfrak{y}\,|=|\,\mathfrak{x}\,|\cdot|\,\mathfrak{y}\,| \iff \{\mathfrak{x}\,,\,\mathfrak{y}\}\ell a\,.$$

BEWEIS. Die Entwicklung im Beweis zu 5.2.2 gilt auch rückläufig, also folgt aus $|\,\mathfrak{x}\star\mathfrak{y}\,|=|\,\mathfrak{x}\,||\,\mathfrak{y}\,|$ die lineare Abhängigkeit von $\{\mathfrak{x},\mathfrak{y}\}$.

Gilt umgekehrt etwa $\mathfrak{x}=c\mathfrak{y}$, so haben wir

$$\begin{array}{rcl} |\,\mathfrak{x}\star\mathfrak{y}\,| & = & |\,c\mathfrak{y}\star\mathfrak{y}\,| \\ & = & |\,c\cdot(\mathfrak{y}\star\mathfrak{y})\,| \\ & = & |\,c\,|\cdot|\,\mathfrak{y}\star\mathfrak{y}\,| \\ & = & |\,c\,|\cdot(|\,\mathfrak{y}\,|\cdot|\,\mathfrak{y}\,|) \\ & = & |\,c\,\mathfrak{y}\,|\cdot|\,\mathfrak{y}\,| \\ & = & |\,\mathfrak{x}\,|\cdot|\,\mathfrak{y}\,|\,. \end{array}$$

□

5. 2. 5 Proposition. *Genau dann gilt* $|\,\mathfrak{x}+\mathfrak{y}\,|=|\,\mathfrak{x}\,|+|\,\mathfrak{y}\,|$, *wenn* $\mathfrak{y}=\mathfrak{o}$ *oder aber* $\mathfrak{x}=c\mathfrak{y}$ *mit* $c\in\mathbf{R}^{\geq\mathbf{0}}$ *ist.*

BEWEIS. Aus dem Beweis der Summenformel folgt unmittelbar, dass in ihr das Gleichheitszeichen genau dann gilt, wenn $\mathrm{Re}\,(\mathfrak{x}\star\mathfrak{y})=|\,\mathfrak{x}\,||\,\mathfrak{y}\,|$ erfüllt ist, also wegen $\mathrm{Re}\,(\mathfrak{x}\star\mathfrak{y})\leq|\,\mathfrak{x}\star\mathfrak{y}\,|\leq|\,\mathfrak{x}\,||\,\mathfrak{y}\,|$, wenn

$$\mathrm{Re}\,(\mathfrak{x}\star\mathfrak{y}) \;=\; |\,\mathfrak{x}\star\mathfrak{y}\,|=|\,x\,||\,\mathfrak{y}\,|$$

erfüllt ist. Das liefert aber

$$|\,\mathfrak{x}\star\mathfrak{y}\,| \;=\; |\,\mathfrak{x}\,|\cdot|\,\mathfrak{y}\,| \rightsquigarrow (\mathfrak{x},\mathfrak{y})\;\ell a\;\;.$$

Setzen wir nun noch zusätzlich $\mathfrak{y}\neq\mathfrak{o}$ voraus, so folgt $\mathfrak{x}=c\mathfrak{y}$ und

$$\begin{aligned}\mathrm{Re}\,(c)\,|\,\mathfrak{y}\,|^2 &= \mathrm{Re}\,(c)(\mathfrak{y}\star\mathfrak{y})\\ &= \mathrm{Re}\,(c\mathfrak{y}\star\mathfrak{y})\\ &= \mathrm{Re}\,(\mathfrak{x}\star\mathfrak{y})\\ &= |\,\mathfrak{x}\,|\,|\mathfrak{y}\,|\\ &= |c|\,|\,\mathfrak{y}\,|^2\end{aligned}$$

und damit $\mathrm{Re}\,(c)=|\,c\,|$, also $c\in\mathbf{R}^{\geq\mathbf{0}}$.
Sei hiernach $\mathfrak{x}=c\mathfrak{y}$ mit $c\in\mathbf{R}^{\geq\mathbf{0}}$. Dann liefert Einsetzen

$$\begin{aligned}\mathrm{Re}\,(\mathfrak{x}\star\mathfrak{y}) &= \mathrm{Re}\;(\,c(\mathfrak{y}\star\mathfrak{y})\,)\\ &= c\,(\mathfrak{y}\star\mathfrak{y})\\ &= |\,c\mathfrak{y}\,|\,|\,\mathfrak{y}\,|\\ &= |\,\mathfrak{x}\,|\,|\,\mathfrak{y}\,|,\end{aligned}$$

also $|\,\mathfrak{x}+\mathfrak{y}\,|=|\,\mathfrak{x}\,|+|\,\mathfrak{y}\,|$. □

Nach der Einführung eines **Längenmaßes** führen wir nun ein **Winkelmaß** ein.

5. 2. 6 Definition. Sind $\mathfrak{x}$ und $\mathfrak{y}$ verschieden von $\mathfrak{o}$, so definieren wir als $\cos(\mathfrak{x},\mathfrak{y})$ die Größe

$$\cos(\mathfrak{x},\mathfrak{y}) \;:=\; \frac{\mathfrak{x}\star\mathfrak{y}}{|\,\mathfrak{x}\,|\,|\,\mathfrak{y}\,|}\qquad(*)$$

Wegen $|\,\mathfrak{x}\star\mathfrak{y}\,|\leq|\,\mathfrak{x}\,|\,|\,\mathfrak{y}\,|$ gilt im Falle eines euklidischen Raumes offenbar, man beachte $(*)$,

$$\begin{aligned}-1 &\leq \cos(\mathfrak{x},\mathfrak{y})\leq+1.\\ \text{und}\qquad \mathfrak{x}\star\mathfrak{y} &= |\,\mathfrak{x}\,|\,|\,\mathfrak{y}\,|\cos(\mathfrak{x},\mathfrak{y})\,,\end{aligned}$$

und hieraus folgt weiter

5. 2. 7 Der Kosinussatz. *Sind $\mathfrak{x},\mathfrak{y}$ beliebig $\neq\mathfrak{o}$ und ist $\mathbf{X}$ euklidisch, so gilt*

$$|\,\mathfrak{x}-\mathfrak{y}\,|^2=|\,\mathfrak{x}\,|^2+|\,\mathfrak{y}\,|^2-2|\,\mathfrak{x}\,|\,|\,\mathfrak{y}\,|\cos(\mathfrak{x},\mathfrak{y})$$

DENN: Beachte erneut $\mathfrak{z}^2 = |\,\mathfrak{z}\,|^2$. □

Offenbar besagt der Kosinussatz im Sonderfall der euklidischen Geometrie:

Im einem jeden Dreieck ist das Quadrat über c gleich der Summe der Quadrate über a und b, vermindert um $2\,|\,a\,||\,b\,|\cos\gamma$.

Damit ist im Falle eines rechtwinkligen Dreiecks ($\gamma = \frac{\pi}{2}$) der Kosinussatz gleichbedeutend mit dem **Satz des Pythagoras**. . Insbesondere entspricht $\gamma = \frac{\pi}{2}$ dem Fall $\cos(\mathfrak{a}, \mathfrak{b}) = 0$.

5. 2. 8 Definition. Sei **Z** wie vereinbart euklidisch oder unitär. Dann nennen wir $\mathfrak{x} \in Z$ **normiert** , wenn $\mathfrak{x}$ die Länge 1 hat.

Offenbar sind alle $\dfrac{1}{|\,\mathfrak{x}\,|}\mathfrak{x}$ normiert.

5. 2. 9 Definition. Sei **Z** wie vereinbart euklidisch oder unitär. Dann nennen wir $\mathfrak{x}$ und $\mathfrak{y}$ **zueinander orthogonal** , wenn die Gleichung $\mathfrak{x} \star \mathfrak{y} = 0$ erfüllt ist.

Sind $\mathfrak{x}$ und $\mathfrak{y}$ orthogonal, so sagen wir auch, es sei $\mathfrak{x}$ orthogonal zu $\mathfrak{y}$, bzw. $\mathfrak{y}$ orthogonal zu $\mathfrak{x}$ und schreiben in diesem Falle $\mathfrak{x} \perp \mathfrak{y}$. (Beachte: $\mathfrak{x} \star \mathfrak{y} = 0 \Longrightarrow \mathfrak{y} \star \mathfrak{x} = 0$.)

5. 2. 10 Definition. $\mathfrak{M} \subseteq \mathfrak{Z}$ heißt ein **Orthogonalsystem** , wenn $\mathfrak{M}$ den Nullvektor nicht enthält und wenn je zwei verschiedene Vektoren aus $\mathfrak{M}$ zueinander orthogonal sind.

$\mathfrak{M} \subseteq \mathfrak{Z}$ heißt ein **Orthonormalsystem** , wenn $\mathfrak{M}$ ein Orthogonalsystem von lauter Vektoren der Länge 1 ist.

Ein Orthonormalsystem $\mathfrak{M}$ heißt eine **Orthonormalbasis,** kurz (ONB), wenn $\mathfrak{M}$ eine Basis ist.

5. 2. 11 Proposition. *Jedes Orthogonalsystem* $\mathfrak{M}$ *aus* $\mathfrak{Z}$ *ist* ℓu.

BEWEIS. Seien $\mathfrak{x}_1, \ldots, \mathfrak{x}_n$ aus $\mathfrak{M}$ und sei

$$s_1\,\mathfrak{x}_1 + s_2\,\mathfrak{x}_2 + \ldots + s_n\,\mathfrak{x}_n = \mathfrak{o}.$$

Dann folgt $s_i\,(\mathfrak{x}_i \star \mathfrak{x}_i) = 0 \rightsquigarrow s_i = 0 \;\; (1 \leq i \leq n)$. □

5. 2. 12 Proposition. *Sei* $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ *eine* ONB *zu* **Z** . *Gilt dann*

$$\begin{aligned} \mathfrak{x} &= x_1\,\mathfrak{e}_1 + x_2\,\mathfrak{e}_2 + \ldots + x_n\,\mathfrak{e}_n \\ \&\;\; \mathfrak{y} &= y_1\,\mathfrak{e}_1 + y_2\,\mathfrak{e}_2 + \ldots + y_n\,\mathfrak{e}_n, \end{aligned}$$

so folgt, man beachte $x_i\mathfrak{e}_i \star y_j\mathfrak{e}_j = \overline{y}_j(x_i(\mathfrak{e}_i \star \mathfrak{e}_j)) = (x_i\overline{y}_j)(\mathfrak{e}_i \star \mathfrak{e}_j)$ *:*

$$\begin{aligned} \mathfrak{x} \star \mathfrak{y} &= x_1\,\overline{y}_1 + \ldots + x_n\,\overline{y}_n \\ \mathfrak{x} \star \mathfrak{e}_i &= x_i \quad (1 \le i \le n). \end{aligned}$$

Ist andererseits $\mathfrak{B}$ *irgendeine Basis zu* $\mathbf{X}$ *, so liefert die Festsetzung:*

$$\mathfrak{b}_i \star \mathfrak{b}_j := 0 \ \ (i \neq j),\ \mathfrak{b}_i \star \mathfrak{b}_i := 1$$

ein Skalarprodukt mit $(\mathfrak{b}_1, \ldots, \mathfrak{b}_n)$ *als* ONB.

BEWEIS. Übung. □

Nach dem letzten Satz ist ein Skalarprodukt fixiert, sobald es festgelegt ist für irgendeine Basis, ja, es liefert jede Basis ein eindeutig bestimmtes Skalarprodukt derart, dass sie (selbst) zur ONB wird.

Dass auch umgekehrt jedes Skalarprodukt (im höchstens abzählbar unendlichen Fall) eine ONB liefert, ist ein Nebenergebnis des nun folgenden Theorems.

5. 2. 13 Ein Satz von Erhard Schmidt. *Sei* $\mathbf{Z}$ *ein euklidischer oder unitärer Vektorraum von höchstens abzählbarer Dimension. Dann existiert zu jedem ℓu System von Vektoren* $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ *genau ein* ONS $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ *mit*

$$(i) \qquad [\,\mathfrak{a}_1, \ldots, \mathfrak{a}_k\,] = [\,\mathfrak{e}_1, \ldots, \mathfrak{e}_k\,] \quad (1 \le k \le n)$$

$$(ii) \qquad |\,\mathfrak{a}_i \to \mathfrak{e}_i\,|_1^n = \det(\,\mathfrak{a}_i \to \mathfrak{e}_i\,) \ \ (1 \le i \le n) > 0.$$

BEWEIS. Sei zunächst ein einzelner Vektor $\mathfrak{a}_1 \neq \mathfrak{o}$ gegeben. Dann gilt

$$\begin{aligned} &(i) \quad \mathfrak{e}_1 := \tfrac{\mathfrak{a}_1}{|\,\mathfrak{a}_1\,|} \quad \rightsquigarrow \quad |\,\mathfrak{e}_1\,| = 1 \\ &(ii) \quad \mathfrak{e}_1 = c_1\mathfrak{a}_1 \ \text{ mit } \ c_1 = \tfrac{1}{|\,\mathfrak{a}_1\,|} > 0\,, \end{aligned}$$

und ist $\mathfrak{e}_1{}'$, c_1' ein weiteres Paar im Sinne des Satzes, so folgt:

$$\begin{aligned} c_1'\mathfrak{a}_1 \star c_1'\mathfrak{a}_1 &= \mathfrak{e}_1{}' \star \mathfrak{e}_1{}' \\ &= \mathfrak{e}_1 \star \mathfrak{e}_1 \\ &= c_1\mathfrak{a}_1 \star c_1\mathfrak{a}_1 \\ \rightsquigarrow \qquad c_1'\overline{c_1'} &= c_1\overline{c_1} \\ \rightsquigarrow \qquad |\,c_1'\,|^2 &= |\,c_1\,|^2 \\ \rightsquigarrow \qquad c_1' &= c_1\,, \end{aligned}$$

also $c_1 = c_1'$ und damit auch $\mathfrak{e}_1{}' = \mathfrak{e}_1$.

Somit gilt die Behauptung des Satzes für $n = 1$.

Sei hiernach im Sinne des Satzes

$$[\,\mathfrak{a}_1, \ldots, \mathfrak{a}_n\,] \;=\; [\,\mathfrak{e}_1, \ldots, \mathfrak{e}_n\,]$$

$$\text{mit} \quad |\,\mathfrak{a}_i \to \mathfrak{e}_i\,|_1^n \;>\; 0.$$

Ist dann $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n, \mathfrak{a}_{n+1})$ ℓu, so folgt zunächst

$$[\,\mathfrak{a}_1, \ldots, \mathfrak{a}_n, \mathfrak{a}_{n+1}\,] \;=\; [\,\mathfrak{e}_1, \ldots, \mathfrak{e}_n, \mathfrak{a}_{n+1}\,]$$

mit linear unabhängigem $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n, \mathfrak{a}_{n+1})$.

Wir betrachten

$$\mathfrak{c} \;:=\; \mathfrak{a}_{n+1} - \sum_1^n (\mathfrak{a}_{n+1} \star \mathfrak{e}_i)\mathfrak{e}_i.$$

Dann gilt $\mathfrak{c} \perp \mathfrak{e}_i$ $(1 \le i \le n)$, und es liefert Division durch $|\,\mathfrak{c}\,|$ einen normierten Vektor $\mathfrak{e}_{n+1}$ mit dieser Eigenschaft. Setzen wir nun noch $\frac{1}{|\,\mathfrak{c}\,|} = c_{n+1}$, so erhalten wir weiter

$$\mathfrak{e}_{n+1} \;=\; -c_{n+1} \sum_1^n (\mathfrak{a}_{n+1} \star \mathfrak{e}_i)\mathfrak{e}_i + c_{n+1}\mathfrak{a}_{n+1}$$

mit $|\,\mathfrak{e}_{n+1}\,| = 1$ und $\mathfrak{e}_{n+1} \perp \mathfrak{e}_i$ $(1 \le i \le n)$, und es gilt aufgrund unserer Voraussetzung

$$|\,\mathfrak{a}_i \to \mathfrak{e}_i\,|_1^{n+1} \;=\; |\mathfrak{a}_i \to \mathfrak{e}_i\,|_1^n \cdot c_{n+1} > 0\,,$$

man entwickle nach der letzten Zeile, sie hat ja nach Konstruktion die Form

$$(0, 0, \ldots, 0, c_{n+1})\ .$$

Zu zeigen bleibt die Eindeutigkeit von $\mathfrak{e}_{n+1}$. Sei hierzu ein zweites $\mathfrak{e}_{n+1}{}'$ mit den gestellten Bedingungen angenommen. Dann erhalten wir für geeignete Elemente c, d :

$$\begin{aligned} \mathfrak{a}_{n+1} \;&=\; \sum_1^n (\mathfrak{a}_{n+1} \star \mathfrak{e}_i)\mathfrak{e}_i + c\,\mathfrak{e}_{n+1} \\ &=\; \sum_1^n a_i\mathfrak{e}_i \qquad\qquad\quad + d\,\mathfrak{e}'_{n+1} \end{aligned}$$

und damit nach Subtraktion etwa

$$\sum_1^n b_i \mathfrak{e}_i + (c\,\mathfrak{e}_{n+1} - d\,\mathfrak{e}'_{n+1}) = \mathfrak{o}.$$

Dabei sind die beiden Summanden aber orthogonal, weshalb sie beide gleich $\mathfrak{o}$ sein müssen – beachte die Implikation

$$\mathfrak{a} \star \mathfrak{b} = 0 \;\;\&\;\; \mathfrak{a} + \mathfrak{b} = \mathfrak{o} \Longrightarrow \mathfrak{b}^2 = \mathfrak{o}\ .$$

Somit haben wir

$$\begin{array}{rcl} c\,\mathfrak{e}_{n+1} = d\,\mathfrak{e}'_{n+1} & \rightsquigarrow & (c\,\mathfrak{e}_{n+1}) \star (c\,\mathfrak{e}_{n+1}) \\ & = & (d\,\mathfrak{e}_{n+1}) \star (d\,\mathfrak{e}'_{n+1}) \\ & \rightsquigarrow & c\,\overline{c} = d\overline{d} \\ & \rightsquigarrow & c^2 = d^2 \\ & \rightsquigarrow & c = d\,, \end{array}$$

also $c = d$ und damit auch $\mathfrak{e}_{n+1} = \mathfrak{e}'_{n+1}$. □

5.3 Die orthogonale Projektion

Im folgenden sei $\mathfrak{A} \perp \mathfrak{B}$ definiert vermöge $\mathfrak{a} \perp \mathfrak{b}$ $(\forall \mathfrak{a} \in \mathfrak{A},\, \mathfrak{b} \in \mathfrak{B})$ – wie üblich. Dann folgt unmittelbar $\mathfrak{A} \perp \mathfrak{B} \Longrightarrow [\,\mathfrak{A}\,] \perp [\,\mathfrak{B}\,]$.

5. 3. 1 Definition. Ist $\mathfrak{A}$ eine Teilmenge von $\mathfrak{x}$, so bezeichnen wir die Menge $\{\mathfrak{x} \,|\, \mathfrak{x} \perp \mathfrak{A}\}$ mit $\mathfrak{A}^\perp$ und bezeichnen $\mathfrak{A}^\perp$ das **Orthokomplement** zu $\mathfrak{A}$.

Hiermit folgt – wiederum – unmittelbar:

5. 3. 2 Proposition. *$\mathfrak{A}^\perp$ ist abgeschlossen in* **X***, und es gilt* $\mathfrak{A}^\perp = [\,\mathfrak{A}\,]^\perp$.

Als nächstes erklären wir den zentralen Begriff dieses Abschnitts:

5. 3. 3 Definition. Sei **X** ein beliebiger euklidischer oder unitärer Vektorraum, sei $\mathfrak{x}$ beliebig aus $\mathfrak{X}$ und **U** ein beliebiger Unterraum. Gilt dann $\mathfrak{x} = \mathfrak{u} + \mathfrak{v}$ mit $\mathfrak{u} \in \mathfrak{U}$ & $\mathfrak{v} = \mathfrak{x} - \mathfrak{u} \in \mathfrak{U}^\perp$, so nennt man $\mathfrak{u}$ **orthogonale Projektion zu $\mathfrak{x}$ in U**.

Eine orthogonale Projektion zu $\mathfrak{x}$ in $\mathbf{U}$ muss nicht notwendig existieren, es gilt aber:

5. 3. 4 Proposition. *Zu jedem $\mathfrak{x}$ aus $\mathbf{X}$ existiert höchstens eine orthogonale Projektion in $\mathbf{U}$.*

DENN: Aus $\mathfrak{x} = \mathfrak{u} + \mathfrak{v} = \mathfrak{u}' + \mathfrak{v}'$ mit $\mathfrak{u}, \mathfrak{u}' \in \mathfrak{U}$, $\mathfrak{v}, \mathfrak{v}' \in \mathfrak{U}^\perp$ resultiert:

$$\begin{aligned} \mathfrak{u} - \mathfrak{u}' \in \mathfrak{U} &\rightsquigarrow \mathfrak{v}' - \mathfrak{v} \in \mathfrak{U} \cap \mathfrak{U}^\perp \\ &\rightsquigarrow (\mathfrak{v}' - \mathfrak{v})^2 = 0 \\ &\rightsquigarrow \mathfrak{v}' - \mathfrak{v} = \mathfrak{o} \\ &\rightsquigarrow \mathfrak{v}' = \mathfrak{v} \ \ \& \ \ \mathfrak{u} = \mathfrak{u}'. \end{aligned}$$

□

Nachdem wir soeben gesehen haben, dass es höchstens eine orthogonale Projektion zu $\mathfrak{x}$ in $\mathbf{U}$ gibt, zeigen wir nun, dass es im Sonderfall endlicher Dimension stets mindestens eine orthogonale Projektion gibt.

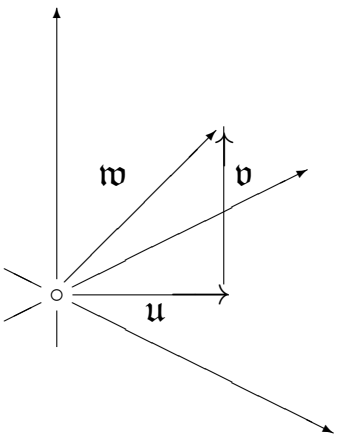
5. 3. 5 Proposition. *Ist $\mathbf{X}$ beliebig, wie oben, und $\mathbf{U}$ ein endlich-dimensionaler Unterraum von $\mathbf{X}$, so existiert zu jedem $\mathfrak{x} \in \mathfrak{X}$ mindestens eine und damit die orthogonale Projektion in $\mathbf{U}$, im weiteren bezeichnet mit $\mathfrak{x}_u$.*

BEWEIS. Sei $(\,\mathfrak{e}_1, \ldots, \mathfrak{e}_u\,)$ eine ONB zu $\mathbf{U}$ und $(\,\mathfrak{e}_1, \ldots, \mathfrak{e}_u\,, \mathfrak{e}_{u+1}\,)$ eine ONB zu $[\,\mathfrak{e}_1, \ldots, \mathfrak{e}_u\,, \mathfrak{x}\,]$. Dann ist

$$\mathfrak{x} = (x_1\mathfrak{e}_1 + \cdots + x_u\mathfrak{e}_u) + (x_{u+1}\mathfrak{e}_{u+1}) = \mathfrak{u} + x_{u+1}\mathfrak{e}_{u+1} = \mathfrak{u} + \mathfrak{v}$$

mit $\mathfrak{u} = \mathfrak{x}_u \in \mathfrak{U}$ & $\mathfrak{v} \in \mathfrak{U}^\perp$. □

Zur Erläuterung geben wir eine geometrische Interpretation im $\mathbf{R^3}$:



$\mathfrak{u}$ ist orthogonale Projektion zu $\mathfrak{w}$ in der x, y-Ebene genau dann, wenn

$$|\,\mathfrak{w} - \mathfrak{u}\,| \leq |\,\mathfrak{w} - \mathfrak{a}\,| \ (\forall \mathfrak{a}\ \text{„der } x, y\text{-Ebene”}).$$

Dieser Sachverhalt erweist sich als symptomatisch, wie der nächste Satz zeigen wird:

5. 3. 6 Proposition. *Sei $\mathbf{X}$ beliebig, wie oben, $\mathbf{U}$ ein beliebiger Unterraum*

zu $\mathbf{X}$ *und* $\mathfrak{u}$ *aus* $\mathbf{U}$ *. Dann sind die Aussagen äquivalent:*

(i) $\mathfrak{u}$ *ist orthogonale Projektion zu* $\mathfrak{x}$ *in* $\mathbf{U}$.

(ii) $|\,\mathfrak{x}-\mathfrak{u}\,| \leq |\,\mathfrak{x}-\mathfrak{a}\,| \quad (\forall \mathfrak{a} \in \mathfrak{U})$.

BEWEIS. $(i) \Longrightarrow (ii)$. Sei $\mathfrak{u} = \mathfrak{x}_u$. Dann ist $\mathfrak{x} = \mathfrak{u} + \mathfrak{v}$ mit $\mathfrak{u} \in \mathfrak{U}$, $\mathfrak{v} \in \mathfrak{U}^\perp$, also $\mathfrak{x} - \mathfrak{u} \perp \mathfrak{U}$. Sei hiernach $\mathfrak{a}$ aus $\mathfrak{U}$. Wir setzen

$$\mathfrak{x} - \mathfrak{a} \;=\; (\mathfrak{x} - \mathfrak{u}) + \mathfrak{w}\,.$$

Das liefert uns $\mathfrak{x} - \mathfrak{u} \perp \mathfrak{u} - \mathfrak{a} = \mathfrak{w} \in \mathfrak{U}$ und damit

$$\begin{aligned} |\,\mathfrak{x}-\mathfrak{a}\,|^{\,2} &= ((\mathfrak{x}-\mathfrak{u}) + \mathfrak{w})^2 \\ &= |\,\mathfrak{x}-\mathfrak{u}\,|^{\,2} + |\,\mathfrak{w}\,|^{\,2} \\ &\geq |\,\mathfrak{x}-\mathfrak{u}\,|^{\,2}. \end{aligned}$$

$(ii) \Longrightarrow (i)$. Zu beweisen ist $\mathfrak{x} - \mathfrak{u} \perp \mathfrak{U}$. Hierzu sei $\mathfrak{y}$ aus $\mathfrak{U}$ mit

$$(\mathfrak{x} - \mathfrak{u}) \star \mathfrak{y} = c \neq 0 \text{ und o. B. d. A. } |\,\mathfrak{y}\,| = 1\,.$$

Dann liegt $\mathfrak{a} := \mathfrak{u} + c\mathfrak{y}$ in $\mathfrak{U}$, und es folgt:

$$\begin{aligned} |\,\mathfrak{x}-\mathfrak{a}\,|^{\,2} &= ((\mathfrak{x}-\mathfrak{u}) - c\mathfrak{y})^2 \\ &= |\,\mathfrak{x}-\mathfrak{u}\,|^{\,2} + |\,c\,|^{\,2} - 2\mathrm{Re}\,(c \cdot (\,(\mathfrak{x}-\mathfrak{u}) \star \mathfrak{y})\,) \\ &= |\,\mathfrak{x}-\mathfrak{u}\,|^{\,2} + |\,c\,|^{\,2} - 2\,|\,c\,|^{\,2} \\ &< |\,\mathfrak{x}-\mathfrak{u}\,|^{\,2}. \end{aligned}$$

Damit sind wir am Ziel! □

5. 3. 7 Proposition. *Sei* $\mathbf{U}$ *ein endlich-dimensionaler Unterraum von* $\mathbf{X}$. *Dann gilt* $\mathbf{U} = \mathbf{U}^{\perp\perp} := (\mathbf{U}^\perp)^\perp$.

BEWEIS. Es ist stets $\mathfrak{U} \subseteq \mathfrak{U}^{\perp\perp}$. Da $\mathbf{U}$ von endlicher Dimension ist, existiert weiter zu jedem $\mathfrak{x}$ die orthogonale Projektion in $\mathbf{U}$. Daher können wir schließen:

Liegt $\mathfrak{x}$ in $\mathfrak{U}^{\perp\perp}$ und ist $\mathfrak{x}_u$ die orthogonale Projektion zu $\mathfrak{x}$ in $\mathfrak{U}$, also $\mathfrak{x} - \mathfrak{x}_u \in \mathfrak{U}^\perp$, so folgt:

$$\begin{aligned} (\mathfrak{x} - \mathfrak{x}_u) \star \mathfrak{x} &= 0 \quad (\text{ wegen } \mathfrak{x} \in \mathfrak{U}^{\perp\perp}\,) \\ \&\quad (\mathfrak{x} - \mathfrak{x}_u) \star \mathfrak{x}_u &= 0 \quad (\text{ wegen } \mathfrak{x} - \mathfrak{x}_u \in \mathfrak{U}^\perp\,). \end{aligned}$$

Das führt dann zu

$$(\mathfrak{x} - \mathfrak{x}_u) \star (\mathfrak{x} - \mathfrak{x}_u) \;=\; 0,$$

also zu $\mathfrak{x} - \mathfrak{x}_u = \mathfrak{o} \rightsquigarrow \mathfrak{x} = \mathfrak{x}_u \in \mathfrak{U}$, was $\mathfrak{U}^{\perp\perp} \subseteq \mathfrak{U}$ bedeutet. □

Schließlich beweisen wir die für den nächsten Abschnitt wichtigen Sätze:

5. 3. 8 Proposition. *Sei* $\mathbf{X}$ *endlich-dimensional und* $\mathbf{U}$ *ein Unterraum von* $\mathbf{X}$*. Dann gilt:*

$$\dim \mathbf{U} + \dim \mathbf{U}^{\perp} = \dim \mathbf{X} \rightsquigarrow \mathbf{U} \oplus \mathbf{U}^{\perp} = \mathbf{X}.$$

BEWEIS. Sei $(\,\mathfrak{e}_1, \ldots, \mathfrak{e}_u\,,\, \mathfrak{e}_{u+1}, \ldots, \mathfrak{e}_n\,)$ ONB zu $\mathbf{X}$ mit der Eigenschaft $\mathfrak{U} = [\,\mathfrak{e}_1, \ldots, \mathfrak{e}_u\,]$. Dann haben wir unmittelbar

$$\dim [\,\mathfrak{e}_1, \ldots, \mathfrak{e}_u\,] + \dim [\,\mathfrak{e}_{u+1}, \ldots, \mathfrak{e}_n\,] = \dim \mathbf{X}\,.$$

Es ist aber $[\,\mathfrak{e}_1, \ldots, \mathfrak{e}_u\,] = \mathfrak{U}$ und $[\,\mathfrak{e}_{u+1}, \ldots, \mathfrak{e}_n\,] \subseteq \mathfrak{U}^{\perp}$, also aus Dimensionsgründen sogar $[\,\mathfrak{e}_{u+1}, \ldots, \mathfrak{e}_n\,] = \mathfrak{U}^{\perp}$. □

Hinweis: 5.3.8 liefert u. a. als Sonderfall den Satz 2.1.9 Man beachte, dass wir dort zwar kein skalares Produkt im engeren Sinne an der Hand hatten, aber doch von der speziellen Basis der *Einheitsvektoren* $\mathfrak{e}_i = (0, \ldots, 1, \ldots 0)$ hätten ausgehen und schließen können wie hier.

5.4 Der Duale Raum

Sei $\mathbf{X}$ ein euklidischer oder unitärer Raum endlicher Dimension und sei $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ eine ONB zu $\mathbf{X}$. Dann liefert die Menge der Endomorphismen $\phi : \mathbf{X} \longmapsto \mathbf{K}$ von $\mathbf{X}$ in den Körper der Skalaren, aufgefasst als eindimensionaler Vektorraum mit der Orthonormalbasis $\mathfrak{e}$, einen Linearen Raum von der Dimension $1 \cdot n$ – wie wir schon im letzten Kapitel sahen. Die dortige Konstruktion einer Basis bedeutet hier natürlich die Ermittelung eines Systems $\chi_i \;\; (1 \leq i \leq n)$ mit

$$\begin{aligned} \chi_i(\mathfrak{e}_k) &= \mathfrak{o} \text{ falls } i \neq k \\ \chi_i(\mathfrak{e}_i) &= \mathfrak{e}_i \text{ falls } . \end{aligned}$$

Ist nun ϕ irgendeine Abbildung dieser Art, so können wir ϕ also darstellen mittels einer **Linearform** $x_1\chi_1+x_2\chi_2+\ldots+x_n\chi_n$ und es entspricht diesem Element in kanonischer Weise das Element $x_1\mathfrak{e}_1 + x_2\mathfrak{e}_2 + \ldots + x_n\mathfrak{e}_n$.

Da $\mathbf{X}$ ein Skalarprodukt besitzt und die beiden betrachteten Vektorräume isomorph sind, können wir natürlich auch auf dem Vektorraum $\mathbf{V}(\mathbf{X} \longmapsto \mathbf{K})$ in kanonischer Weise ein skalares Produkt erklären. Diese erfüllt dann

$$\begin{aligned} & (x_1\chi_1 + x_2\chi_2 + \ldots + x_n\chi_n) \star (y_1\chi_1 + y_2\chi_2 + \ldots + y_n\chi_n) \\ = \; & (x_1\mathfrak{e}_1 + x_2\mathfrak{e}_2 + \ldots + x_n\mathfrak{e}_n) \star (y_1\mathfrak{e}_1 + y_2\mathfrak{e}_2 + \ldots + y_n\mathfrak{e}_n) \,, \end{aligned}$$

insbesondere also $\chi_i \star \chi_k = \delta_{i,k}$ worin $\delta_{i,k}$ das KRONECKER-Symbol bedeutet, definiert vermöge:

$$\delta_{i,k} = \begin{cases} 0, & \text{falls } i \neq k \\ 1, & \text{falls } i = k \end{cases}$$

Damit haben wir den Ausgangsraum dann dargestellt als einen Raum von linearen Abbildungen bzw. als einen Raum von Linearformen.

Der so entstehende Raum heißt der zu $\mathbf{X}$ duale Raum.

Kapitel 6

Adjungierte

6.1 Adjungierte Abbildungen

Ziel dieses Abschnitts ist eine Untersuchung spezieller Endomorphismen, also auch spezieller Matrizen, auf besondere Eigenschaften. Dazu werden wir ganz allgemein starten, indem wir ausgehen von Abbildungen $\phi : \mathbf{X} \longmapsto \mathbf{Y}$ und $\psi : \mathbf{Y} \longmapsto \mathbf{X}$ zweier Vektorräume $\mathbf{X}$ und $\mathbf{Y}$ mit den jeweiligen Skalarprodukten $\star$ bzw. $*$ die der Bedingung genügen:

$$\phi\mathfrak{x} * \mathfrak{y} \;=\; \mathfrak{x} \star \psi\,\mathfrak{y},$$

also – kurz – von der Situation:

$$\begin{array}{c} \phi : \mathbf{X} \longmapsto \mathbf{Y} \quad , \quad \psi : \mathbf{Y} \longmapsto \mathbf{X} \\ (\phi\mathfrak{x} * \mathfrak{y} \;=\; \mathfrak{x} \star \psi\,\mathfrak{y}), \end{array}$$

die *per definitionem* die zu Grunde gelegten Skalarprodukte aufs Engste berücksichtigen.

Insbesondere werden wir uns für jene Endomorphismen interessieren, die das Skalarprodukt „respektieren", also $\phi(\mathfrak{x}\star\mathfrak{y}) = \phi\mathfrak{x}*\phi\mathfrak{y}$ erfüllen. Sie bilden, wie man relativ leicht bestätigt, eine Gruppe, die so genannte **unitäre** bzw. im euklidischen Fall die so genannte **orthogonale** Gruppe .

6. 1. 1 Definition. Seien $\mathbf{X}$ und $\mathbf{Y}$ beide euklidisch oder unitär. Dann nennen wir die linearen Abbildungen

$$\phi : \mathbf{X} \longmapsto \mathbf{Y} \quad \text{und} \quad \phi^* : \mathbf{Y} \longmapsto \mathbf{X}\,,$$

adjungiert, wenn sie

$$(\phi\mathfrak{x}) * \mathfrak{y} \;=\; \mathfrak{x} \star \phi^*\mathfrak{y}$$

und damit auch $\phi^*\mathfrak{y} * \mathfrak{x} = \mathfrak{y} \star \phi\mathfrak{x}$ erfüllen.

Existiert zu ϕ ein adjungiertes ϕ^*, so ist dieses adjungierte eindeutig bestimmt wegen

$$\mathfrak{x} \star (\phi^*\mathfrak{y} - \phi'\mathfrak{y}) = 0 \ \ (\forall \mathfrak{x} \in \mathfrak{x}) \Longrightarrow \phi^*\mathfrak{y} = \phi'\mathfrak{y}.$$

Allerdings muss keineswegs eine solche Abbildung existieren, dies lässt sich am Beispiel 3 aus Kapitel 5 belegen.

Es gilt aber im Sonderfall der für das Folgende bedeutende Satz:

6. 1. 2 Proposition. *Sei* $\mathbf{X}$ *n-dimensional mit dem Skalarprodukt* $\star$ *und* $\mathbf{Y}$ *ein Vektorraum mit dem Skalarprodukt* $*$ *. Dann existiert zu jeder linearen Abbildung (auch bezeichnet als linearer Operator)* $\phi : \mathbf{X} \longmapsto \mathbf{Y}$ *ein adjungierter linearer Operator* $\phi^* : \mathbf{Y} \longmapsto \mathbf{X}$ *.*

BEWEIS. Ist $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ eine ONB zu $\mathbf{X}$, so gilt für

$$\phi^*\mathfrak{y} \ := \ \sum_{i=1}^{n} (\mathfrak{y} * \phi\mathfrak{e}_i)\mathfrak{e}_i$$

erstens: ϕ^* ist linear

und zweitens:

$$\begin{aligned}
\phi\mathfrak{x} * \mathfrak{y} &= \sum x_i(\phi\mathfrak{e}_i * \mathfrak{y}) \\
&= \sum x_i \overline{(\mathfrak{y} * \phi\mathfrak{e}_i)} \\
&= \sum (\mathfrak{x} \star \mathfrak{e}_i) \cdot \overline{(\mathfrak{y} * \phi\mathfrak{e}_i)} \\
&= \sum \overline{(\mathfrak{y} * \phi\mathfrak{e}_i)} \cdot (\mathfrak{x} \star \mathfrak{e}_i) \\
&= \sum \mathfrak{x} \star ((\mathfrak{y} * \phi\mathfrak{e}_i)\mathfrak{e}_i) \\
&= \mathfrak{x} \star \phi^*\mathfrak{y},
\end{aligned}$$

und damit die Behauptung. □

6. 1. 3 Proposition. *Ist* $\mathbf{X}$ *euklidisch oder unitär und sind die Abbildungen* $\phi : \mathbf{X} \longmapsto \mathbf{Y}$ *und* $\phi^* : \mathbf{Y} \longmapsto \mathbf{X}$ *adjungiert, so gilt:*

(*i*) $\ker \phi^* = (\phi\mathfrak{X})^\perp$
(*ii*) $\operatorname{rg} \phi$ *endlich* $\Longrightarrow$ (ϕ *surjektiv* $\Longleftrightarrow$ ϕ^* *injektiv*) *.*

DENN: Zunächst gilt:

$$\begin{aligned}
\mathfrak{y} \in \ker \phi^* &\iff \phi^*\mathfrak{y} = \mathfrak{o} \\
&\iff \mathfrak{x} \star \phi^*\mathfrak{y} = 0 \ \ (\forall \mathfrak{x} \in \mathfrak{X}) \\
&\iff \phi\mathfrak{x} \star \mathfrak{y} = 0 \ \ (\forall \mathfrak{x} \in \mathfrak{X}) \\
&\iff \mathfrak{y} \in (\phi\mathfrak{X})^\perp
\end{aligned}$$

und es resultiert im Falle eines endlichen Ranges von ϕ, also immer im Falle endlicher Dimension von $\mathbf{Y}$

$$\begin{aligned}
\phi\,\text{surjektiv} &\implies (\phi\mathfrak{X})^\perp = \mathfrak{O} \\
&\implies \ker \phi^* = \mathfrak{O} \\
&\implies \phi^*\,\text{injektiv} \\
&\ \ \& \quad (\phi\mathfrak{X})^\perp = \ker \phi^* = \mathfrak{O} \\
&\implies \phi\mathfrak{X} = (\phi\mathfrak{X})^{\perp\perp} = \mathfrak{O}^\perp = \mathfrak{Y}. \\
&\implies \phi\,\text{surjektiv}
\end{aligned}$$

die vorletzte Zeile nach 5.3.8 □

Insbesondere ist also unter (ii) die Dimension von $\mathbf{X}$ notwendig endlich.

6. 1. 4 Proposition. *Seien* $\mathbf{X}$ *bzw.* $\mathbf{Y}$ *euklidisch bzw. unitär und seien* ϕ *und* ϕ^* *adjungiert. Dann gilt*

$$\operatorname{rg}\phi^* = \operatorname{rg}\phi.$$

DENN: unter den gemachten Voraussetzungen gilt:

$$\begin{aligned}
\operatorname{rg}\phi^* &= \dim \mathbf{Y} - \dim(\ker \phi^*) \\
&= \dim \mathbf{Y} - \dim(\phi\mathbf{X})^\perp \\
&= \dim(\phi\mathbf{X})^{\perp\perp} \\
&= \dim(\phi\mathbf{X}) \\
&= \operatorname{rg}\phi.
\end{aligned}$$

□

Wie im „Vorspann" erwähnt, interessieren uns natürlich die den linearen Abbildungen ϕ und ϕ^* zugeordneten Matrices (Matrizen). Hierzu vorab

6. 1. 5 Definition. Sei A eine komplexe $m \times n$-Matrix. Dann setzen wir für $1 \leq i, j \leq m, n$

$$A^* := (\overline{A})^\top = \overline{A^\top}, \text{ also } (a_{i,k})^* = (\overline{a_{k,i}}).$$

6. 1. 6 Proposition. *Bezüglich des Operators $*$ gelten die Gleichungen:*

$$A^{**} = A, \ \ (A+B)^* = A^* + B^*, \ \ (AB)^* = B^* A^*, \ \ |\, A^* \,| = |\, \overline{A} \,|.$$

Nun sind wir in der Lage, ϕ und ϕ^* durch Matrizen zu „kodieren".

6. 1. 7 Proposition. *Seien* $\mathbf{X}$ *und* $\mathbf{Y}$ *zwei n-dimensionale euklidische bzw. unitäre Vektorräume und seien weiter $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ eine* ONB *zu* $\mathbf{X}$ *sowie $(\mathfrak{f}_1, \ldots, \mathfrak{f}_m)$ eine* ONB *zu* $\mathbf{Y}$.

Wird dann ϕ bezüglich dieser Basen vermittelt durch A, so wird das adjungierte ϕ^* vermittelt durch A^*.

BEWEIS. Gelte

	$\phi\mathfrak{e}_1$	$\phi\mathfrak{e}_2$	$\ldots$	$\phi\mathfrak{e}_n$
$\mathfrak{f}_1$	a_{11}	a_{12}	$\ldots$	$a_{1,n}$
$\mathfrak{f}_2$	a_{21}	a_{22}	$\ldots$	$a_{2,n}$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
$\mathfrak{f}_m$	$a_{m,1}$	$a_{m,2}$	$\ldots$	$a_{m,n}$.

Dann haben wir

$$\begin{aligned} \phi\mathfrak{e}_i * \mathfrak{f}_k &= a_{k,i} \\ \text{und} \qquad \phi^*\mathfrak{f}_k \star \mathfrak{e}_i &= b_{i,k} \end{aligned}$$

Folglich gilt

$$\begin{aligned} b_{i,k} = \phi^*\mathfrak{f}_k \star \mathfrak{e}_i &= \overline{\mathfrak{e}_i \star \phi^*\mathfrak{f}_k} \\ &= \overline{\phi\mathfrak{e}_i * \mathfrak{f}_k} = \overline{a_{k,i}} \end{aligned}$$

und damit $B = A^*$, also die Behauptung. □

6.2 Normale Endomorphismen

6. 2. 1 Definition. Ein Endomorphismus $\phi : \mathbf{X} \longmapsto \mathbf{X}$ heißt **normal**, wenn ϕ ein adjungiertes ϕ^* besitzt und diese eindeutig bestimmte ϕ^* zudem der Bedingung genügt:

(N) $$\phi \circ \phi^* \;=\; \phi^* \circ \phi\,.$$

6. 2. 2 Proposition. *Sei* $\mathbf{X}$ *ein n-dimensionaler euklidischer oder unitärer Vektorraum. Dann ist* ϕ *genau dann normal, wenn gilt:*

$$\phi\mathfrak{x} \star \phi\mathfrak{y} \;=\; \phi^*\mathfrak{x} \star \phi^*\mathfrak{y}.$$

BEWEIS. Ist ϕ normal, so folgt

$$\begin{aligned}\phi\mathfrak{x} \star \phi\mathfrak{y} &= \mathfrak{x} \star (\phi^* \circ \phi)\mathfrak{y}\\ &= \mathfrak{x} \star (\phi \circ \phi^*)\mathfrak{y}\\ &= \phi^*\mathfrak{x} \star \phi^*\mathfrak{y},\end{aligned}$$

und gilt $\phi\mathfrak{x} \star \phi\mathfrak{y} = \phi^*\mathfrak{x} \star \phi^*\mathfrak{y}$, so haben wir

$$\begin{aligned}((\phi \circ \phi^*)\mathfrak{x}) \star \mathfrak{y} &= (\phi(\phi^*\mathfrak{x})) \star \mathfrak{y} \quad (\forall \mathfrak{y})\\ &= \phi^*\mathfrak{x} \star \phi^*\mathfrak{y}\\ &= \phi\mathfrak{x} \star \phi\mathfrak{y}\\ &= \phi^*(\phi\mathfrak{x}) \star \mathfrak{y}\\ &= ((\phi^* \circ \phi)\mathfrak{x}) \star \mathfrak{y},\\ &\rightsquigarrow\\ (\phi \circ \phi^*)\mathfrak{x} &= (\phi^* \circ \phi)\mathfrak{x} \;\; (\forall \mathfrak{x} \in \mathfrak{X})\end{aligned}$$

□

6. 2. 3 Proposition. *Ist* ϕ *normal, so gilt* $\ker\phi = \ker\phi^*$.

DENN: ist ϕ normal, so folgt:

$$\begin{aligned}\phi\mathfrak{x} = \mathfrak{o} &\iff \phi\mathfrak{x} \star \phi\mathfrak{x} = 0\\ &\iff \phi^*\mathfrak{x} \star \phi^*\mathfrak{x} = 0\\ &\iff \phi^*\mathfrak{x} = \mathfrak{o}.\end{aligned}$$

□

6. 2. 4 Proposition. *Ist* $\mathbf{X}$ *euklidisch oder unitär und ist* ϕ *normal, so hat* ϕ^* *dieselben* EVn *wie* ϕ *und zwar jeweils mit dem konjugiert komplexen* EW *, im euklidischen Falle also mit dem gleichen* EW *.*

DENN: Unter den gemachten Voraussetzungen folgt:

$$\begin{aligned} \phi\mathfrak{x} = c\mathfrak{x} &\implies (\phi\mathfrak{x} - c\mathfrak{x})^2 = 0 \\ &\implies (\phi^*\mathfrak{x} - \overline{c}\mathfrak{x})^2 = 0 \\ &\implies \phi^*\mathfrak{x} - \overline{c}\mathfrak{x} = 0 \\ &\implies \phi^*\mathfrak{x} = \overline{c}\mathfrak{x}\ . \end{aligned}$$ □

Hiernach können wir beweisen:

6. 2. 5 Proposition. *Sei* $\mathbf{X}$ *n-dimensional unitär. Dann ist* ϕ *genau dann normal, wenn* $\mathbf{X}$ *eine* ONB $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ *aus lauter* EVn *besitzt.*

BEWEIS. (a) Da $\mathbf{X}$ unitär ist, existiert wegen des Fundamentalsatzes mindestens ein EW c mit EV $\mathfrak{e}_1$ vom Betrage 1. Damit sind wir im Falle $\dim \mathbf{X} = 1$ am Ziel.

Andernfalls sei $\mathbf{X}$ von der Dimension n und der Satz schon bewiesen für die Dimension $n-1$. Ist ϕ dann normal, so folgt

$$\begin{aligned} \mathfrak{E} := [\,\mathfrak{e}_1\,] \ \text{ und } \ \mathfrak{U} := \mathfrak{E}^\perp = [\,\mathfrak{e}_1\,]^\perp \\ \implies \\ \phi\,\mathfrak{U} \subseteq \mathfrak{U} \ \text{ und } \ \phi^*\,\mathfrak{U} \subseteq \mathfrak{U}, \end{aligned}$$

denn dann gilt für jedes $\mathfrak{x} \in \mathfrak{U}$:

$$\begin{aligned} \phi\,\mathfrak{x} \star \mathfrak{e}_1 \ &= \ \mathfrak{x} \star \phi^*\mathfrak{e}_1 \ = \ \mathfrak{x} \star \overline{c}\mathfrak{e}_1 \ = \ 0 \implies \phi\,\mathfrak{x} \in \mathfrak{E}^\perp = \mathfrak{U} \\ \& \ \ \phi^*\mathfrak{x} \star \mathfrak{e}_1 \ &= \ \mathfrak{x} \star \phi\,\mathfrak{e}_1 \ = \ \mathfrak{x} \star c\mathfrak{e}_1 \ = \ 0 \implies \phi^*\mathfrak{x} \in \mathfrak{E}^\perp = \mathfrak{U}, \end{aligned}$$

weshalb wir nach Induktionsvoraussetzung auch in diesem Fall am Ziel sind.

(b) Sei nun umgekehrt $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ eine ONB zu $\mathbf{X}$ aus lauter EVn zu ϕ. Dann liefert die Festsetzung

$$\psi\,\mathfrak{e}_i \ := \ \overline{c}_i\mathfrak{e}_i$$

einen zu ϕ adjungierten Endomorphismus mit

$$\phi \circ \psi \ = \ \psi \circ \phi\,.$$

Denn mit Hilfe des *Kronecker-Symbols*

$$\delta_{i,k} = \begin{cases} 0, & \text{falls } i \neq k \\ 1, & \text{falls } i = k \end{cases}$$

s. o. – erhalten wir

$$\begin{aligned}\phi\,\mathfrak{e}_i \star \mathfrak{e}_k &= (c_i\mathfrak{e}_i) \star \mathfrak{e}_k \\ &= c_i\delta_{i,k} \\ &= c_k\delta_{k,i} \\ &= \mathfrak{e}_i \star (\overline{c}_k\mathfrak{e}_k) \\ &= \mathfrak{e}_i \star \psi\,\mathfrak{e}_k,\end{aligned}$$

also allgemein

$$\phi\,\mathfrak{x} \star \mathfrak{y} = \mathfrak{x} \star \psi\,\mathfrak{y},$$

und es ist ferner

$$\begin{aligned}(\psi\circ\phi)\,\mathfrak{e}_i &= \psi\,(c_i\mathfrak{e}_i) = c_i\,\psi\mathfrak{e}_i = (c_i\overline{c}_i)\,\mathfrak{e}_i \\ &\;\&\\ (\phi\circ\psi)\,\mathfrak{e}_i &= \phi\,(\overline{c}_i\mathfrak{e}_i) = \overline{c}_i\,\phi\mathfrak{e}_i = (\overline{c}_ic_i)\,\mathfrak{e}_i\ .\end{aligned}$$ □

Der soeben geführte Beweis lässt sich im Reellen natürlich nicht kopieren, denn es muss ja kein reeller EW existieren. Man betrachte etwa $x^2 = -1$. Es gilt aber – natürlich – aufgrund des letzten Beweises:

6. 2. 6 Korollar. *Ist* **X** *n-dimensional euklidisch, so existiert eine* ONB *aus lauter* EV *genau dann, wenn* ϕ *ein normaler Endomorphismus mit lauter reellen* EWn *ist.*

Insbesondere hat sich *implizit* herausgestellt, dass unter den in 6.2.5 gegebenen Umständen zu einem Paar verschiedener EWe ein Paar orthogonaler EVn gehört, denn in die Darstellung eines EVs $\mathfrak{x}$ mit dem EW c über der ONB aus lauter EVn können nur Basisvektoren mit dem EW c eingehen, warum?

Um auch den allgemeinen reellen Fall zu erfassen, betrachten wir im folgenden die komplexe Erweiterung **Z** von **X**. Offenbar haben wir fast unmittelbar:

6. 2. 7 Proposition. *Mit* ϕ *ist auch* $\hat{\phi}$ *normal, man betrachte* $\widehat{\phi^*}$ *und rechne nach.*

Weiter können wir zeigen:

6. 2. 8 Proposition. *Ist* ϕ *ein normaler Endomorphismus des euklidischen Raumes* **X** *mit* ONB $(\mathfrak{e}_1,\ldots,\mathfrak{e}_n)$ *und* $\mathfrak{e} = \mathfrak{x} + i\mathfrak{y}$ *ein normierter* EV

zu $\hat{\phi}$ *mit nicht reellem* EW $c = a + bi$*, so ist* $\mathfrak{e}' := \mathfrak{x} - i\mathfrak{y}$ *ebenfalls ein normierter* EV *zu* ϕ *und zwar mit dem* EW $\overline{c}$ *sowie* $\mathfrak{e}' \perp \mathfrak{e}$.

BEWEIS. Da $\mathfrak{x}$ und $\mathfrak{y}$ aus $\mathbf{X}$ stammen, gilt $\mathfrak{x} \star \mathfrak{y} = \mathfrak{y} \star \mathfrak{x}$. Das führt vorab zu

$$\mathfrak{e}' \star \mathfrak{e}' = |\,\mathfrak{x}\,|^2 + |\,\mathfrak{y}\,|^2 + i(\mathfrak{x} \star \mathfrak{y} - \mathfrak{y} \star \mathfrak{x}) = \mathfrak{e} \star \mathfrak{e} = 1,$$

weshalb $\mathfrak{e}'$ normiert ist. Weiter haben wir

$$\begin{aligned} \hat{\phi}\,\mathfrak{e} &= \hat{\phi}\,(\mathfrak{x} + i\mathfrak{y}) \\ &= \phi\,\mathfrak{x} + i\phi\,\mathfrak{y} \\ &= (a + bi)(\mathfrak{x} + i\mathfrak{y}) \\ &= (a\mathfrak{x} - b\mathfrak{y}) + i(a\mathfrak{y} + b\mathfrak{x}) \\ &\rightsquigarrow \\ \phi\,\mathfrak{x} = a\mathfrak{x} - b\mathfrak{y} \quad &\& \quad \phi\,\mathfrak{y} = a\mathfrak{y} + b\mathfrak{x}\,, \end{aligned}$$

und das liefert:

$$\begin{aligned} \hat{\phi}\,\mathfrak{e}' &= \hat{\phi}\,(\mathfrak{x} - i\mathfrak{y}) \\ &= \phi\,\mathfrak{x} - i\phi\,\mathfrak{y} \\ &= (a\mathfrak{x} - b\mathfrak{y}) - i(a\mathfrak{y} + b\mathfrak{x}) \\ &= (a - bi)(\mathfrak{x} - i\mathfrak{y}) \\ &= \overline{c}\,\mathfrak{e}', \end{aligned}$$

weshalb $\mathfrak{e}'$ EV zu $\hat{\phi}$ mit EW $\overline{c}$ ist. Es ist $\mathfrak{e}'$ aber auch EV zu $\hat{\phi}^{\,*}$ mit dem EW $\overline{\overline{c}} = c$ und daher

$$\begin{aligned} c\,(\mathfrak{e} \star \mathfrak{e}') &= c\mathfrak{e} \star \mathfrak{e}' \\ &= \hat{\phi}\,\mathfrak{e} \star \mathfrak{e}' \\ &= \mathfrak{e} \star \hat{\phi}^{\,*}\mathfrak{e}' \\ &= \mathfrak{e} \star c\mathfrak{e}' \\ &= \overline{c}\,(\mathfrak{e} \star \mathfrak{e}'), \end{aligned}$$

also wegen $c \notin \mathbf{R}$ dann $\mathfrak{e} \star \mathfrak{e}' = 0$, d. h. $\mathfrak{e} \perp \mathfrak{e}'$. □

Hiernach können wir den normalen euklidischen Endomorphismus beschreiben.

6. 2. 9 Hauptsatz über normale Endomorphismen. *Sei* $\mathbf{X}$ *ein endlich dimensionaler euklidischer Raum. Dann ist* $\phi : \mathbf{X} \longmapsto \mathbf{X}$ *genau dann normal, wenn es eine* ONB *zu* $\mathbf{X}$ *gibt, bezüglich der* ϕ *vermittelt wird durch eine Matrix des Typs*

$$A = \begin{pmatrix} c_1 & & & & & \\ & \ddots & & & & \\ & & c_k & & & \\ & & & \boxed{} & & \\ & & & & \boxed{\begin{matrix} a & b \\ -b & a \end{matrix}} & \\ & & & & & \ddots \end{pmatrix},$$

worin die c_i *jeweils reelle* EWe *sind und die Kästchen für* EWe *des Typs* $a + bi$ *stehen.*

BEWEIS. (a) Im Fall $n = 1$ ist nichts zu zeigen. Sei deshalb $n \geq 2$ und die Behauptung bewiesen für $n - 1$. Wir unterscheiden

Fall 1: Besitze ϕ einen EW in $\mathbf{R}$.

Dann können wir unseren Beweis schon an dieser Stelle fortfahren wie unter Proposition 6.2.5

Fall 2: Besitze ϕ hiernach keinen EW in $\mathbf{R}$.

Wir betrachten $\mathbf{Z}$ und setzen ϕ fort zur $\hat{\phi}$. Zu diesem Endomorphismus existiert ein normierter EV $\mathfrak{e} = \mathfrak{x} + i\mathfrak{y}$ mit nicht reellem EW $c = a + bi$. Dann ist aber, wie wir sahen, auch $\mathfrak{e}\,' = \mathfrak{x} - i\mathfrak{y}$ EV zu $\hat{\phi}$ und zwar mit dem EW $a - bi$.

Wir setzen nun

$$\mathfrak{f}_1 \;:=\; \frac{1}{\sqrt{2}}\,(\mathfrak{e} + \mathfrak{e}\,') = \sqrt{2}\,\mathfrak{x}$$

$$\mathfrak{f}_2 \;:=\; \frac{1}{i\sqrt{2}}\,(\mathfrak{e} - \mathfrak{e}\,') = \sqrt{2}\,\mathfrak{y}.$$

Dann gelten

$$\mathfrak{f}_1\,,\,\mathfrak{f}_2 \;\in\; \mathfrak{X} \tag{6.2}$$

$$|\,\mathfrak{f}_1\,| \;=\; 1 \;=\; |\,\mathfrak{f}_2\,| \tag{6.3}$$

$$\mathfrak{f}_1 \star \mathfrak{f}_2 \;=\; 0 \tag{6.4}$$

$$\phi\,\mathfrak{f}_1 = a\mathfrak{f}_1 - b\mathfrak{f}_2 \;\&\; \phi\,\mathfrak{f}_2 = af_2 + b\mathfrak{f}_1 \tag{6.5}$$

Denn: $(i), (ii), (iii)$ folgen durch Nachrechnen. Ferner erhalten wir:

$$\begin{aligned}
\phi\,\mathfrak{f}_1 &= \hat{\phi}\,\frac{1}{\sqrt{2}}\,(\mathfrak{e}+\mathfrak{e}\,') \\
&= \frac{1}{\sqrt{2}}\,\left(\hat{\phi}\,\mathfrak{e}+\hat{\phi}\,\mathfrak{e}\,'\right) \\
&= \frac{1}{\sqrt{2}}\,(c\mathfrak{e}+\overline{c}\mathfrak{e}\,') \\
&= \frac{1}{\sqrt{2}}\,(c\mathfrak{x}+ci\mathfrak{y}+\overline{c}\mathfrak{x}-\overline{c}i\mathfrak{y}) \\
&= \frac{1}{\sqrt{2}}\,(c+\overline{c})\mathfrak{x}+\frac{1}{\sqrt{2}}\,i\,(c-\overline{c})\mathfrak{y} \\
&= \sqrt{2}\,\mathfrak{x}-\sqrt{2}\;\mathfrak{y} \\
&= a\mathfrak{f}_1 - b\mathfrak{f}_2 \quad (\text{mit } a=b=\sqrt{2})\,,
\end{aligned}$$

und es gilt eine analoge Herleitung für $\phi\,\mathfrak{f}_2$. Somit entspricht hinsichtlich $\mathfrak{f}_1, \mathfrak{f}_2$ dem Endomorphismus ϕ ein „Zweierkästchen" der beschriebenen Art. Also können wir unseren Beweis auch in diesem Falle fortsetzen wie unter Proposition 6.2.5.

(b) Werde nun umgekehrt ϕ bezüglich einer ONB vermittelt durch eine Matrix i. S. des Satzes. Sind dann $\mathfrak{f}_1, \mathfrak{f}_2$ die zu einem „a,b-Kästchen" gehörenden normierten Basisvektoren, gilt also:

$$\begin{aligned}
\phi\,\mathfrak{f}_1 &= a\mathfrak{f}_1 - b\mathfrak{f}_2 \\
\&\quad \phi\,\mathfrak{f}_2 &= a\mathfrak{f}_2 + b\mathfrak{f}_1\,,
\end{aligned}$$

so erhalten wir mit

$$\begin{aligned}
\psi\,\mathfrak{f}_1 &:= a\mathfrak{f}_1 + b\mathfrak{f}_2 \\
\&\quad \psi\,\mathfrak{f}_2 &:= a\mathfrak{f}_2 - b\mathfrak{f}_1
\end{aligned}$$

zum einen

$$\phi \circ \psi = \psi \circ \phi \;\;\&\;\; \phi\mathfrak{x} \star \mathfrak{y} = \mathfrak{x} \star \psi\,\mathfrak{y}\,,$$

wegen

$$(\phi \circ \psi)(\mathfrak{f}_1) = \phi(\psi\mathfrak{f}_1) = a^2 f_1 - b^2\mathfrak{f}_2 = \psi(\phi\mathfrak{f}_1) = (\psi \circ \phi)(\mathfrak{f}_1)$$

und der entsprechenden Herleitung für $\mathfrak{f}_2$, sowie zum anderen:

$$\begin{aligned}
\phi\mathfrak{x} \star \mathfrak{y} &= \phi(x_1\mathfrak{f}_1 + x_2\mathfrak{f}_2) \star (y_1\mathfrak{f}_1 + y_2\mathfrak{f}_2) \\
&= (x_1 a\mathfrak{f}_1 - x_1 b\mathfrak{f}_2 + x_2 b\mathfrak{f}_1 + x_2 a\mathfrak{f}_2) \star (y_1\mathfrak{f}_1 + y_2\mathfrak{f}_2) \\
&= (ax_1 + bx_2)\mathfrak{f}_1 - (bx_1 - ax_2)) \star (y_1\mathfrak{f}_1 + y_2\mathfrak{f}_2) \\
&= ax_1y_1 + bx_2y_1 - bx_1y_2 + ax_2y_2 \\
&= \mathfrak{x} \star \psi\mathfrak{y}\,.
\end{aligned}$$

Das bedeutet insgesamt, dass ϕ und ψ adjungiert und zudem normal sind. □

Damit haben wir für normale Endomorphismen eine Matrixdarstellung gewonnen, die zwar nicht ganz so überschaubar ist, wie eine Diagonal-Matrix, die aber doch bei weitem leichter zu handhaben ist als eine beliebige Matrix.

Mit der Darstellung normaler Endomorphismen ist die Basis gelegt für die Darstellung spezieller klassischer Endomorphismen.

6.3 Selbstadjungierte Endomorphismen

Unter den Endomorphismen eines unitären bzw. euklidischen Raumes $\mathbf{X}$ sind vor allem diejenigen $\phi : \mathbf{X} \longmapsto \mathbf{X}$ von Interesse, die mit ihren adjungierten zusammenfallen.

6. 3. 1 Definition. $\phi : \mathbf{X} \longmapsto \mathbf{X}$ heißt **selbstadjungiert**, kurz *s.a.* , wenn gilt $\phi\mathfrak{x} \star \mathfrak{y} = \mathfrak{x} \star \phi\mathfrak{y}$.

Unmittelbar klar ist:

6. 3. 2 Proposition. *Jeder s.a. Endomorphismus ist normal.*

Weiter haben wir – man rechne nach:

6. 3. 3 Proposition. *Mit ϕ ist auch $\hat{\phi}$ s.a.*

Schließlich erhalten wir das bedeutende Ergebnis

6. 3. 4 Proposition. *Sei $\mathbf{X}$ euklidisch oder unitär und sei der Endomorphismus $\phi : \mathbf{X} \longmapsto \mathbf{X}$ s.a. . Dann hat das charakterische Polynom lauter reelle Nullstellen, ϕ also lauter reelle* EWe .

BEWEIS. Wie wir sahen, haben ϕ und ϕ^* dieselben EVn jedoch jeweils mit konjugiert komplexen EWn . Folglich erfüllt im unitären Fall jeder EW c die Bedingung $c = \overline{c}$ und damit $c \in \mathbf{R}$. Natürlich trägt dieser Beweis auch noch im euklidischen Fall.

Es gilt aber sogar, dass alle Nullstellen des charakteristischen Polynoms in $\mathbf{C}$ reell sind. Um dies zu zeigen, gehen wir über zu der komplexen Erweiterung $\mathbf{Z}$ von $\mathbf{X}$ und betrachten $\mathbf{Z}$ bezüglich einer reellen Basis $\mathfrak{B}$. Man beachte, dass dies stets möglich ist. Haben wir nämlich irgend eine Basis, so liefern die reellen und die imaginären Komponenten der Basisvektoren zusammen ein Erzeugendensystem, also auch die reellen Komponenten zusammen mit den „von i befreiten" imaginären Komponenten.

Dann lassen sich aber alle Vektoren $\mathfrak{x} \in \mathfrak{X}$ reell über $\mathfrak{B}$ kombinieren – klar, da ja der komplexe Anteil der komplexen Darstellung verschwindet. Also ist $\mathfrak{B}$ auch Basis zu $\mathbf{X}$, und dies bedeutet, dass ϕ und $\hat{\phi}$ dasselbe charakteristische Polynom besitzen und somit alle komplexen Nullstellen des charakteristischen Polynoms von ϕ sogar reell sind. □

Als unmittelbare Folgerung hieraus ergibt sich, dass das charakteristische Polynom von ϕ lauter reelle Koeffizienten besitzt, insbesondere also, dass die Determinante der vermittelnden Matrix reell ist und ebenso die Spur $\sum_1^n a_{ii}$ von A . Darüber hinaus ergibt sich aus der Normalität von ϕ :

6. 3. 5 Proposition. *Zu jedem s.a. Endomorphismus eines n–dimensionalen $\mathbf{X}$ existiert eine* ONB *aus lauter* EVn *, und es wird ϕ bezüglich dieser Basis durch eine reelle Diagonalmatrix vermittelt.* [1)]

[1)] Tatsächlich können wir uns hier natürlich auf 6.2.5 beschränken und da ϕ *s.a.* ist, also $\phi = \phi^*$ erfüllt ist, verkürzt sich der dortige Beweis auf die Feststellung: Es gilt die Aussage für $n = 1$ und ist sie schon für $n - 1$ bewiesen, so folgt sie fast unmittelbar durch Zerlegung von $\mathbf{X}$ in zwei zueinander orthogonale Komponenten $\mathbf{U}$,$\mathbf{V}$, wegen $\phi\mathfrak{U} \subseteq \mathfrak{U} \ldots$.

Weiter sei erwähnt

6. 3. 6 Proposition. *Ist ϕ ein beliebiger Endomorphismus mit adjungiertem ϕ^*, so ist $\phi \circ \phi^*$ also auch $\phi^* \circ \phi$ sogar s.a. , und es sind alle etwaigen* EW *von $\phi^* \circ \phi$ nicht negativ reell.*

DENN: die erste Behauptung ist fast evident und die zweite ergibt sich aus

$$(\phi^* \circ \phi)\,\mathfrak{x} = c\,\mathfrak{x} \Longrightarrow c\,(\mathfrak{x} \star \mathfrak{x}) = ((\phi^* \circ \phi)\mathfrak{x} \star \mathfrak{x}) = \phi\mathfrak{x} \star \phi\mathfrak{x} \geq 0.$$

Man beachte $\mathfrak{x} \neq \mathfrak{o} \rightsquigarrow \mathfrak{x} \star \mathfrak{x} > 0$. □

Wir schauen nun nach Matrixdarstellungen *s.a.* Endomorphismen.

6. 3. 7 Definition. Eine komplexe Matrix A heißt **hermitesch** (nach Charles Hermite, 1822–1901), wenn $A = A^*$ erfüllt ist. Ist A reell und zudem hermitesch, so heißt A auch **symmetrisch** .

Per definitionem ist eine hermitesche Matrix stets quadratisch. Weiterhin liegen die Diagonalenelemente einer hermiteschen Matrix (wegen $c = \overline{c}$) notwendig auf der reellen Achse, und schließlich ist fast unmittelbar klar – man beachte $\phi \sim A \Longleftrightarrow \phi^* \sim A^*$:

6. 3. 8 Proposition. *Sei* $\mathbf{X}$ *endlich–dimensional und unitär bzw. euklidisch sowie* $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ *eine* ONB *zu* $\mathbf{X}$ *. Dann ist ϕ s.a. genau dann, wenn ϕ hinsichtlich dieser* ONB *durch eine hermitesche bzw. symmetrische Matrix dargestellt wird.*

Damit erhalten wir aufgrund unsrerer bisherigen Ausführungen als Hauptresultat über hermitesche bzw. symmetrische Matrizen

6. 3. 9 Proposition. *Alle* EW *einer hermiteschen oder symmetrischen Matrix sind reell.*

Insbesondere besitzt also das charakteristische Polynom einer hermiteschen Matrix A reelle Koeffizienten, und es sind Determinante und Spur von A reell. Schließlich ist jede hermitesche bzw. symmetrische Matrix zu einer reellen Diagonalmatrix ähnlich.

Endlich sei angemerkt, dass zu jedem Paar verschiedener EWe *ein Paar orthogonaler* EVn *gehört, vgl. die Anmerkung hinter 6.2.5 .*

Im weiteren befassen wir uns mit einer zum *s.a.* Endomorphismus verwandten Abbildungsart.

6. 3. 10 Definition. $\phi : \mathbf{X} \longmapsto \mathbf{X}$ heißt *anti-selbstadjungiert*, auch kurz *a.s.a.* , wenn gilt $\phi\mathfrak{x} \star \mathfrak{y} = -\mathfrak{x} \star \phi\mathfrak{y}$.

Unmittelbar klar ist auch hier:

6. 3. 11 Proposition. *Jeder a.s.a. Endomorphismus ist normal.*

Weiter haben wir – man rechne nach:

6. 3. 12 Proposition. *Mit ϕ ist auch $\hat{\phi}$ a.s.a.*

Schließlich erhalten wir das bedeutende Ergebnis

6. 3. 13 Proposition. *Ist $\phi : \mathbf{X} \longmapsto \mathbf{X}$ ein a.s.a. Endomorphismus, so hat ϕ lauter rein imaginäre* EWe .

BEWEIS. Ist c EW zu dem *a.s.a.* Endomorphismus ϕ, so gilt im Falle $\phi\mathfrak{x} = c\mathfrak{x}$

$$\begin{aligned} c(\mathfrak{x} \star \mathfrak{x}) = c\mathfrak{x} \star \mathfrak{x} &= \phi\mathfrak{x} \star \mathfrak{x} \\ &= -\mathfrak{x} \star \phi\mathfrak{x} = -\mathfrak{x} \star c\mathfrak{x} = -\overline{c}(\mathfrak{x} \star \mathfrak{x}), \end{aligned}$$

also $c = -\overline{c}$ (wegen $\mathfrak{x} \neq \mathfrak{o}$). □

Wir kommen nun zur Matrixbeschreibung von *a.s.a.* Endomorphismen.

6. 3. 14 Definition. Sei A eine komplexe Matrix, dann heißt A **schief–hermitesch** , wenn $A^* = -A$ erfüllt ist. Ist A reell und schief–hermitesch, so heißt A auch **schief–symmetrisch** .

Per definitionem ist eine schief–hermitesche Matrix stets quadratisch. Weiterhin liegen die Diagonalenelemente einer schief–hermiteschen Matrix notwendig auf der imaginären Achse, und es ist $\phi^* = -\phi$ fast unmittelbar klar – wenn ϕ bzw. ϕ^* den Matrizen $-A$ bzw. A^* bezüglich einer vorgegebenen ONB entsprechen.

6. 3. 15 Proposition. *Sei $\mathbf{X}$ endlich–dimensional und unitär bzw. euklidisch sowie $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ eine* ONB *zu $\mathbf{X}$. Dann gilt: ϕ ist a.s.a. gdw. ϕ hinsichtlich dieser* ONB *durch eine schief–hermitesche bzw. schief–symmetrische Matrix vermittelt wird.*

Zusammenfassend haben wir also, vgl. die letzte Fußnote,

6. 3. 16 Proposition. *Zu jedem a.s.a. Endomorphismus ϕ eines endlich–dimensionalen unitären Raumes* $\mathbf{X}$ *existiert eine* ONB *aus lauter* EVn *von* ϕ *.*

Hinsichtlich dieser Basis entspricht ϕ einer Diagonalmatrix, deren Hauptdiagonalenelemente alle auf der imaginären Achse liegen, und es ist jede schief–hermitesche Matrix zu einer solchen Diagonalmatrix ähnlich.

Endlich haben wir auf der Grundlage von 6.2.9

6. 3. 17 Proposition. *Zu jedem a.s.a. Endomorphismus ϕ eines endlich–dimensionalen euklidischen Raumes existiert eine* ONB *bezüglich der ϕ durch eine reelle Matrix A der Form*

$$A = \begin{pmatrix} \ddots & & & & \\ & \ddots & & & \\ & & \boxed{} & & \\ & & & \boxed{\begin{matrix} 0 & b \\ -b & 0 \end{matrix}} & \\ & & & & \ddots \end{pmatrix},$$

repräsentiert wird, und jede schief–symmetrische Matrix A ist ähnlich zu einer Matrix diesen Typs.

Schließlich sei festgehalten:

6. 3. 18 Ein Erster Zerlegungssatz. *Sei* $\mathbf{X}$ *euklidisch oder unitär und sei $\phi : \mathbf{X} \longmapsto \mathbf{X}$ ein beliebiger Endomorphismus mit adjungiertem ϕ^*. Dann lässt sich ϕ eindeutig als Summe*

$$\phi \;=\; \phi_1 + \phi_2$$

mit s.a. ϕ_1 und a.s.a. ϕ_2 darstellen.

BEWEIS. Wir setzen

$$\begin{aligned} & \phi_1 \;:=\; \tfrac{1}{2}(\phi + \phi^*) \\ \& \qquad & \phi_2 \;:=\; \tfrac{1}{2}(\phi - \phi^*). \end{aligned}$$

Dann rechnet man leicht nach, dass ϕ_1 *s.a.* und ϕ_2 *a.s.a.* ist. Haben wir nun zudem im Sinne des Satzes

$$\begin{array}{rcl} \phi & = & \psi_1 + \psi_2 \,, \\ \phi_1 - \psi_1 & = & \psi_2 - \phi_2 \end{array}$$

so folgt
mit *s.a.* linker und *a.s.a.* rechter Seite, was zunächst zu der Gleichheit $\phi_1 - \psi_1 = 0 = \psi_2 - \phi_2$, also zu $\phi_1 = \psi_1$ und damit weiter zu $\phi_2 = \psi_2$ führt. □

Wir beenden diesen Abschnitt mit einem Hinweis auf den späteren Abschnitt über Projektionen, den der interessierte Leser schon an dieser Stelle studieren mag.

6.4 Orthogonale und unitäre Abbildungen

Ist ϕ ein Endomorphismus eines unitären (euklidischen) Raumes $\mathbf{X}$, so „nimmt" ϕ z. B. die Linearität des Raumes „mit". Keineswegs aber ist auch gesichert, dass ϕ etwa ebenso die „Orthogonalität(en)" „mitnimmt", denn die Bilder orthogonaler Paare $\mathfrak{a}, \mathfrak{b}$ müssen ja keineswegs wieder orthogonal sein und auch ist nicht gesichert, dass ein Endomorphismus längentreu ist.

Klassische Abbildungen, die dies leisten, sind z. B. die Drehung – etwa der Ebene – um den Ursprung oder die Spiegelung an einer Achse (Geraden durch den Ursprung), denn diese Abbildungen sind ja Kongruenzabbildungen im Sinne der euklidischen Geometrie.

Wollen wir nun erneut soviel Klassisches wie möglich herüberretten in die Theorie der linearen Räume – hier mit Skalarprodukt – , so bietet es sich an, das Skalarprodukt ins Spiel zu bringen, denn es werden ja Längen und (der Kosinus eines) Winkel(s) definiert über das Skalarprodukt.

6. 4. 1 Definition. Seien $\mathbf{X}$ und $\mathbf{Y}$ euklidisch bzw. unitär. Dann heißt eine lineare Abbildung $\phi : \mathbf{X} \longmapsto \mathbf{Y}$ **orthogonal** bzw. **unitär,** falls sie der Bedingung genügt:

$$\phi\,\mathfrak{x}_1 \star \phi\,\mathfrak{x}_2 \;=\; \mathfrak{x}_1 \star \mathfrak{x}_2 \,.$$

Es wird sich zeigen, dass orthogonale (unitäre) Abbildungen neben der "Algebra" auch die "Geometrie von $\mathbf{X}$" respektieren. Genauer :

6. 4. 2 Proposition. *Seien* $\mathbf{X}, \mathbf{Y}$ *euklidisch* (*unitär*). *Dann sind pw. äquivalent:*

(*i*) $\phi : \mathbf{X} \longmapsto \mathbf{Y}$ *ist orthogonal* (*unitär*),

(*ii*) $|\,\mathfrak{x}\,| = 1 \Longrightarrow |\,\phi\,\mathfrak{x}\,| = 1$, *also Winkeltreue, da der Kosinus mitgeht,*

(*iii*) $|\,\mathfrak{x}\,| = |\,\phi\,\mathfrak{x}\,|$, *also Längentreue und damit auch Winkeltreue,*

(*iv*) $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ ONS $\Longrightarrow (\phi\,\mathfrak{e}_1, \ldots, \phi\,\mathfrak{e}_n)$ ONS .

BEWEIS. $(i) \Longrightarrow (ii)$, denn aus $|\,\mathfrak{x}\,| = 1$ folgt:

$$\phi\,\mathfrak{x} \star \phi\,\mathfrak{x} = \mathfrak{x} \star \mathfrak{x} = 1 \rightsquigarrow |\,\phi\,\mathfrak{x}\,| = 1.$$

$(ii) \Longrightarrow (iii)$, denn ist o. B. d. A. $\mathfrak{x} \neq \mathfrak{o}$, so folgt mit $\mathfrak{e} = \frac{1}{|\mathfrak{x}|}\,\mathfrak{x}$ zum einen $\mathfrak{x} = |\,\mathfrak{x}\,|\mathfrak{e}$ und zum andern $|\,\mathfrak{e}\,| = 1$, also

$$|\,\phi\,\mathfrak{x}\,| = |\,\mathfrak{x}\,|\,|\,\phi\,\mathfrak{e}\,| = |\,\mathfrak{x}\,|\,.$$

$(iii) \Longrightarrow (iv)$. Zunächst sind wegen $|\,\phi\,\mathfrak{e}_i\,| = |\,\mathfrak{e}_i\,| = 1$ alle $\phi\,\mathfrak{e}_i$ normiert . Weiter sind für alle $i \neq j$ $(i, j \in \{1, \ldots, n\})$ die Bilder $\phi\,\mathfrak{e}_i$, $\phi\,\mathfrak{e}_j$ orthogonal, wegen

$$\begin{aligned} 2\,\mathrm{Re}\,(\phi\,\mathfrak{e}_i \star \phi\,\mathfrak{e}_j) &= |\,\phi\,\mathfrak{e}_i + \phi\,\mathfrak{e}_j\,|^2 - |\,\phi\,\mathfrak{e}_i\,|^2 - |\,\phi\,\mathfrak{e}_j\,|^2 \\ &= |\,\mathfrak{e}_i + \mathfrak{e}_j\,|^2 - |\,\mathfrak{e}_i\,|^2 - |\,\mathfrak{e}_j\,|^2 \\ &= 1 + 1 - 1 - 1 = 0 \end{aligned}$$

und

$$\begin{aligned} 2\,\mathrm{Im}\,(\phi\,\mathfrak{e}_i \star \phi\,\mathfrak{e}_j) &= |\,\phi\,\mathfrak{e}_i + i\phi\,\mathfrak{e}_j\,|^2 - |\,\phi\,\mathfrak{e}_i\,|^2 - |\,\phi\,\mathfrak{e}_j\,|^2 \\ &= |\,\mathfrak{e}_i + i\mathfrak{e}_j\,|^2 - |\,\mathfrak{e}_i\,|^2 - |\,\mathfrak{e}_j\,|^2 = 0. \end{aligned}$$

$(iv) \Longrightarrow (i)$. Aus (iv) resultiert $|\,e\,| = 1 \Longrightarrow |\,\phi\,\mathfrak{e}\,| = 1$. Seien nun weiter $\mathfrak{x}_1 \neq \mathfrak{o}$ und $\mathfrak{x}_2$ beliebig aus $\mathfrak{X}$. Dann unterscheiden wir die Fälle (a), in dem $\{\mathfrak{x}_1, \mathfrak{x}_2\}$ ℓa sei und (b), in dem $\{\mathfrak{x}_1, \mathfrak{x}_2\}$ ℓu sei.

(a) Sei $\mathfrak{x}_2 = c\frac{1}{|\,\mathfrak{x}_1\,|}\,\mathfrak{x}_1$. Dann folgt mit $\mathfrak{e} := \frac{1}{|\,\mathfrak{x}_1\,|}\,\mathfrak{x}_1$:

$$\begin{aligned} \mathfrak{x}_1 \star \mathfrak{x}_2 &= |\,\mathfrak{x}_1\,|\,e \star c\,\mathfrak{e} \\ &= \overline{c}|\,\mathfrak{x}_1\,|\,(\mathfrak{e} \star \mathfrak{e}) \\ &= \overline{c}|\,\mathfrak{x}_1\,|\,(\phi\,\mathfrak{e} \star \phi\,\mathfrak{e}) \\ &= |\,\mathfrak{x}_1\,|\phi\,\mathfrak{e} \star c\,\phi\,\mathfrak{e} \\ &= \phi\,(|\,\mathfrak{x}_1\,|\,\mathfrak{e}) \star \phi\,(c\,\mathfrak{e}) \\ &= \phi\,\mathfrak{x}_1 \star \phi\,\mathfrak{x}_2 \end{aligned}$$

(b) Sei $\{\mathfrak{x}_1, \mathfrak{x}_2\}$ nun ℓu. Dann gibt es eine ONB zu $[\,\mathfrak{x}_1, \mathfrak{x}_2\,]$, etwa $(\mathfrak{e}_1, \mathfrak{e}_2)$, und es folgt mit

$$\begin{aligned} \mathfrak{x}_1 &= x_{11}\,\mathfrak{e}_1 + x_{12}\,\mathfrak{e}_2 \\ \mathfrak{x}_2 &= x_{21}\,\mathfrak{e}_1 + x_{22}\,\mathfrak{e}_2 \end{aligned}$$

Die Gleichheit

$$\begin{aligned} \phi\,\mathfrak{x}_1 \star \phi\,\mathfrak{x}_2 &= (x_{11}\,\phi\,\mathfrak{e}_1 + x_{12}\,\phi\,\mathfrak{e}_2) \star (x_{21}\,\phi\,\mathfrak{e}_1 + x_{22}\,\phi\,\mathfrak{e}_2) \\ &= x_{11}\,\overline{x_{21}} + x_{12}\,\overline{x_{22}} \\ &= \mathfrak{x}_1 \star \mathfrak{x}_2\,. \end{aligned}$$

Damit sind wir am Ziel. □

Weiter liefert 6.4.2

6. 4. 3 Proposition. *Ist ϕ orthogonal auf $\mathbf{X}$, so ist $\hat{\phi}$ unitär auf $\mathbf{Z}$,*
man rechne nach, und
6. 4. 4 Proposition. *Ist ϕ orthogonal, so ist ϕ auch injektiv,*

denn, man beachte:

$$\begin{aligned} \mathfrak{x} \neq \mathfrak{x}' &\implies \mathfrak{x} - \mathfrak{x}' \neq \mathfrak{o} \\ &\implies |\,\mathfrak{x} - \mathfrak{x}'\,| \neq 0 \\ &\implies |\,\phi\,\mathfrak{x} - \phi\,\mathfrak{x}'\,| \neq 0. \\ &\implies \phi\,\mathfrak{x} \neq \phi\,\mathfrak{x}'. \end{aligned}$$

6. 4. 5 Proposition. *Sei $\phi : \mathbf{X} \longmapsto \mathbf{Y}$ ein orthogonaler bzw. unitärer Isomorphismus. Dann ist auch ϕ^{-1} orthogonal bzw. unitär, und es ist $\phi^* = \phi^{-1}$.*

Ist umgekehrt $\phi : \mathbf{X} \longmapsto \mathbf{Y}$ ein Isomorphismus mit $\phi^* = \phi^{-1}$, so ist ϕ orthogonal bzw. unitär.

BEWEIS. (a) Seien $\mathfrak{y}_1, \mathfrak{y}_2$ aus $\mathfrak{Y}$. Dann gilt zunächst

$$\begin{aligned} \phi^{-1}\mathfrak{y}_1 \star \phi^{-1}\mathfrak{y}_2 &= \phi\,\phi^{-1}\mathfrak{y}_1 \star \phi\,\phi^{-1}\mathfrak{y}_2 \\ &= \mathfrak{y}_1 \star \mathfrak{y}_2 \end{aligned}$$

und damit weiter:

$$\begin{aligned} \phi\,\mathfrak{x} \star \mathfrak{y} &= \phi^{-1}\phi\,\mathfrak{x} \star \phi^{-1}\mathfrak{y} \\ &= \mathfrak{x} \star \phi^{-1}\mathfrak{y}. \end{aligned}$$

(b) Sei hiernach ϕ ein Isomorphismus mit $\phi\,\mathfrak{x}\star\mathfrak{y} = \mathfrak{x}\star\phi^{-1}\mathfrak{y}$. Dann folgt

$$\begin{aligned}\phi\,\mathfrak{x}_1 \star \phi\,\mathfrak{x}_2 &= \mathfrak{x}_1 \star \phi^{-1}\phi\,\mathfrak{x}_2 \\ &= \mathfrak{x}_1 \star \mathfrak{x}_2\,.\end{aligned}$$

Damit sind wir am Ziel. □

Wir interessieren uns natürlich für die den orthogonalen bzw. unitären Abbildungen entsprechenden Matrizen.

6. 4. 6 Definition. Eine komplexe quadratische Matrix A heißt **orthogonal** bzw. **unitär**, wenn sie $A^* = A^{-1}$ erfüllt.

Es folgt – wie nicht anders zu erwarten –

6. 4. 7 Proposition. *Seien* $\mathbf{X}$ *und* $\mathbf{Y}$ *von gleicher endlicher Dimension. Dann gilt: Eine lineare Abbildung* $\phi : \mathbf{X} \longmapsto \mathbf{Y}$ *ist unitär* (*orthogonal*)*, gdw. ihr bezüglich beliebiger* ONBn *von* $\mathbf{X}$ *und von* $\mathbf{Y}$ *eine unitäre* (*orthogonale*) *Matrix entspricht.*

HINWEIS: Man beachte $\phi^* \longleftrightarrow A^*$ und 6.4.5.

Orthogonale bzw. unitäre Matrizen besitzen eine bemerkenswerte charakteristische Eigenschaft:

6. 4. 8 Proposition. *Es sind je zwei der nachfolgenden Aussagen äquivalent:*

(*i*) *A ist unitär* (*orthogonal*)
(*ii*) *Die Zeilen von A bilden ein* ONS [2)] ,
(*iii*) *Die Spalten von A bilden ein* ONS ,

BEWEIS. Bedingung (*ii*) ist gleichwertig mit $AA^* = E$, Bedingung (*iii*) ist gleichwertig mit $A^*A = E$, und jede dieser Gleichungen beinhaltet $A^* = A^{-1}$. □

Hiernach können wir beweisen:

6. 4. 9 Proposition. (*a*) *Jeder unitäre bzw. orthogonale Automorphismus* ϕ *ist normal und alle* EWe *eines solchen* ϕ *liegen auf dem Einheitskreis. Ist zudem* $\mathbf{X}$ *endlich dimensional, so gilt darüber hinaus* $|\det\phi| = 1$.

[2)] natürlich bezüglich $(a_1,\dots,a_n)\star(b_1,\dots b_n) = \sum_1^n a_i\bar{b}_i$

(*b*) *Ist umgekehrt ϕ ein normaler Endomorphismus eines endlich dimensionalen unitären Raumes, dessen* EWe *auf dem Einheitskreis liegen, so ist ϕ unitär.*

BEWEIS. (a) Wegen $\phi^* = \phi^{-1}$ ist ϕ normal. Gilt weiter $\phi\,\mathfrak{x} = c\,\mathfrak{x}$, so folgt:

$$\begin{aligned} \phi\,\mathfrak{x} = c\,\mathfrak{x} &\rightsquigarrow c\overline{c}\,(\mathfrak{x}\star\mathfrak{x}) = \phi\,\mathfrak{x}\star\phi\,\mathfrak{x} = 1\,(\mathfrak{x}\star\mathfrak{x}) \\ &\rightsquigarrow c\overline{c} = 1. \end{aligned}$$

Endlich gilt – man erinnere $|\,A\,| = |\,A^T\,|$ und $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ sowie $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$, also $|\det\phi| = |\det\phi^*|$, die Gleichungskette:

$$|\det\phi| = |\det\phi^*| \;=\; |\det\phi^{-1}| = |\det\phi|^{-1},$$

und damit $|\det\phi| = 1$.

(b) Sei ϕ ein normaler Endomorphismus von $\mathbf{X}$. Dann gibt es, zumindest in der komplexen Erweiterung $\mathbf{Z}$, eine ONB aus lauter EVn von ϕ, und es entspricht ϕ hinsichtlich dieser Basis eine Diagonalmatrix A, deren Hauptdiagonalenelemente die EWe von ϕ sind. Da diese EWe auf dem Einheitskreis liegen, verschwindet keiner von ihnen, weshalb A regulär, ϕ also sogar ein Automorphismus ist.

Dem adjungierten ϕ^* entspricht aber die Matrix A^* mit den Hauptdiagonalenelementen $\overline{c}_i$. Deshalb haben wir $AA^* = E$, beachte $c_i\overline{c_i} = |c_i|^2 = 1$, und somit $\phi^* = \phi^{-1}$, weshalb ϕ nach 6.4.5 unitär (orthogonal) ist. □

6. 4. 10 Proposition. *Die Menge aller unitären bzw. orthogonalen Endomorphismen eines unitären (euklidischen) Raumes* $\mathbf{X}$ *auf sich bildet bezüglich $\circ$ eine Gruppe, genannt die* **unitäre** *bzw.* **orthogonale Gruppe.**

BEWEIS. Man beachte: das Bild eines ONS ist wieder ein ONS. Somit ist die betrachtete Menge abgeschlossen bezüglich $\circ$. Weiter ist die identische Abbildung unitär. Und schließlich ist mit ϕ auch ϕ^{-1} unitär. □

6. 4. 11 Ein zweiter Zerlegungssatz. *Sei* $\mathbf{X}$ *ein endlich dimensionaler unitärer (euklidischer) Raum und ϕ ein beliebiger Automorphismus. Dann lässt sich ϕ auf genau eine Weise darstellen in der Form*

$$\phi \;=\; \phi_1 \circ \phi_2$$

mit unitärem (orthogonalem) ϕ_1 *und selbstadjungiertem* ϕ_2, *dessen* EWe *ausnahmslos positiv sind.*

BEWEIS. Sei $\psi_0 = \phi^* \circ \phi$. Dann ist ψ_0 selbstadjungiert – man rechne nach – mit lauter nicht negativen reellen EWn. Ferner ist mit ϕ auch ϕ^* ein Automorphismus. Daher sind die EWe von ψ_0 sogar positiv reell. Demzufolge existiert eine ONB $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ von $\mathbf{X}$ aus lauter EVn von ψ_0 mit $\psi_0(\mathfrak{e}_i) = c_i\,\mathfrak{e}_i, c_i > 0 \;\; (1 \leq i \leq n)$.

Wir setzen nun $\psi\,\mathfrak{e}_i := \sqrt{c_i}\,\mathfrak{e}_i$. Dann ist auch dies ein selbstadjungierter Endomorphismus mit lauter positiven EWn, und es gilt offenbar $\psi \circ \psi = \psi_0 = \phi^* \circ \phi$ und wegen der Selbstadjungiertheit darüber hinaus auch $\psi = \psi^*$ und $\psi^{-1} = (\psi^{-1})^*$, man rechne nach. Hiernach setzen wir $\phi_1 := \phi \circ \psi^{-1}$. Dann folgt ${\phi_1}^* = {\phi_1}^{-1}$, vermöge:

$$\begin{aligned} {\phi_1}^* &= (\phi \circ \psi^{-1})^* \\ &= (\psi^{-1)^*} \circ \phi^* \\ &= \psi^{-1} \circ \phi^* \circ \phi \circ \phi^{-1} \\ &= \psi^{-1} \circ \psi \circ \psi \circ \phi^{-1} \\ &= \psi \circ \phi^{-1} \\ &= {\phi_1}^{-1}. \end{aligned}$$

Somit ist ϕ_1 unitär und folglich $\phi = \phi_1 \circ \psi$ eine Darstellung der gewünschten Art.

Zur Eindeutigkeit: Sei hiernach $\phi = \chi_1 \circ \chi_2$ ebenfalls eine Zerlegung im Sinne des Satzes und $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ die oben ausgezeichnete ONB. Dann folgt zunächst

$$\begin{aligned} \psi \circ \psi &= \phi^* \circ \phi \\ &= ({\chi_2}^* \circ {\chi_1}^*) \circ (\chi_1 \circ \chi_2) \\ &= \chi_2 \circ ({\chi_1}^{-1} \circ \chi_1) \circ \chi_2 \\ &= \chi_2 \circ \chi_2. \end{aligned}$$

Nun haben aber χ_2 und $\chi_2 \circ \chi_2 = \psi \circ \psi$ als selbstadjungierte Automorphismen dieselben EVn und zwar χ_2 mit den positiven EWn ${d_i}^2 = c_i \rightsquigarrow d_i = \sqrt{c_i}$.

HINWEIS: Man zerlege $\mathbf{X}$ direkt in $[\mathfrak{e}_1] \oplus [\mathfrak{e}_2, \ldots, \mathfrak{e}_n]$ und induziere über $\dim \mathbf{X}$.

Also stimmen ψ und χ_2 überein in ihren EVn und EWn , woraus $\chi_2 = \psi$ resultiert und damit weiter $\phi_1 = \chi_1$, man multipliziere von rechts mit ψ^{-1} , also die behauptete Eindeutigkeit. □

Endlich sei mit Blick auf quadratische Formen herausgestellt:

6. 4. 12 Proposition. *Zu jeder hermiteschen (symmetrischen) Matrix A gibt es eine unitäre (orthogonale) Matrix P derart, dass $P^{-1}AP =: D$ eine reelle Diagonalmatrix ist. Insbesondere gilt somit auch $D = P^*AP$.*

BEWEIS. Sei $\mathbf{X}$ ein unitärer bzw. euklidischer Raum. Wir wählen eine Basis B und betrachten den von A vermittelten Endomorphismus ϕ. Dieser ist *s.a.* und lässt sich demzufolge bzgl. einer geeigneten ONB durch eine reelle Diagonalmatrix D vermitteln. Zu der Transformation von B nach dieser ONB gehört aber eine unitäre (orthogonale) Matrix P, da die identische Abbildung unitär (orthogonal) ist. Damit gilt unsere Behauptung auf Grund von $P^* = P^{-1}$. □

6.5 Skalare Produkte und Matrizen

Nachdem wir im letzten Abschnitt den Begriff der unitären bzw. orthogonalen Matrix geklärt haben, sind wir nun in der Lage, alle denkbaren skalaren Produkte eines unitären (euklidischen) Raumes zu charakterisieren.

Ist $\star$ ein skalares Produkt und $(\mathfrak{b}_1, \ldots, \mathfrak{b}_n)$ eine Basis zu $\mathbf{X}$, so liegen die Werte $\mathfrak{x} \star \mathfrak{y}$ fest, da sie sich aus den Basisdarstellungen von $\mathfrak{x}$ und $\mathfrak{y}$ ergeben. Genauer gilt

$$\begin{aligned} \mathfrak{x} &= x_1\mathfrak{b}_1 + \ldots + x_n\mathfrak{b}_n \\ \mathfrak{y} &= y_1\mathfrak{b}_1 + \ldots + y_n\mathfrak{b}_n \\ &\rightsquigarrow \\ \mathfrak{x} \star \mathfrak{y} &= \sum_{i,k=1}^{n} x_i \cdot (\mathfrak{b}_i \star \mathfrak{b}_k) \cdot \overline{y}_k \,. \end{aligned}$$

Schreiben wir hierin $\mathfrak{x}$ und $\mathfrak{y}$ als Matrizen X und Y vom Typ $n \times 1$, so können wir auch „kodieren" bzw. „notieren":

$$\mathfrak{x} \star \mathfrak{y} = X^\top B\, \overline{Y} \quad (B = \mathfrak{b}_i \star \mathfrak{b}_k) \,,$$

wenn wir nur „stillschweigend vereinbaren", die Matrix „als Summe zu lesen". Wir fragen nun ganz allgemein, wann eine **Bilinearform**

$$\mathfrak{x} \star \mathfrak{y} \;:=\; \sum_{i,k=1}^{n} x_i \cdot b_{ik} \cdot \overline{y}_k$$

bei dieser Vereinbarung ein skalares Produkt auf $\mathbf{R}^n$ bzw. $\mathbf{C}^n$ liefert.

Offenbar sind die drei ersten Gesetze des skalaren Produktes stets erfüllt, hingegen das vierte nicht immer. Wir fragen deshalb weiter: Was zeichnet diejenigen Matrizen B aus, die auch bezüglich (S4) unseren Wünschen genügen, also bezüglich

$$\mathfrak{x} \star \mathfrak{y} \;=\; X^\top B\, \overline{Y}$$

ein skalares Produkt stiften. Hier gilt

6. 5. 1 Proposition. *Genau dann liefert $X^\top A\, \overline{Y}$ ein skalares Produkt in $\mathbf{R}^n$ bzw. $\mathbf{C}^n$, wenn die Matrix A symmetrisch bzw. hermitesch ist, und zudem lauter positive* EWe *besitzt.*

BEWEIS. Es ist also zu zeigen:

$$\begin{aligned} & A \quad \begin{matrix}\text{hermitesch}\\ \text{symmetrisch}\end{matrix} \quad \text{mit positiven EWn} \\ \iff \quad & \forall X \neq 0 :\; X^\top A\, \overline{X} > 0. \end{aligned}$$

(a) Sei A eine Matrix im Sinne des Satzes und sei $X \neq 0$. Dann können wir A nach 6.3.12 als PDP^{-1} mit unitärem bzw. orthogonalem P und positiver Diagonalmatrix D annehmen. Damit folgt dann weiter:

$$\begin{aligned} \mathfrak{x} \star \mathfrak{x} \;&:=\; X^\top A\, \overline{X} \\ &=\; \left(X^\top P\right) \left(P^{-1} A P\right) \left(P^{-1}\, \overline{X}\right) \\ &=\; \left(X^\top P\right) D \left(P^*\, \overline{X}\right) \\ &=\; \left(P^\top X\right)^\top D \left(\overline{P^\top\, X}\right) \\ &=\; X'^\top D\, \overline{X'} \\ &=\; x_1' \cdot c_1 \cdot \overline{x_1'} + \ldots + x_n' \cdot c_n \cdot \overline{x_n'} \\ &\rightsquigarrow \\ \mathfrak{x} \star \mathfrak{x} \;&=\; c_1 \cdot |\, x_1' \,|^2 + \ldots + c_n \cdot |\, x_n' \,|^2 \end{aligned}$$

und damit wegen $\mathfrak{x} \neq \mathfrak{o}$ und $c_i > 0$ insgesamt

$$\mathfrak{x} \star \mathfrak{x} \;=\; X^\top A\, \overline{X} > 0.$$

(b) Sei nun $X^\top A\, \overline{Y} =: \mathfrak{x} \star \mathfrak{y}$ ein skalares Produkt. Dann gilt zunächst

$$\begin{aligned} \mathfrak{x} \star \mathfrak{y} &= X^\top A\, \overline{Y} \\ &= \sum_{i,k=1}^{n} x_i \cdot a_{ik} \cdot \overline{y_k}\ , \end{aligned}$$

und damit weiter – wegen $\mathfrak{x} \star \mathfrak{y} = \overline{\mathfrak{y} \star \mathfrak{x}}$

$$\sum_{i,k=1}^{n} x_i \cdot a_{ik} \cdot \overline{y_k} = \sum_{i,k=1}^{n} \overline{y_k \cdot a_{ki} \cdot \overline{x_i}} = \sum_{i,k=1}^{n} x_i \cdot \overline{a_{ki}} \cdot \overline{y_k}$$

also mit $x_i = 1 = y_k$ und $x_j = 0 = y_\ell$ $(j \neq i, \ell \neq k)$

$$a_{ik} = \overline{a_{ki}} \rightsquigarrow A = A^*\,.$$

Und ist nun weiter c ein EW zu $A = A^*$ mit EV $\mathfrak{x}$ (*per definitionem* $\neq \mathfrak{o}$), so folgt

$$\sum_{k=1}^{n} a_{ik} x_k \;=\; c x_i \quad (1 \leq i \leq n)$$

und damit für $\overline{\mathfrak{x}} := (\overline{x_1}, \ldots, \overline{x_n})$ wegen $\mathfrak{x} \neq \mathfrak{o} \rightsquigarrow \overline{\mathfrak{x}} \neq \mathfrak{o}$:

$$\begin{aligned} \overline{\mathfrak{x}} \star \overline{\mathfrak{x}} &= \sum_{i,k=1}^{n} \overline{x_i} \cdot a_{ik} \cdot \overline{\overline{x_k}} \\ &= \sum_{i,k=1}^{n} \overline{x_i} \cdot a_{ik} \cdot x_k \\ &= \sum_{i=1}^{n} \Big(\overline{x_i} \cdot \Big(\sum_{k=1}^{n} a_{ik} \cdot x_k \Big)\Big) \\ &= \sum_{i=1}^{n} \overline{x_i} \cdot c x_i \\ &= c \cdot \left(\overline{x_1} \cdot x_1 + \ldots + \overline{x_n} \cdot x_n\right) \\ &= c \cdot \left(|\, x_1 \,|^2 + \ldots + |\, x_n \,|^2\right) > 0 \end{aligned}$$

also auch $c > 0$. □

6.6 Projektionen *

Wir bemerken vorweg: Die nun folgenden Ausführungen hätten auch im Anschluss an Abschnitt 6.2 über selbstadjungierte Abbildungen vorgetragen werden können.

In Kapitel 6 wurde der Begriff der orthogonalen Projektion entwickelt – im folgenden kurz als Projektion bezeichnet – und zwar sollte $\mathfrak{x}_u$ (orthogonale) Projektion von $\mathfrak{x}$ in $\mathbf{U}$ heißen, wenn $\mathfrak{x} = \mathfrak{x}_u + \mathfrak{v}$ mit $\mathfrak{x}_u \in \mathfrak{U}$ und $\mathfrak{v} \in \mathfrak{U}^\perp$ erfüllt ist. Dabei zeigte es sich, dass $\mathfrak{x}_u$ im endlich dimensionalen Fall stets existiert und ganz allgemein im Fall der Existenz eindeutig bestimmt ist.

Weiter zerfällt der Vektorraum $\mathbf{X}$ nach 5.3.8 im n–dimensionalen Fall für jedes $\mathfrak{U} \subseteq \mathfrak{X}$ in die direkte Summe $\mathbf{X} = \mathbf{U} \oplus \mathbf{U}^\perp$.

Daher ist die orthogonale Projektion $\phi : \mathfrak{x} \longrightarrow \mathfrak{x}_u$ zum einen idempotent und zum andern *s.a.* Tatsächlich gilt aber sogar:

6. 6. 1 Lemma. *Sei* $\mathbf{X}$ *unitär, dann ist ein Endomorphismus* ϕ *eine Projektion genau dann, wenn er idempotent und zudem s.a. ist.*

DENN: Gilt $\phi \circ \phi = \phi$ und $\phi\mathfrak{x} \star \mathfrak{y} = \mathfrak{x} \star \phi\mathfrak{y}$, so folgt für alle $\mathfrak{x}$

$$\begin{array}{rrcl} & \mathfrak{x} & = & \phi\mathfrak{x} + (\mathfrak{x} - \phi\mathfrak{x}) \\ \& & \mathfrak{y} & = & \phi\mathfrak{z} \in \phi\mathfrak{X} \\ & & \Longrightarrow & \\ \mathfrak{y} \star (\mathfrak{x} - \phi\mathfrak{x}) & & = & \phi\mathfrak{z} \star (\mathfrak{x} - \phi\mathfrak{x}) \\ & & = & \mathfrak{z} \star (\phi\mathfrak{x} - (\phi \circ \phi)\mathfrak{x}) \\ & & = & 0\,. \end{array}$$

also ist $\phi\mathfrak{x}$ orthogonale Projektion in $\phi\mathbf{X}$.

Der Rest ergibt sich aus unserer Vorbemerkung. □

Hiernach folgt

6. 6. 2 Der Projektionssatz. *Sei* $\mathbf{X}$ *unitär,* ϕ *ein normaler Endomorphismus von* $\mathbf{X}$ *und* $(\mathfrak{e}_1, \ldots, \mathfrak{e}_n)$ *eine* ONB *aus lauter Eigenvektoren zu* ϕ*. Dann lässt sich* ϕ *als Linearkombination* $\phi = \sum c_j \pi_j$ *darstellen, worin die* c_j *die* EWe *von* ϕ *und die* π_j *die Projektion in die ERe* $\mathbf{W}_i$ *zu* ϕ *sind.*

Weiter gilt für die eingeführten π_j $(1 \leq j \leq m)$ *und die ERe* $\mathbf{W}_j$

(i) $\pi_i \circ \pi_i = \pi_i$

(ii) $\pi_i \circ \pi_k = 0$ *im Falle* $i \neq k$

(iii) $\pi_1 + \ldots + \pi_m = id$

(iv) $\mathbf{X} = \mathbf{W}_1 \oplus \ldots \oplus \mathbf{W}_m$,

und es gibt i. w. keine andere Linearkombination zu ϕ *, die diesen Bedingungen genügt.*

BEWEIS. Sei c_j irgendein EW zu ϕ . Ist dann c_j EW genau zu den Basisvektoren $\mathfrak{e}_{j,1}, \ldots, \mathfrak{e}_{j,k_j}$, so setzen wir

$$\pi_j(\mathfrak{x}) \;:=\; \sum_{\ell=1}^{k_j} x_\ell \, \mathfrak{e}_{j,\ell} \ ,$$

das heißt, wir verkürzen die Basisdarstellung von $\mathfrak{x}$ um diejenigen Summanden $x_p \, \mathfrak{e}_p$, die unter ϕ einen anderen EW als c_j haben. Das liefert *per definitionem* (i) bis (iii) .

Insbesondere erhalten wir mit dieser Definition $\pi_i(\mathfrak{e}_j) = \mathfrak{e}_j$, falls $c_i = c_j$, also EW zu $\mathfrak{e}_j$ ist, und $\pi_i(\mathfrak{e}_j) = \mathfrak{o}$, falls $c_i \neq c_j$ und damit kein EW zu $\mathfrak{e}_j$ ist.

Weiter folgt unmittelbar

$$\begin{array}{rrcl} & \pi_j(\mathfrak{x}) & = & \mathfrak{x}_{Wj} \\ & & \text{und} & \\ & \phi & = & c_1\pi_1 + \ldots + c_m\pi_m, \\ \text{wegen} & \phi\mathfrak{x} & = & \phi(\pi_1\mathfrak{x} + \ldots + \pi_m\mathfrak{x}) \\ & & = & c_1\pi_1\mathfrak{x} + \ldots + c_m\pi_m\mathfrak{x} \\ & & = & (c_1\pi_1 + \ldots + c_m\pi_m)\mathfrak{x}. \end{array}$$

Sei hiernach

$$\phi \;=\; c_1\sigma_1 + \ldots + c_m\sigma_m$$

ebenfalls eine Darstellung, die den Bedingungen (i) bis (iii) genügt. Wir zeigen, dass dann auch $\sigma_j = \pi_j \ \ (1 \leq j \leq m)$ erfüllt ist. Hierzu reicht der Nachweis von

$$\begin{array}{rcl} \sigma_j(\mathfrak{e}_i) & = & \pi_j(\mathfrak{e}_i) \\ (1 \leq j \leq m \quad , & & 1 \leq i \leq n) \ , \end{array}$$

also von

$$\sigma_j(\mathfrak{e}_i) = \begin{cases} \mathfrak{e}_i\,, & \text{falls } c_j \text{ ein EW zu } \mathfrak{e}_i \\ \mathfrak{o}\,, & \text{falls } c_j \text{ kein EW zu } \mathfrak{e}_i\ . \end{cases}$$

Annahme: Der EW zu $\mathfrak{e}_i$ ist c_j . Dann folgt:

$$\phi(\mathfrak{e}_i) = c_j\mathfrak{e}_i \ = \ \sigma_1(c_1\mathfrak{e}_i) + \ldots + \sigma_m(c_m\mathfrak{e}_i),$$

also nach Anwendung des „Operators" σ_k auf beide Seiten

$$\begin{aligned} \sigma_k(c_j\mathfrak{e}_i) \ &= \ \sigma_k(c_k\mathfrak{e}_i) \\ &\rightsquigarrow \\ (c_j - c_k)(\sigma_k\mathfrak{e}_i) \ &= \ \mathfrak{o} \end{aligned}$$

für jeden EW c_k.

Ist c_k nun nicht EW zu $\mathfrak{e}_i$, also $c_j \neq c_k$, so erhalten wir aus der letzten Gleichung

$$\sigma_k(\mathfrak{e}_i) \ = \ \mathfrak{o}\,.$$

Ist hingegen $c_k = c_j$, also c_k sehr wohl ein EW zu $\mathfrak{e}_i$, so folgt

$$\sigma_k(\mathfrak{e}_i) \ = \ \sigma_j(\mathfrak{e}_i) = \mathfrak{e}_i\,,$$

wegen $\sigma_1 + \ldots + \sigma_m = \mathrm{id}$, denn wir haben nach Voraussetzung:

$$\sigma_1(\mathfrak{e}_i) + \ldots + \sigma_m(\mathfrak{e}_i) \ = \ \mathfrak{o} + \ldots + \sigma_j(\mathfrak{e}_i) + \ldots + \mathfrak{o} = \mathfrak{e}_i\,.$$

Damit sind wir am Ziel, denn man beachte, dass die π_i so definiert wurden, dass die direkte Zerlegung $X = W_1 \oplus \ldots \oplus W_m$ *per definitionem* (*constructionem*) folgt. □

Ist ϕ im obigen Sinne zerlegt, so sagen wir auch, ϕ sei **spektralisiert** .

HINWEIS. Der letzte Satz hat natürlich seine Entsprechung für Matrizen. Dabei handelt es sich nach Konstruktion um eine Darstellung der diagonalisierten Matrix zu A, also um eine Darstellung von

$$D \ = \ \begin{pmatrix} c_1 & & & & \\ & \ddots & & & \\ & & c_1 & & \\ & & & \ddots & \\ & & & & c_m \\ & & & & & \ddots \\ & & & & & & c_m \end{pmatrix} \ = \ c_1E_1 + \ldots + c_mE_m\ ,$$

worin die einzelnen E_j aus D dadurch hervorgehen, dass man in D c_j ersetzt durch 1 und c_k $(k \neq j)$ durch 0 .

Dies führt dann für normale Matrizen A mit $S^{-1}AS = D$ für die Definition $D_j := S^{-1} \cdot E_j S$ $(1 \leq j \leq m)$ zu

$$A \;=\; c_1 D_1 + \ldots + c_m D_m$$

mit

$$(i) \quad D_j^2 = D_j = S^{-1} E_j S$$

$$(ii) \quad D_j D_k = 0 = S^{-1} E_j E_k S$$

$$(iii) \quad E = D_1 + \ldots + D_m \,,$$

wobei (i) aus $S^{-1}E_jS \cdot S^{-1}E_jS$, (ii) aus $S^{-1}E_jS \cdot S^{-1}E_kS$ und (iii) aus der Gleichung $S^{-1} \cdot (\sum E_j) \cdot S = S^{-1}ES = E$ resultiert.

Demzufolge gilt:

Spektralisierung

=

Diagonalisierung + Trivial-Entzerrung .

Kapitel 7

Die Jordansche Normalform

Ist A eine komplexe Matrix, so zerfällt das charakteristische Polynom nach dem Fundamentalsatz der Algebra in Linearfaktoren, doch mag es sein, dass die algebraischen und geometrischen Ordnungen der einzelnen EWe nicht in jedem Falle übereinstimmen. Das bedeutet, dass sich eine komplexe Matrix nicht notwendig diagonalisieren, wohl aber erwarten lässt, dass immer noch eine stark vereinfachte Transformierte zu A existiert. Um eine solche Vereinfachung geht es in diesem Kapitel. Wir beginnen mit einem schlichten, aber hochrelevantem Hinweis.

7. 0. 3 Lemma. *Ist B eine Blockmatrix vom Typ*

$$\begin{pmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_m \end{pmatrix},$$

so geht A in eine ähnliche Matrix über, wenn man die B_i permutiert oder aber, wenn man eins der B_i ersetzt durch ein ähnliches B_i^*.

DENN: dies ergibt sich unmittelbar aus

$$\begin{pmatrix} A \\ B \end{pmatrix} \cdot \begin{pmatrix} C \\ D \end{pmatrix} = \begin{pmatrix} AC \\ BD \end{pmatrix}$$

oder aber auch aus der Konstruktion gemäß Kapitel 6. Man beachte: Blökken entsprechen ℓ–tupel von Vektoren

$$\mathfrak{y}_k, \mathfrak{y}_{k+1}, \ldots, \mathfrak{y}_{k+e} \text{ bzw. } \phi\mathfrak{y}_k, \phi\mathfrak{y}_{k+1}, \ldots, \phi\mathfrak{y}_{k+\ell}$$

bzw. anders formuliert: Blöcke stehen für Unterraumendomorphismen

$$[\,\mathfrak{u}_1,\ldots,\mathfrak{u}_m\,]\longmapsto\phi[\,\mathfrak{u}_1,\ldots,\mathfrak{u}_m\,]\,.$$ □

Unter Berücksichtigung dieses Lemmas können wir weiter zeigen:

7. 0. 4 Proposition. *Jede komplexe Matrix A ist ähnlich zu einer oberen Dreiecksblockmatrix B, deren Dreiecksblöcke B_j $(1\leq j\leq m)$ in der Diagonalen jeweils belegt sind mit dem* EW c_j.

BEWEIS. Der Satz ist evident für die Dimension 1. Er sei nun schon bewiesen für alle $k\times k$–Matrizen mit $k\leq n-1$.

Dann gilt der Satz auch für alle $n\times n$–Matrizen, wie wir jetzt zeigen werden:

Sei hierzu c_1 EW zu dem EV $\mathfrak{x}_1$ und $(\,\mathfrak{x}_1,\ldots,\mathfrak{x}_n\,)$ eine Basis zu $\mathbf{C}^n$. Vermittelt dann A bezüglich der Einheitsbasis $(\,\mathfrak{e}_1,\ldots,\mathfrak{e}_n\,)$ den Endomorphismus ϕ, so wird dieser Endomorphismus ϕ bezüglich $(\,\mathfrak{x}_1,\ldots,\mathfrak{x}_n\,)$ vermittelt durch eine Matrix B vom Typ

$$\begin{pmatrix} c_1, b_{12},\ldots,b_{1n}\\ 0\\ \vdots \qquad C\\ 0\end{pmatrix}=:B,$$

worin C nach Induktionsvoraussetzung zu einem G der gewünschten Art ähnlich ist, also $G=R^{-1}CR$ mit G vom gesuchten Typ erfüllt. [1] Das liefert weiter

$$B\sim\begin{pmatrix}1,0,\ldots,0\\0\\\vdots\quad R^{-1}\\0\end{pmatrix}\cdot\begin{pmatrix}c_1,b_{12},\ldots,b_{1,n}\\0\\\vdots\qquad C\\0\end{pmatrix}\cdot\begin{pmatrix}1,0,\ldots,0\\0\\\vdots\quad R\\0\end{pmatrix}$$

$$=\begin{pmatrix}c_1,s_2,\ldots,s_n\\0\\\vdots\quad R^{-1}CR\\0\end{pmatrix}=\begin{pmatrix}c_1,s_2,\ldots,s_j,\ldots,s_n\\0\qquad\qquad\vdots\\\vdots\qquad\qquad c_m\\0\end{pmatrix}:=F\,.$$

[1] Der Leser beachte hier und im folgenden, dass in einer oberen Dreiecksmatrix stets in der Diagonalen die EWe dieser Matrix stehen und dass die EWe von C auch solche von A sind.

Diese Matrix F ist ähnlich zu A, vermittelt ϕ bezüglich einer geeigneten Basis $(\mathfrak{y}_1, \ldots, \mathfrak{y}_n)$ und enthält als obere Dreiecksmatrix in der Diagonalen natürlich lauter EWe. Somit brauchen wir nur noch die erste Zeile entsprechend unserer Zielsetzung „abzuräumen".

Hierzu nehmen wir an, es seien die Spalten 1 bis $j-1$ bereits wunschgemäß umgeformt. Dann betrachten wir die Spalte j. Hier gilt nach Konstruktion von F zu ϕ zunächst o. B. d. A. $c_m \neq c_1$, da B_1 schon der angestrebten Umformung entspricht, und

$$\phi\mathfrak{y}_j = s_j\mathfrak{y}_1 + \mathfrak{a} + c_m\mathfrak{y}_j,$$

also für jedes $t \in \mathbf{C}$

$$\phi(\mathfrak{y}_j + t\mathfrak{y}_1) = s_j\mathfrak{y}_1 + \mathfrak{a} + c_m\mathfrak{y}_j + tc_1\mathfrak{y}_1.$$

erfüllt ist.

Wir setzen nun $\phi(\mathfrak{y}_j + t\mathfrak{y}_1) \doteq \mathfrak{a} + c_m(\mathfrak{y}_j + t\mathfrak{y}_1)$,

also $s_j\mathfrak{y}_1 + \mathfrak{a} + c_m\mathfrak{y}_j + tc_1\mathfrak{y}_1 \doteq \mathfrak{a} + c_m\mathfrak{y}_j + c_mt\mathfrak{y}_1$,

also $s_j + t(c_1 - c_m) \doteq 0$.

Dies ist der Fall für $t = s_j/(c_m - c_1)$, beachte $c_1 \neq c_m$.

Somit liefert Ersetzung von $\mathfrak{y}_j$ durch $\mathfrak{y}_j + t\mathfrak{y}_1$ mit $t = s_j/(c_m - c_1)$ eine neue Basis, derart, dass die korrespondierende Matrix auch in Spalte j unserer Bedingung genügt.

Daher können wir sukzessive fortfahren, bis wir zu einer Matrix gelangen, die den Bedingungen des Satzes genügt und ähnlich ist zu A. □

Augrund von 7.0.4 und 7.0.3 können wir uns im weiteren auf das Studium von Blockmatrizen des Typs

$$A = \begin{pmatrix} c_i & \cdots & \cdots & \cdots & \\ & \ddots & & & \vdots \\ & & & & \vdots \\ & & & \ddots & \vdots \\ \mathrm{O} & & & & c_i \end{pmatrix} \qquad (c_i \text{ EW zu } \phi)$$

beschränken. Sei also T eine obere Dreiecksmatrix. Dann bezeichnen wir die Matrix $T - cE$ mit T^- und haben somit

$$T = T^- + cE$$

mit oberer Dreiecksmatrix T^- vom Typ $d_{ii} = 0$. Dies liefert weiter *geradeaus*

$$T^{-n} = (T - cE)^n = 0.$$

Deshalb können wir uns auf nilpotente Blockmatrizen des angegebenen Typs beschränken, denn man beachte

$$\begin{aligned} A &= S^{-1} \cdot T^- \cdot S \\ &\Rightarrow \\ A + cE &= S^{-1} \cdot T^- \cdot S + cE \\ &= S^{-1} \cdot T^- \cdot S + S^{-1} \cdot cE \cdot S \\ &= S^{-1} \cdot (T^- + cE) \cdot S\,, \\ &= S^{-1} \cdot T \cdot S\,, \end{aligned}$$

und dies bedeutet, dass eine „günstige" Darstellung von T^- zugleich eine solche für die Matrix $A = T^- + cE$ mitliefert.

Ziel unserer weiteren Bemühungen wird es sein, zu zeigen, dass jede Matrix A von der **Höhe** m, d. h. mit $A^m = 0 \neq A^{m-1}$ $(\exists m \geq 2)$ ähnlich ist zu einer Matrix, deren obere Nebendiagonale belegt ist mit Einsen, während alle übrigen Felder belegt sind mit 0, wofür wir auch sagen werden, es lasse sich A **jordanisieren** .

Um diesen Prozess überschaubar zu halten, arbeiten wir paradigmatisch, d. h. wir beschränken uns auf ein konkretes m, im folgenden auf $m = 5$, also $m - 1 = 4$, wobei aber die wesentlichen Ideen deutlich werden,

7. 0. 5 Proposition. *Sei ϕ ein Endomorphismus $\mathbf{X} \longmapsto \mathbf{X}$ mit $\phi^5 = 0 \neq \phi^4$.*

BEWEIS. Wir wählen eine Basis zu $\phi^4\mathbf{X}$, etwa $(\phi^4\,\mathfrak{x}_1, \ldots, \phi^4\,\mathfrak{x}_r)$. Dann ist die Menge der Vektoren

$$\phi^4\,\mathfrak{x}_1, \ldots, \phi^4\,\mathfrak{x}_r$$

$$\phi^3\,\mathfrak{x}_1, \ldots, \phi^3\,\mathfrak{x}_r$$

$$\phi^2\,\mathfrak{x}_1, \ldots, \phi^2\,\mathfrak{x}_r$$

$$\phi^1\,\mathfrak{x}_1, \ldots, \phi^1\,\mathfrak{x}_r$$

$$\phi^0\,\mathfrak{x}_1, \ldots, \phi^0\,\mathfrak{x}_r$$

linear unabhängig. DENN: Ist eine Linearkombination über dieser Menge gegeben, so können wir durch Anwendung des Operators $\phi^k \;\; (k = 4, 3, 2, 1)$ sukzessive zeigen, dass die Koeffizienten von $\mathfrak{x}_1, \ldots, \mathfrak{x}_r$ bzw. $\phi\,\mathfrak{x}_1, \ldots, \phi\,x_r$ bzw. ... bzw. $\phi^3\,\mathfrak{x}_1, \ldots, \phi^3\,\mathfrak{x}_r$ verschwinden.

Als nächstes erinnern wir an den Dimensionssatz:

$$\dim(\ker\phi) + \dim(\mathrm{im}\phi) = \dim\mathbf{X}\ .$$

Aufgrund dieses Satzes können wir durch Ergänzung von $\phi^4\,\mathfrak{x}_1, \ldots, \phi^4\,\mathfrak{x}_r$ zu einer Basis von $\ker(\phi)(\phi^3\mathbf{X})$ den Anteil

$$\phi^3\mathfrak{x}_1, \ldots, \phi^3\mathfrak{x}_r, \;\; \phi^4\mathfrak{x}_1, \ldots, \phi^4\mathfrak{x}_r$$

zu einer Basis von $\phi^3(\mathbf{X})$ ausdehnen. Denn, man beachte:

Nach Ergänzung von $\phi^4\,\mathfrak{x}_1, \ldots, \phi^4\,\mathfrak{x}_r$ zu einer Basis des Kerns von ϕ bezogen auf $(\phi^4\mathbf{X})$ ist nach dem Dimensionssatz die Anzahl der Vektoren dieser Basis vereint mit $\{\phi^3\mathfrak{x}_1, \ldots, \phi^3\mathfrak{x}_r\}$ gleich der Dimension von $\phi^3\mathbf{X}$, und es ist darüber hinaus auch die Menge all dieser Vektoren ℓu, da wir andernfalls wie oben durch Anwendung des Operators ϕ einen Widerspruch herleiten könnten.

Dies ist der eigentliche Schlüssel:

DENN: Die Basisergänzung in $\phi^3\,\mathbf{X}$ besteht aus Elementen des Typs $\phi^3\,\mathfrak{y}_1$, $\ldots, \phi^3\,\mathfrak{y}_s$. Die einzelnen Vektoren dieser Ergänzung können nämlich nicht aus $\phi^4\,\mathbf{X}$ sein, sind aber nach Konstruktion aus $\phi^3\,\mathbf{X}$. Somit sind die Vektoren $\mathfrak{y}_1, \ldots, \mathfrak{y}_s$ aus $\mathfrak{X}\backslash\phi\,\mathfrak{X}$, und man bestätigt wie oben, dass die Menge der Vektoren

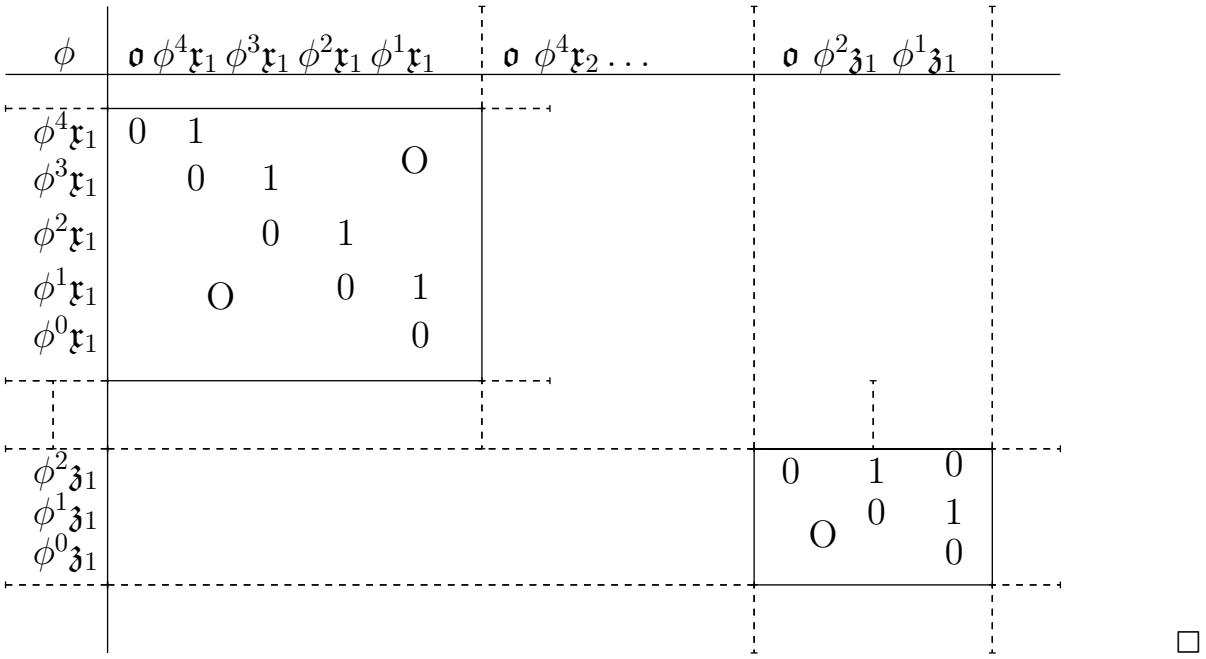
$$\begin{array}{l}
\phi^4\,\mathfrak{x}_1, \ldots, \phi^4\,\mathfrak{x}_r \\
\phi^3\,\mathfrak{x}_1, \ldots, \phi^3\,\mathfrak{x}_r, \;\; \phi^3\,\mathfrak{y}_1, \ldots, \phi^3\,\mathfrak{y}_t \\
\qquad\vdots \\
\qquad\vdots \\
\phi^0\,\mathfrak{x}_1, \ldots, \phi^0\,\mathfrak{x}_r, \;\; \phi^0\,\mathfrak{y}_1, \ldots, \phi^0\,\mathfrak{y}_s
\end{array}$$

ℓu ist, denn es ist ja jede „Zeilenmenge" $\{\phi^k \cdots\}$ ℓu, da andernfalls auch $\{\phi^3 \cdots\}$ ℓa wäre, man bemühe den Operator ϕ^{4-k}. Somit liefert Fortsetzung unseres Verfahrens nach n, in unserem Fall also nach 5 Schritten eine Basis

zu $\mathbf{X}$ vom Typ

$$\begin{array}{rrrrrrrrr}
\phi^4\,\mathfrak{x}_1, & \phi^3\,\mathfrak{x}_1, & \phi^2\,\mathfrak{x}_1, & \phi^1\,\mathfrak{x}_1, & \phi^0\,\mathfrak{x}_1, & \ldots, & \phi^4\,\mathfrak{x}_r, & \phi^3\,\mathfrak{x}_r, \ldots, & \phi^0\,\mathfrak{x}_r \\
\phi^3\,\mathfrak{y}_1, & \phi^2\,\mathfrak{y}_1, & \phi^1\,\mathfrak{y}_1, & \phi^0\,\mathfrak{y}_1, & \ldots, & \phi^3\,\mathfrak{y}_s, & \phi^2\,\mathfrak{y}_s, & \ldots, & \phi^0\,\mathfrak{y}_s \\
\phi^2\,\mathfrak{z}_1, & \phi^1\,\mathfrak{z}_1, & \phi^0\,\mathfrak{z}_1, & \ldots, & \phi^2\,\mathfrak{z}_t, & \phi^1\,\mathfrak{z}_t, \ldots, & \phi^0\,\mathfrak{z}_t\,, & & \\
\ddots & & \ddots & & \ddots & & \ddots & &
\end{array}$$

Und hieraus ergibt sich für ϕ als eine der darstellenden Matrizen:



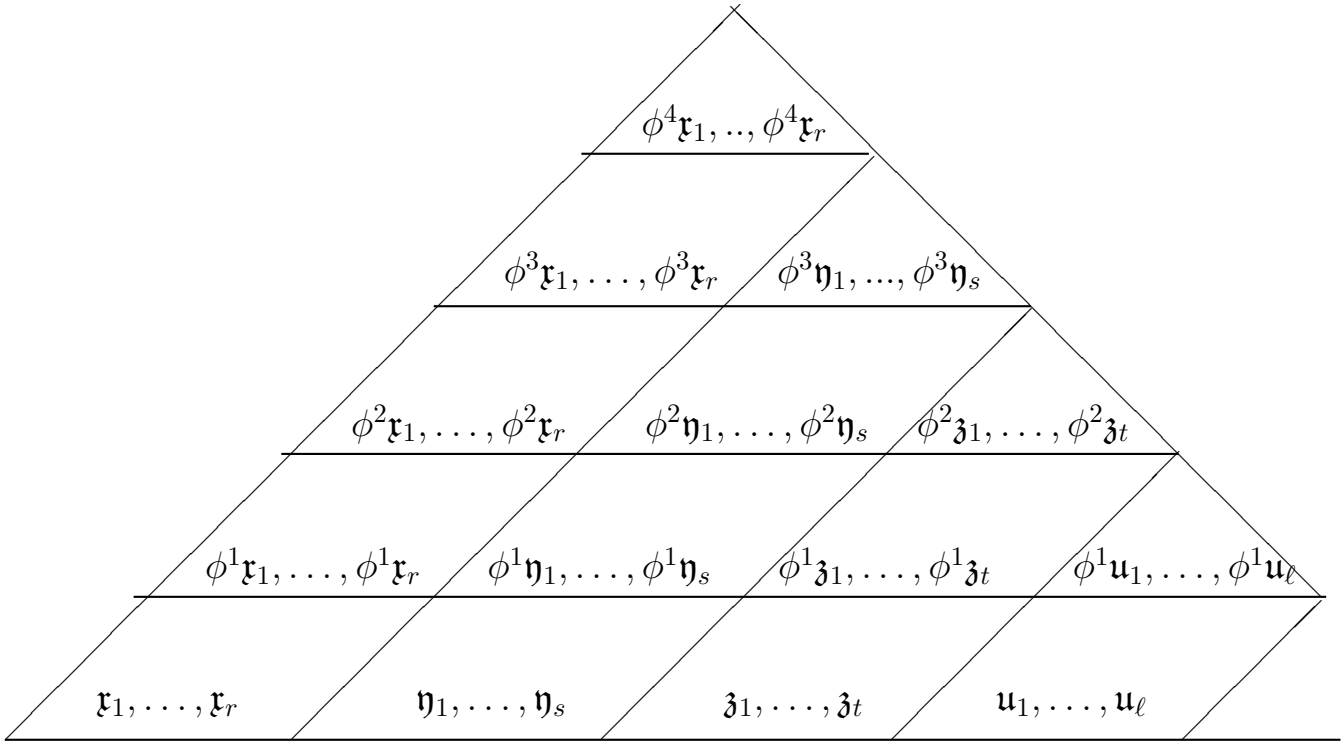
□

Es ist unser nächstes Ziel, die Anzahl der Blöcke in Abhängigkeit vom Rang gewisser Matrizen zu bestimmen. Dies leistet

7. 0. 6 Proposition. *Sei ϕ ein nilpotenter Endomorphismus des $\mathbf{C}^n$ und m die erste natürliche Zahl mit $\phi^m = 0$. Dann besitzt die Matrixdarstellung von ϕ bezüglich einer geeigneten Basis* **Jordansche Normalform**. *Dabei ist die Anzahl der Jordanblöcke vom Typ $k \times k$ $(0 \leq k \leq m)$ gleich*

$$B(k) = \operatorname{rg}(\phi^{k-1}) - 2 \cdot \operatorname{rg}(\phi^k) + \operatorname{rg}(\phi^{k+1})$$

DENN: ist $m = 1$, so ist dies evident, in jedem anderen Falle aber resultiert unsere Behauptung exemplarisch aus der nachfolgenden Pyramide, man betrachte sie etwa für $k = 3$.



$$\begin{array}{lll} & \nearrow & \\ \text{Anzahl der} & 3\times 3: & \operatorname{rg}(\phi^2) - 2\cdot\operatorname{rg}(\phi^3) + \operatorname{rg}(\phi^4), \\ \text{Blöcke vom Typ:} & k\times k: & \operatorname{rg}(\phi^{k-1}) - 2\cdot\operatorname{rg}(\phi^k) + \operatorname{rg}(\phi^{k+1}). \end{array}$$

□

Hiernach ist es leicht, eine Jordanform zu einer nilpotenten Matrix A zu konstruieren. Damit können wir dann aber auch jedes B_i aus 7.0.4 jordanisieren, wobei sich jeder Schritt erübrigt, wenn $B_i = B_i^-$ erfüllt ist, also $B_i^{-1} = O$ erfüllt ist bzw. – gleichbedeutend hiermit – B_i Diagonalgestalt hat.

Weiter ist es aufgrund von $B(k)$ und eines fast trivialen Lemmas auch nicht komplizierter, die Jordanform zu einem beliebigen A herzuleiten, dessen EWe bekannt sind. Denn, da man A nach 7.0.4 als trianguliert annehmen darf, gilt allgemein:

7. 0. 7 Das Jordanisierungstheorem. *Sei A eine komplexe Matrix. Dann besitzt A eine Darstellung $A = S^{-1}BS$ mit einer Dreiecksmatrix B, gebildet aus Jordanblöcken vom Typ*

$$\begin{pmatrix} c_i & 1 & & & \\ & c_i & 1 & & \\ & & \ddots & \ddots & 1 \\ & & & & c_i \end{pmatrix},$$

in denen jeweils

$$B(k) = \operatorname{rg}(B_i - c_iE)^{k-1} - 2 \cdot \operatorname{rg}(B_i - c_iE)^k + \operatorname{rg}\,(B_i - c_iE)^{k+1}$$

viele Blöcke vom Typ $k \times k$ mit EW c_i auftreten, worin k jeweils zwischen 0 und der Höhe von B_i^- liegt. [2)]

Wir werden nun zeigen, dass wir erst gar nicht auf die Matrizen B_i, die ja das Ergebnis einer Triangulierung sind, zurückzugreifen brauchen. Das wird dann einen „Arbeitsgang" einsparen.

Erinnern wir uns: Sind A und B ähnlich, so vermitteln sie bezüglich geeignet gewählter Basen denselben Endomorphismus ϕ und dies gilt dann natürlich auch für ihre Potenzen. Es gilt also $\operatorname{rg}(A^k) = \operatorname{rg}(B^k)$ $(\forall k \in \mathbb{N})$.

Weiter sind mit A und B auch $a - cE$ und $B - cE$ ähnlich wegen

$$\begin{aligned} A = S^{-1}BS \Longrightarrow A - cE &= S^{-1}BS - cE \\ &= S^{-1}BS - S^{-1}cES \\ &= S^{-1}(B - cE)S\ . \end{aligned}$$

Folglich haben wir vorweg:

$$\operatorname{rg}(B - c_iE)^k = \operatorname{rg}(A - c_iE)^k .$$

Nun ist aber für B aus 7.0.4 $B - c_iE$ eine Dreiecksmatrix, in deren Diagonalen außer im Bereich $B_i - c_iE$ lauter Werte $c_j - c_i \neq 0$ und in deren Bereich $B_i - c_iE$ lauter Nullen stehen, und man erkennt sofort, dass der

[2)] Man beachte, dass hier auch der Fall berücksichtigt wird, in dem B_i eine Diagonalmatrix ist, B_i^* also die Ordnung 0 hat.

Rang einer Blockmatrix gleich der Summe der Ränge der Blöcke ist. Das führt uns weiter zu

$$\operatorname{rg}(B - c_i E) = \operatorname{rg}(B_i - c_i E) + \sum_{j \neq i} \operatorname{rg}(B_j - c_i E)$$

und damit wegen der Regularität der Blöcke $B_j - c_i E$ $(j \neq i)$ im Falle er algebraischen Ordnung m_i von c_i zu $\operatorname{rg}(B_j - c_i E)^k = \operatorname{rg}(B_j - c_i E) = m_i$ $(j \neq i)$, also zu

$$\operatorname{rg}(B - c_i E)^k = \operatorname{rg}(B_i - c_i E)^k + \sum_{j \neq i} \operatorname{rg}(B_j - c_i E)^k$$

bzw. zu

$$\operatorname{rg}(B_i - c_i E)^k = \operatorname{rg}(B - c_i E)^k - (n - m_i).$$

Das bedeutet dann für die Blockzahlen

$$\begin{aligned}
& B(i,k) \\
= \;& \operatorname{rg}(B_i - c_i E)^{k-1} - 2 \cdot \operatorname{rg}(B_i - c_i E)^k + \operatorname{rg}(B_i - c_i E)^{k+1} \\
= \;& \operatorname{rg}(B - c_i E)^{k-1} - (n - m_i) \\
& - 2 \cdot \operatorname{rg}(B - c_i E)^k + 2 \cdot (n - m_i) \\
& + \operatorname{rg}(B - c_i E)^{k+1} - (n - m_i) \\
= \;& \operatorname{rg}(A - c_i E)^{k-1} - 2 \cdot \operatorname{rg}(A - c_i E)^k + \operatorname{rg}(A - c_i E)^{k+1}.
\end{aligned}$$

Folglich lässt sich zu jeder beliebigen Ausgangsmatrix nach Ermittelung ihrer EWe c_i und deren Ordnung $\operatorname{ord}(c_i)$ im charakteristischen Polynom eine Jordanform unter ausschließlicher Berechnung von Rangwerten zu den Matrizen $(A - c_i E)^k$ $(0 \leq k \leq \operatorname{ord}(c_i))$ gewinnen.

Kapitel 8

Quadratische Formen

Bisher wurden hauptsächlich lineare Gleichungen der Form

$$a_1\,x_1 + a_2\,x_2 + \ldots + a_n\,x_n = b$$

betrachtet. Die linke Seite

$$a_1\,x_1 + a_2\,x_2 + \ldots + a_n\,x_n$$

dieser Gleichung ist eine Funktion in n Unbekannten und wird als **Linearform** bezeichnet. Sie enthält weder Produkte noch Potenzen ihrer Variablen. Wir werden jetzt Funktionen untersuchen, in denen Quadrate und Produkte von Argumenten vorkommen. Solchen Funktionen begegnet man in vielen Anwendungen, etwa in der Geometrie, bei mechanischen Schwingungen, in der Statistik und Elektrotechnik" (Howard Anton).

Wir erinnern zunächst an die Untersuchung skalarer Produkte. Dort hatten wir die Schreibweise $X^\top AY$ eingeführt, sie soll hier als bekannt vorausgesetzt werden. Grundgegebenheit sei im folgenden stets ein euklidischer Raum $\mathbf{X}$.

8. 0. 8 Definition. Unter einer **quadratischen Form** verstehen wir jeden Ausdruck vom Typ

$$\sum_{i=1}^{n}\sum_{j=1}^{n} x_i \cdot a_{ij} \cdot x_j \;=:\; X^\top AX$$

mit einer $n \times 1$-Matrix X und einer symmetrischen Matrix A.

8. 0. 9 Definition. Eine quadratische Form heißt **nicht-negativ definit**, wenn sie ausschließlich nicht-negative Werte annimmt, sie heißt **positiv**

definit , wenn sie für nicht verschwindende Belegungen von X ausschließlich positive Werte annimmt.

Beispiele:

$$q(x_1, x_2) := x_1^2 - 18x_1x_2 + 5x_2^2 \tag{8.1}$$
$$= x_1^2 - 9x_1x_2 - 9x_2x_1 + 5x_2^2$$

hat die Matrix $\begin{pmatrix} 1 & -9 \\ -9 & 5 \end{pmatrix}$ und ist nicht nicht-negativ definit, wegen

$$q(1, 1) = -12\,.$$

$$q(x_1, x_2) := x_1^2 - 4x_1x_2 + 5x_2^2 \tag{8.2}$$

ist positiv definit, wegen

$$q(x_1, x_2) = (x_1 - 2x_2)^2 + x_2^2$$

$$q(x_1, x_2, x_3) = (x_1 - x_3)^2 + (x_2 - x_3)^2 \tag{8.3}$$
$$= x_1^2 + x_2^2 + 2x_3^2 - 2x_1x_3 - 2x_2x_3$$

ist nicht-negativ definit, nicht aber positiv definit, wegen

$$q(a, a, a) = 0. \tag{8.4}$$

für alle (a, a, a) .

8. 0. 10 Definition. Eine **symmetrische Matrix** heißt **nicht-negativ** bzw. **positiv definit**, wenn die assoziierte quadratische Form nicht-negativ bzw. positiv definit ist.

Es ist unser Ziel, quadratische Formen durch Transformation in überschaubarere Formen (also symmetrische Matrizen in überschaubarere symmetrische Matrizen) zu überführen, um auf diese Weise eine akzentuiertere Darstellung z. B. geometrischer oder physikalischer Sachverhalte zu ermöglichen.

8.1 Klassen quadratischer Formen

Sei $X^\top AX$ eine quadratische Form. Wir fragen nach der Auswirkung einer Basistransformation $X = PY$, das heißt, von

$$x_i \;=\; \sum_{k=1}^{n} p_{ik} \cdot y_k \qquad (1 \le i \le n).$$

Wegen $X^\top AX = (PY)^\top \cdot A \cdot (PY) = Y^\top (P^\top AP)Y = Y^\top BY$ wird $X^\top AX$ transformiert zu $Y^\top BY$ mit $B = P^\top AP$. Dabei gilt $B^\top = P^\top A^\top P = P^\top AP = B$, weshalb mit A auch B symmetrisch ist. Dies legt die folgende Erklärung nahe:

8. 1. 1 Definition. Zwei quadratische Formen $X^\top AX$ und $Y^\top BY$ heißen **äquivalent**, wenn es eine reguläre komplexe Matrix P gibt, mit $B = P^\top AP$.

Ist P zusätzlich sogar reell, so nennen wir die beiden Formen **reell äquivalent**, ist P darüber hinaus orthogonal, so nennen wir die beiden Formen **orthogonal äquivalent**.

Wie man leicht sieht, ist

$$A \sim B :\Longleftrightarrow B = P^\top AP \quad (P \text{ regulär})$$

in der Tat eine Äquivalenzrelation, man beachte $(PQ)^\top = Q^\top P^\top$ und

$(PP^{-1})^\top = (P^{-1})^\top \cdot P^\top = E \rightsquigarrow (P^{-1})^\top = (P^\top)^{-1}$ sowie $|\,AB\,| = |\,A\,|\,|\,B\,|$.

8. 1. 2 Proposition. *Zwei quadratische Formen $X^\top AX$ und $Y^\top BY$ sind genau dann orthogonal äquivalent, wenn ihre charakteristischen Polynome übereinstimmen.*

DENN: Nach Satz 6.4.12 lässt sich jedes symmetrische A mittels eines orthogonalen P diagonalisieren. Es gilt aber für orthogonale P insbesondere $P^\top = P^{-1}$. □

Damit erhalten wir als Korollar

8. 1. 3 Die Hauptachsentransformation. *Sind $c_1, \ldots, c_n$ die* EWe *von A, so ist die quadratische Form $X^\top AX$ orthogonal äquivalent zu der Form*

$$c_1 \cdot y_1^2 + \ldots + c_n \cdot y_n^2\,.$$

Mit anderen Worten: Eine quadratische Form kann noch so „wild" angelegt sein, es gibt eine orthogonale Matrix durch die sie in eine „ungemischte" Form überführt wird.

Unter den EWn von A gibt es natürlich $n - \operatorname{rg} A$ viele Nullen. Deshalb hat die oben vorgestellte Form effektiv „lediglich" die Länge $\operatorname{rg} A =: r \leq n$. Dies findet seine Ausprägung auch im nächsten Satz.

8. 1. 4 Proposition. *Jede quadratische Form $X^\top AX$ vom Rang $\operatorname{rg} A = r$ und p vielen (mehrfach gezählten) positiven (Eigen-) Werten ist reell äquivalent zu der Form*

$$y_1^2 + \ldots + y_p^2 - y_{p+1}^2 - \ldots - y_r^2 .$$

BEWEIS. Hat A den Rang r, so hat jede Diagonalform zu A genau r von 0 verschiedene EWe $c_1, \ldots, c_r$. Wir nehmen nun an, es seien $c_1, \ldots, c_p$ positiv und $c_{p+1}, \ldots, c_r$ negativ, und es sei P eine Orthogonalmatrix mit

$$P^\top AP = D = \begin{pmatrix} c_1 & & & & \\ & \ddots & & & \\ & & c_r & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix} .$$

Dann liefert die Diagonalmatrix Q mit

$$\begin{array}{rrcll} & q_{ii} & = & \frac{1}{\sqrt{c_i}} & (1 \leq i \leq p) , \\ & q_{jj} & = & \frac{1}{\sqrt{-c_j}} & (p+1 \leq j \leq r) , \\ \text{und} & q_{kk} & = & 1 & (r+1 \leq k \leq n) \end{array}$$

die Gleichung

$$B = (PQ)^\top A(PQ) = Q^\top DQ = \begin{pmatrix} E_p & & \\ & -E_{r-p} & \\ & & O_{n-r} \end{pmatrix} .$$

Es ist aber PQ regulär reell. Folglich ist $X^\top AX$ reell äquivalent zu

$$Y^\top BY = y_1^2 + \ldots + y_p^2 - y_{p+1}^2 - \ldots - y_r^2 .$$

□

Schließlich gilt im Blick auf reelle Äquivalenz:

8. 1. 5 Proposition. *Zwei quadratische Formen*

$$\begin{aligned} X^\top AX &= x_1^2 + \ldots + x_p^2 - x_{p+1}^2 - \ldots - x_r^2 \\ Y^\top BY &= y_1^2 + \ldots + y_q^2 - y_{q+1}^2 - \ldots - y_s^2 \end{aligned}$$

sind genau dann reell äquivalent, wenn $r = s$ und $p = q$ erfüllt ist.

BEWEIS. Gilt $r = s$ und $p = q$, so sind die beiden Formen *a fortiori* reell äquivalent, da A und B dann sogar gleich sind.

Seien hiernach $X^\top AX$ und $Y^\top BY$ reell äquivalent. Dann haben A und B den gleichen Rang, denn sie stimmen ja nach 8.1.4 überein in der Anzahl der EWe. Es stimmen A und B aber auch überein in der Anzahl der positiven EWe.

Hierzu gehen wir o. B. d. A. aus von $p < q$ und $B = P^\top AP$ mit $P = (p_{ik})$. Dann folgt:

$$Y^\top BY = (PY)^\top A(PY) = X^\top AX$$

mit $X = PY$, und wir können wegen $p < q$ reelle Werte $a_1, \ldots, a_n$ so wählen, dass die a_1 bis a_q nicht alle verschwinden und

$$\begin{aligned} p_{11} \cdot a_1 \;+\; p_{12} \cdot a_2 \;+\ldots+\; p_{1n} \cdot a_n &= 0 \\ \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \quad \vdots & \\ p_{p,1} \cdot a_1 \;+\; p_{p,2} \cdot a_2 \;+\ldots+\; p_{p,n} \cdot a_n &= 0 \\ a_{q+1} &= 0 \\ \vdots \quad \vdots & \\ a_n &= 0 \end{aligned}$$

erfüllen. Das liefert dann nach Einsetzen von $(\, a_1, \ldots, a_n \,)^\top$ für Y mit $b_i := \sum\limits_{k=1}^{n} p_{ik} \cdot a_k$ $(p+1 \le i \le r)$ auf der linken Seite nach Konstruktion

$$a_1^2 + \ldots + a_q^2 \,,$$

und auf der rechten Seite

$$-b_{p+1}^2 - \ldots - b_r^2 \;,$$

da ja die Werte a_{q+1} bis a_n verschwinden, also insgesamt den Widerspruch

$$0 < a_1^2 + \ldots + a_q^2 = -b_{p+1}^2 - \ldots - b_r^2 \le 0 \,.$$

Folglich ist auch $p = q$ erfüllt. □

Die Form aus 8.1.5 heißt auch die kanonische Form zu $X^\top AX$. Als unmittelbare Folgerungen aus resultieren aus den beiden letzten Sätzen

8. 1. 6 Korollar. *Zwei quadratische Formen sind genau dann reell äquivalent, wenn sie die gleiche kanonische Form haben.*

8. 1. 7 Korollar. *Zwei quadratische Formen sind genau dann reell äquivalent, wenn ihre Matrizen den gleichen Rang und die gleiche Anzahl positiver* EWe *haben.*

Demzufolge sind diese beiden Werte invariant gegenüber Transformationen vom Typ $X = PY$ mit regulärem P.

Endlich kommen wir zu

8. 1. 8 Proposition. *Jede quadratische Form $X^\top AX$ vom Rang* $\operatorname{rg} A = r$ *ist (komplex) äquivalent zu der Form*

$$y_1^2 + y_2^2 + \ldots + y_r^2 .$$

BEWEIS. Sei p die Zahl der (mehrfach gezählten) positiven EW von A. Wir wählen eine reguläre Matrix P, so dass $X^\top P^\top APX$ die reelle kanonische Form von $X^\top AX$ ist, also

$$P^\top AP = \begin{pmatrix} E_p & & \\ & -E_{r-p} & \\ & & O_{n-r} \end{pmatrix}$$

erfüllt ist. Dann erhalten wir mit der Diagonalmatrix

$$Q = \begin{pmatrix} E_p & & \\ & i \cdot E_{r-p} & \\ & & E_{n-r} \end{pmatrix}$$

die Beziehung

$$(PQ)^\top A(PQ) = Q^\top (P^\top AP)Q = \begin{pmatrix} E_r & O \\ O & O \end{pmatrix}.$$

Nun ist aber PQ regulär. Daher überführt $X = (PQ)Y$ die Form $X^\top AX$ nach

$$y_1^2 + \ldots + y_r^2 \,. \qquad \square$$

Die einzelnen Äquivalenzsätze haben gezeigt, was nicht anders zu erwarten war, nämlich:

Je schlichter die Transformation, umso eleganter die Form.

Rin Blick zurück: Theorie der quadratischen Formen ist Theorie der symmetrischen Matrizen. Insbesondere wird untersucht, wann zwei symmetrische Matrizen zueinander äquivalent sind im Sinne von

$$A = P^\top BP$$

mit regulärem P. Die große Bedeutung einer solchen Untersuchung liegt unter anderem darin, dass es gelingt, „kompliziertere" Formen auf dem Wege einer **Koordinatentransformation** zurückzuführen auf „überschaubarere" Formen.

Ein Beispiel: Man finde eine Transformation $X^\top PY$, welche die quadratische Form

$$x^2 + 2y^2 + 3z^2 + 4xy + 4yz$$

in ihre kanonische Form überführt.

Lösung: Wir gehen entlang des Beweises zu 8.1.4.

1. Schritt. Wir ermitteln die symmetrische Matrix A und erhalten

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 2 & 2 \\ 0 & 2 & 3 \end{pmatrix}.$$

2. Schritt. Wir ermitteln die EW zu A und erhalten

$$\mathrm{EW}_1 = 2, \quad \mathrm{EW}_2 = 5, \quad \mathrm{EW}_3 = -1 \,.$$

3. Schritt. Wir ermitteln als ein System paarweise orthogonaler EVn die Vektoren

$$\mathrm{EV}_1 = (2, 1, -2), \quad \mathrm{EV}_2 = (1, 2, 2), \quad \mathrm{EV}_3 = (2, -2, 1)$$

und normieren durch Multiplikation mit $\frac{1}{3}$.

4. Schritt. Wir notieren

$$P := \begin{array}{c} \begin{matrix} \text{EV}_1/3 & \ldots & \text{EV}_3/3 \end{matrix} \\ \begin{pmatrix} \frac{2}{3} & \frac{1}{3} & \frac{2}{3} \\ \frac{1}{3} & \frac{2}{3} & -\frac{2}{3} \\ -\frac{2}{3} & \frac{2}{3} & -\frac{1}{3} \end{pmatrix} \end{array}$$

5. Schritt. Wir bilden $P^\top AP = P^{-1}AP$ und erhalten

$$P^\top AP = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

6. Schritt. Wir bilden

$$Q = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & \frac{1}{\sqrt{5}} & 0 \\ 0 & 0 & \frac{1}{\sqrt{-(-1)}} \end{pmatrix}.$$

und erhalten

$$(PQ)^\top \cdot A \cdot (PQ) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

8.2 Zur Zerlegung quadratischer Formen

Es stellt sich die „natürliche Frage", wann eine quadratische Form das Produkt zweier linearer Formen darstellt, also zerlegbar ist. Hier erhalten wir:

8. 2. 1 Proposition. *Eine quadratische Form $X^\top AX$ ist Produkt zweier linearer Faktoren, mit Koeffizienten eventuell aus* $\mathbf{C}$*, gdw.* $\operatorname{rg} A \leq 2$ *erfüllt ist.*

BEWEIS. Sei zunächst

$$X^\top AX = (a_1x_1 + \ldots + a_nx_n)(b_1x_1 + \ldots + b_nx_n)\,.$$

Sind die beiden Faktoren ℓu, so dürfen wir – eventuell nach Permutation – annehmen, dass

$$\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \neq 0$$

erfüllt ist. Wir setzen nun

$$\begin{aligned} y_1 &:= a_1x_1 + a_2x_2 + \ldots + a_nx_n \\ y_2 &:= b_1x_1 + b_2x_2 + \ldots + b_nx_n \\ y_i &= x_i \ (3 \leq i \leq n) \end{aligned}$$

und beachten, dass hierdurch $Y = QX$ mit regulärem Q erfüllt ist, also

$$X = Q^{-1}Y.$$

Damit folgt:

$$\begin{aligned} X^\top AX &= (Q^{-1}Y)^\top A(Q^{-1}Y) \\ &= Y^\top((Q^{-1})^\top AQ^{-1})Y = y_1 \cdot y_2 \,. \end{aligned}$$

$y_1 \cdot y_2$ ist aber eine quadratische Form vom Rang 2, da die zugehörige Matrix die Gestalt

$$\begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix}$$

hat. Folglich gilt $\operatorname{rg} A \leq 2$ zumindest, wenn die beiden Faktoren y_1, y_2 voneinander ℓu sind.

Seien die obigen Faktoren nun ℓa. Dann dürfen wir annehmen, dass $a_1 \neq 0$ ist und dass

$$X^\top AX = k(a_1x_1 + \ldots + a_nx_n)^2$$

mit $k \neq 0$ erfüllt ist. Diesmal setzen wir

$$\begin{aligned} y_1 &:= a_1x_1 + \ldots + a_nx_n \\ y_i &:= x_i \ (2 \leq i \leq n) \end{aligned}$$

und sehen wie oben, dass $X^\top AX$ äquivalent ist zu der Form ky_1^2, die Rang 1 hat.

Da die Faktoren komplexe Koeffizienten aufweisen dürfen, sind die in Frage stehenden Matrizen allerdings nicht notwendig reell.

Habe nun umgekehrt $X^\top AX$ einen Rang kleiner als oder gleich 2.

Dann ist $X^\top AX$ äquivalent zu y_1^2 oder zu $y_1^2 + y_2^2$ mit regulärem P, und es sind y_1^2 wie auch $y_1^2 + y_2^2$ zerlegbar über $\mathfrak{C}$ – beachte

$$y_1^2 + y_2^2 = (y_1 + iy_2)(y_1 - iy_2)\,.$$

Daher erhalten wir eine Zerlegung von $X^\top AX$ auf dem Wege der Transformation $Y = P^{-1}X$. □

Ein Beispiel: Man zeige, dass die quadratische Form $5x_1^2+4x_3^2+4x_1x_2-12x_1x_3-8x_2x_3$ ein Produkt von linearen Faktoren ist und gebe diese Faktoren an.

Lösung: Die EWe sind $12, -3, 0$. Also zerfällt die Form. Die orthogonale Matrix, die A diagonalisiert, ist Q (wie oben). Daher transformiert $X = QY$ die Form $X^\top AX$ zu

$$\begin{aligned} X^\top AX &= (QY)^\top A(QY) \\ &= Y^\top (Q^\top AQ)Y \\ &= 12y_1^2 - 3y_2^2 \\ &= 3 \cdot (2y_1 + y_2)(2y_1 - y_2)\,. \end{aligned}$$

Nun gilt es, die y-Werte durch x-Werte auszudrücken. Wegen $Y = Q^\top X$ haben wir diesbezüglich

$$\begin{aligned} y_1 &= \tfrac{1}{3}(2x_1 + x_2 - 2x_3) \\ y_2 &= \tfrac{1}{3}(x_1 + 2x_2 + 2x_3) \end{aligned}$$

und

$$\begin{aligned} 2y_1 + y_2 &= \tfrac{1}{3}(5x_1 + 4x_2 - 2x_3) \\ 2y_1 - y_2 &= x_1 - 2x_3. \end{aligned}$$

Also erhalten wir:

$$X^\top AX = (5x_1 + 4x_2 - 2x_3) \cdot (x_1 - 2x_3).$$

8.3 Eine Anwendung auf die Geometrie

Die allgemeine Gleichung 2. Grades in den Unbestimmten x, y, z hat die Form

$$\begin{aligned}(*) \qquad & a \cdot x^2 \ + b \cdot y^2 \ + \ c \cdot z^2 \\ & + 2f \cdot xy \ + \ 2g \cdot yz \ + \ 2h \cdot zx \\ & + \ 2\ell \cdot x \ + \ 2m \cdot y \ + \ 2n \cdot z \ + \ d = 0\,.\end{aligned}$$

Einer Gleichung dieses Typs mit reellen Koeffizienten entspricht jeweils eine Punktmenge des $\mathbf{R^3}$, allgemein bezeichnet als Quadrik. Quadriken lassen sich offenbar umso leichter klassifizieren, je überschaubarer die repräsentierende Gleichung ist. Somit ist eine Reduktion von $(*)$ ein Anliegen der Geometrie (bzw. Physik). Geleistet werden kann dies in jedem Falle durch eine Rotation, eine Abbildung, die hier vorzustellen ist:

8. 3. 1 Definition. Ist $(\,\mathfrak{b}_1, \ldots, \mathfrak{b}_n\,)$ eine Basis des $\mathbf{R}^n$, so nennen wir $(\,\mathfrak{b}_1, \ldots, \mathfrak{b}_n\,)$ **positiv orientiert**, wenn die Determinante $|\,\mathfrak{b}_1, \ldots, \mathfrak{b}_n\,|$ einen positiven Wert annimmt, und dementsprechend **negativ orientiert**, wenn $|\,\mathfrak{b}_1, \ldots, \mathfrak{b}_n\,| < 0$ erfüllt ist.

Es folgt:

8. 3. 2 Proposition. *Zwei Basen* $(\,\mathfrak{a}_1, \ldots, \mathfrak{a}_n\,)$ *und* $(\,\mathfrak{b}_1, \ldots, \mathfrak{b}_n\,)$ *sind genau dann gleich orientiert, wenn die Überführungsmatrix* C *eine positive Determinante besitzt.*

BEWEIS. Überführt C die Vektoren $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ in ihre $\mathfrak{b}$-Darstellung, so gilt:

$$\mathfrak{a}_k = c_{1k}\mathfrak{b}_1 + c_{2k}\mathfrak{b}_2 + \ldots + c_{nk}\mathfrak{b}_n\ ,$$

also
$$a_{ki} = c_{1k}b_{1i} + c_{2k}b_{2i} + \ldots + c_{nk}b_{ni}.$$

und damit

$$A^\top = C^\top \cdot B \rightsquigarrow |\,A\,| = |\,A^\top\,| = |\,C^\top\,|\,|\,B\,| = |\,C\,|\,|\,B\,|\,. \qquad \square$$

8. 3. 3 Definition. Eine Transformation $PX = Y$ heißt eine **Rotation**, wenn P eine orthogonale Matrix mit positiver Determinante ist.

Natürlich sollte gesichert sein, dass die Rotation im abstrakten Sinn von 8.3.3, bezogen auf den klassischen Fall des $\mathbf{R^3}$, übereinstimmt mit der

Rotation im anschaulichen Sinn, das heißt, mit der starren Bewegung mit Fixpunkt 0. Dass dies so ist, lässt sich wie folgt einsehen:

Die Rotation im anschaulichen Sinne überführt das System der EVn stetig und längentreu in sein Bildsystem. Somit erfolgt diese Abbildung *via* einer orthogonalen Matrix P, deren Determinante positiv sein muss, da sich die Orientierung aufgrund der Stetigkeit der Determinantenfunktion nicht ändert.

Sei nun umgekehrt ϕ ein Automorphismus, vermittelt durch eine orthogonale Matrix P mit positiver Determinante. Dann geht $(\mathfrak{e}_1, \ldots, \mathfrak{e}_3)$ über in eine gleichorientierte Basis, und es bleiben alle Abstände starr, da P orthogonal ist.

Die große Bedeutung der Rotation basiert darauf, dass sie neben der Translation eine hochnatürliche Abbildung des $\mathbf{R^3}$ darstellt. Aus diesem Grunde interessiert selbstverständlich u. a. eine spezifische Darstellung ihrer Matrix.

Da die Matrix *per definitionem* orthogonal ist, hat sie eine Darstellung im Sinne von 6.4.9. Doch darüber hinaus sind wir in der Lage, die einzelnen Positionen alternativ noch wie folgt zu beschreiben:

8. 3. 4 Proposition. *Sei* $\mathbf{X}$ *ein euklidischer Raum und* ϕ *eine Rotation. Dann lässt sich* ϕ *bezüglich einer geeignet gewählten* ONB $(\mathfrak{e}_1, \ldots \mathfrak{e}_n)$ *vermitteln durch eine Matrix des Typs*

$$A = \begin{pmatrix} +1 & \ddots & & & & \\ & & -1 & \ddots & & \\ & & & & \boxed{\begin{matrix} \cos\alpha_\ell & \sin\alpha_\ell \\ -\sin\alpha_\ell & \cos\alpha_\ell \end{matrix}} & \\ & & & & & \ddots \end{pmatrix}.$$

BEWEIS. Nach 6.4.9 liegen alle EW auf dem Einheitskreis und werden daher eindeutig repräsentiert durch einen Winkel α_ℓ mit $0 \leq \alpha_\ell < 2\pi$. Dies liefert die Behauptung nach 6.2.9. □

Nach diesem Exkurs kehren wir zurück zur Bearbeitung von $(*)$:

Die Terme vom Grade 2 in $(*)$ bilden eine quadratische Form in x, y, z mit

der Matrix

$$\begin{pmatrix} a & f & h \\ f & b & g \\ h & g & c \end{pmatrix} =: H \ ,$$

und es hat dieses H wegen seiner Symmetrie ein Tripel paarweise orthogonaler EVn, das als orthonormal und positiv orientiert angenommen werden darf, etwa

$$\begin{aligned} \mathfrak{f}_1 &= (f_{11}, f_{21}, f_{31}) \sim f_{11}\mathfrak{e}_1 + f_{12}\mathfrak{e}_2 + f_{13}\mathfrak{e}_3 \\ \mathfrak{f}_2 &= (f_{21}, \dots \\ \mathfrak{f}_3 &= \end{aligned}$$

Wir wählen nun $\mathfrak{f}_1, \mathfrak{f}_2, \mathfrak{f}_3$ als neues Koordinatensystem.

Dann ist die Matrix des Übergangs von der $\mathfrak{f}$-Basis zur $\mathfrak{e}$-Basis gleich

$$\begin{pmatrix} f_{11} & f_{12} & f_{13} \\ f_{21} & f_{22} & f_{23} \\ f_{31} & f_{32} & f_{33} \end{pmatrix} =: P$$

und, da beide Basen orthonormal und gleichorientiert sind, repräsentiert P eine Rotation.

Seien hiernach (x, y, z) und (x', y', z') die Koordinatenvektoren desselben Punktes im $\mathfrak{e}$- bzw. $\mathfrak{f}$-System. Dann haben wir

$$(R) \qquad \begin{aligned} x &= f_{11}x' + f_{12}y' + f_{13}z' \\ y &= f_{21}x' + f_{22}y' + f_{23}z' \\ z &= f_{31}x' + f_{32}y' + f_{33}z' \, . \end{aligned}$$

Bezeichnen wir nun die zu (x, y, z) bzw. (x', y', z') korrespondierenden $n \times 1$-Matrizen mit X bzw. X', so erhalten wir in Matrizenschreibweise $PX' = X$, und es wird der quadratische Anteil von $(*)$ transformiert zu

$$\begin{aligned} (PX')^\top \cdot H \cdot (PX') &= X'^\top \cdot (P^\top H P) \cdot X' \\ &= X'^\top D X' \\ &= k_1 x'^{\,2} + k_2 y'^{\,2} + k_3 z'^{\,2} \, , \end{aligned}$$

worin $k_1, \ldots, k_3$ die EW von H sind und D eine Diagonalform von H darstellt.

Folglich überführt die Transformation (R) die linke Seite aus $(*)$ nach

$$(*,*) \quad k_1 \cdot x'^2 + k_2 \cdot y'^2 + k_3 \cdot z'^2 + 2\ell' \cdot x' + 2m' \cdot y' + 2n' \cdot z' + d = 0,$$

das heißt, es ist uns gelungen, die „gemischten" Glieder durch eine Rotation „verschwinden" zu lassen. Um die Form $(*,*)$ weiter zu vereinfachen, unterscheiden wir nun drei Fälle

1. Genau ein k_i ist verschieden von 0.
2. Genau zwei k_i sind verschieden von 0.
3. Genau drei k_i sind verschieden von 0.

FALL 1. Sei o. B. d. A. $k_1 \neq 0 = k_2 = k_3$.
Die Translationen

$$\begin{aligned} x'' &= x' + \ell'/k_1 \\ y'' &= y' \\ &= z', \end{aligned}$$

liefern

$$k_1 \cdot x''^2 + 2m' \cdot y'' + 2n' \cdot z'' + d' = 0.$$

FALL 2. Sei o. B. d. A. $k_1 \neq 0 \neq k_2$, $k_3 = 0$.
Die Translationen

$$\begin{aligned} x'' &= x' + \ell'/k_1 \\ y'' &= y' + m'/k_2 \\ z'' &= z \end{aligned}$$

liefern

$$k_1 \cdot x''^2 + k_2 \cdot y''^2 + 2n' \cdot z'' + d'' = 0.$$

ZU FALL 3. Sei $k_1 \neq 0 \neq k_2 \neq 0 \neq k_3$
Die Translationen

$$\begin{aligned} x'' &= x' + \ell'/k_1 \\ y'' &= y' + m'/k_1 \\ z'' &= z' + n'/k_1 \end{aligned}$$

liefern

$$k_1 \cdot x''^2 + k_2 \cdot y''^2 + k_3 \cdot z''^2 + d'' = 0.$$

Wie der Leser leicht erkennt, „verbleibt" in die dem $k_i \neq 0$ zugehörende Variable jeweils in zweiter Potenz, während die anderen Variablen nur noch in erster Potenz „verbleiben".

Division durch $k_1 \cdot k_2 \cdot k_3$ und anschließende Normierung des absoluten Gliedes führen zu weiterer Kanonisierung , wobei die Nenner jeweils als Quadrate geschrieben werden können.

Damit ist $(*, *)$ dann *via* **„Rotation und Translation"** in eine Darstellung überführt, welche die korrespondierenden Flächen einer Klassifizierung im Sinne der analytischen Geometrie zugänglich macht.

Ist irgendeine Quadrik gegeben, so können wir z gleich 0 setzen. Auf diese Weise erhalten wir die **Spur** der Quadrik .

Wie sich Quadriken geometrisch darstellen, findet der Leser etwa in dem empfehlenswerten Buch von Howard Anton: Lineare Algebra, Bibliothek der Universität Kassel.

Literaturverzeichnis

[1] Anton, H.: *Lineare Algebra, Einführung·Grundlagen·Übungen.* Spektrum, Akademischer Verlag, Heidelberg-Berlin-Oxford, 1995.

[2] Brieskorn, E., *Lineare Algebra und Analytische Gometrie.* Friedrich Vieweg, Braunschweig-Wiebaden, 1983.

[3] Kowalsky, H. J.: *Lineare Algebra.* 9., überarbeitete und erweiterte Auflage, Walter de Gruyter, Berlin-New York, 1979.

[4] Neuhaus/Kippels: *Lineare Algebra/Analytische Geometrie.* Institut der Mathematik an der Universität Köln, 1949.

[5] Schreier, O. / E. Sperner, *Analytische Geometrie.* Erster Band, Hamburger Mathematische Einzelschriften, 10. Heft, 1931.

[6] Schreier, O. / E. Sperner, *Analytische Geometrie.* Zweiter Band, Hamburger Mathematische Einzelschriften, 19. Heft, 1935.

Kapitel 9

A Singular Value Decomposition

Im Vordergrund dieser Vorlesung standen Strukturaspekte. In diesem Kapitel wenden wir uns der Numerik zu.

Zwei Fehler sind unvermeidbar, wollen wir Konkretes in Zahlen erfassen:

Zum einen können Messgeräte, und dazu gehört natürlich auch das Auge, bestenfalls nur extrem gute Näherungswerte liefern, zum anderen aber kann eine numerische Messung nur in begrenzter Stellenzahl, also gerundet protokolliert werden.

Wenngleich nun auch die Natur gnädig ist, sie lässt den Flieger nicht gleich vom Himmel stürzen, weil die Flatterrechnung „flattert"und sie lässt auch die Börse nicht gleich „[k](c)ra(s)[c]hen" wegen minimaler Kalkulationsfehler. Jedoch, es können sich Fehler zu verhängnisvollen Werten aufsummieren, davon zeugen Börsencrashs und Brückenkatastrophen.

Dies zu verhindern – soweit es denn geht – helfen Kalkulationen, sprich' hilft die Numerik.

Es mag ein glänzendes Gespür gewesen sein, das die Römer zu großartigen Brücken und Wasserläufen befähigt hat, siehe Pont Avén, stolz mögen die Kathedralen seit Jahrhunderten die Jahrhunderte überdauern. Doch, wo der Flieger fliegen soll, gilt:

Messen und Numerik vor allem!

Deshalb hier in einem Anhang ein wenig Numerik zum Schnuppern, entlang eines Primers von Sonia Leach zum Single-Value-Decomposition- (SVD)-Verfahren. Es wird z. B. eingesetzt bei der Deutschen Luft- und Raumfahrt-Gesellschaft (DLR)[1)] und ebenso bei der Deutschen Bundesbank (DBB)[2)].

[1)] Nach einem Hinweis von Dr. Johannes Bosbach

[2)] Nach einem Hinweis von Bundesbankdirektor Jörg Binder, dem der Autor auch die Übermittelung des vorgestellten Primers verdankt.

Singular Value Decomposition – A Primer

Sonia Leach
Department of Computer Science
Brown University Providence RI 02912
DRAFT VERSION

1 Introduction

The singular value decomposition (SVD) is a powerful technique in many matrix computations and analyses. Using the SVD of a matrix in computations rather than the original matrix has the advantage of being more robust to numerical error. Additionally, the SVD exposes the geometric structure of a matrix, an important aspect of many matrix calculations. A matrix can be described as a transformation from one vector space to another. The components of the SVD quantify the resulting change between the underlying geometry of those vector spaces.

The SVD is employed in a variety of applications, from least squares problems to solving systems of linear equations. Each of these applications exploit key properties of the SVD, its relation to the rank of a matrix and its ability to approximate matrices of a given rank. Many fundamental aspects of linear algebra rely on determining the rank of a matrix, making the SVD an important and widely-used technique. This primer serves as a short introduction to the SVD and its applications. More comprehensive coverage can be found in numerous references, such as [5, 3, 8]. Organization of the paper is as follows:

Section 2 introduces the definition of the SVD, followed by a discussion of the properties of the components of the SVD. Section 3 explores further properties of the SVD and provides a geometric interpretation of the singular values. Section 3 lists a number of interesting applications and Section 4 concludes the paper with a discussion of the advantages and disadvantages of using the SVD.

2 Definition of the SVD

In this section, we assume a familiarity with the basic terminology of linear algebra, and refer the reader to [1] for a more complete coverage. We restrict our attention to matrices of real numbers and refer the reader to [2] for a discussion of the SVD using complex numbers. This presentation is largely adapted from [4].

Using the superscript T to denote the transpose of a vector or matrix, we say two vectors $\mathfrak{x}$ and $\mathfrak{y}$ are orthogonal if $\mathfrak{x}^T\mathfrak{y} = 0$. In a two or three dimensional space, this simply means that the vectors are perpendicular.

Let A be a square matrix such that its columns are mutually orthogonal vectors of length 1 i. e. $\mathfrak{x}^T\mathfrak{x} = 1$. Then A is an orthogonal matrix and $ATA = I$, the identity matrix. To simplify the notation, assume that a matrix A has at least as many rows as columns $M \geq N$.

A **singular value decomposition** of an $M \times N$ matrix A is any factorization of the form

$$A = U\Sigma TV^T$$

where U is an $M \times M$ orthogonal matrix, V is an $N \times N$ orthogonal matrix, and Σ is an $M \times N$ diagonal matrix with $s_{ij} = 0$ if $i \neq j$ and $s_{ii} = si \geq 0$. Furthermore, it can be shown that there exist non unique matrices U and V such that $s_1 \geq s_2 \geq ... \geq s_N \geq 0$ [5]. Henceforth we will assume the SVD has such a property. The quantities s_i are called the **singular values** of A, and the columns of U and V are called the left and right **singular vectors**, respectively.

For example, the matrix

$$A = \begin{pmatrix} 0.96 & 1.72 \\ 2.28 & 0.96 \end{pmatrix}$$

has the SVD

$$A = U\Sigma V^T = \begin{pmatrix} 0.6 & -0.8 \\ 0.8 & 0.6 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0.8 & 0.6 \\ 0.6 & -0.8 \end{pmatrix}$$

We see that the columns of U and V are of unit length since $(0.6)^2+(0.8)^2 = 1$ and a simple calculation of dot products will show them to be mutually orthogonal. From the components of the SVD we can determine many

properties of the original matrix. The **null space** of a matrix A is the set of $\mathfrak{x}$ for which $A\mathfrak{x} = \mathfrak{o}$, and the **range** of A is the set of $\mathfrak{b}$ for which $A\mathfrak{x} = \mathfrak{b}$ has a solution for $\mathfrak{x}$. Let u_j and v_j be the columns of U and V respectively. Then the decomposition of $A = U\Sigma V^T$ can be written as

$$Av_j = s_j u_j, j = 1, 2, ..., N$$

If $s_j = 0$ then $Av_j = 0$ and v_j is in the null space of A, whereas if $s_j \neq 0$ then u_j is in the range of A. Consequently, we can construct bases for various vector subspaces defined by A. A set of vectors $v_1, v_2, ..., v_k$ in a vector space $\mathcal{V}$ is said to form a **basis** for $\mathcal{V}$ if every vector $\in \mathfrak{V}$ can be expressed as a linear combination of them in exactly one way. Let V_0 be the set of columns v_j for which $s_j = 0$ and let V_1 be the remaining columns v_j. Similarly, let U_1 be the set of columns u_j for which $s_j \neq 0$ and let U_0 be the remaining columns u_j, including those with $j > n$. Thus, if k is the number of non-zero singular values, there are k columns in V_0, $N - k$ columns in V_1, and U_1, and $M - N + k$ columns in U_0. Each of these sets forms a basis for the vector subspaces of A.

1. V_0 is an orthonormal basis for $Nullspace(A)$.

2. V_1 is an orthonormal basis for the orthogonal complement of $Nullspace$ (A).

3. U_1 is an orthonormal basis for $Range(A)$.

4. U_0 is an orthonormal basis for the orthogonal complement of $Range(A)$.

As we shall see in the next two sections, the singular values of A can be used in many other ways to determine properties of A, as well as to partition the M-dimensional vector space (of the mapping defined by A) into dominant and sub-dominant subspaces.

3 Properties of the SVD

3.1 SVD and Matrix Norms

Often when speaking about vectors and matrices, we are interested in the lengths of the vectors and the resulting length of a vector when multiplied by a matrix. A familiar concept of length in two dimensions is the Euclidean distance from the origin to the point specified by the coordinates of the

vector x_1, x_2. This distance is calculated by the formula $({x_1}^2 + {x_2}^2)^{\frac{1}{2}}$. In the general case of N dimensions the length or norm of a vector $\mathfrak{x}$ is defined by

$$\|\mathfrak{x}\| := ({x_1}^2 + {x_2}^2 + ... + {x_N}^2)^{\frac{1}{2}} = (\mathfrak{x}^T\mathfrak{x})^{\frac{1}{2}}$$

When a vector $\mathfrak{x}$ is multiplied by a matrix A the length of the resulting vector $A\mathfrak{x}$ changes according to the matrix A. If A is orthogonal, the length is preserved. Otherwise, the quantity $\frac{\|A\mathfrak{x}\|}{\|\mathfrak{x}\|}$ measures how much A *stretches* $\mathfrak{x}$. Thus calculating the norm of a matrix intuitively means finding the maximum stretch factor. If the SVD of a matrix is given, this computation is simplified. The Euclidean norm of a matrix, sometimes referred to as the L_2 norm, is defined as follows. Let $\mathfrak{x}$ be an N-dimensional vector, and A be an $M \times N$ matrix, then

$$\|A\|_E = \max_{\|x\|=1} \left\{ \frac{\|A\mathfrak{x}\|}{\|\mathfrak{x}\|} \right\}$$

An alternative norm for A is the Frobenius norm, which is the Euclidean norm of a vector constructed by stacking the columns of A in one $M * N$ vector. The Frobenius norm is then

$$\|A\|_F = \left(\sum_{i=1}^{m} \sum_{j=1}^{n} |a_{ij}|^2 \right)^{\frac{1}{2}}$$

Given the SVD of a matrix A, these norms can easily be computed. Proofs of the following facts are given in [5], [2]. Let $U\Sigma TV^T$ be the SVD of $M \times N$ matrix A, where $\{a_1, s_2, ..., s_k\}$ are the non-zero singular values in Σ. Then

$$\|A\|_E = s_1$$

$$\|A\|_F = \left(\sum_{l=1}^{k} {s_k}^2 \right)^{\frac{1}{2}}$$

To return to an earlier notion, we mentioned that multiplying a vector $\mathfrak{x}$ by a matrix A effectively stretches the vector. This geometric interpretation can be viewed more clearly in terms of the singular values of A. The set of vectors $\mathfrak{x}$ of length N for which $\|x\| = 1$ defines a unit circle. Multiplication of these vectors by the $M \times N$ matrix A results in a set of M-dimensional vectors $\mathfrak{b} = A\mathfrak{x}$ with varying lengths. Geometrically, this set defines a k-dimensional ellipsoid embedded in an M-dimensional space, where k is the

number of non-zero singular values. Figure 1 depicts the situation when $M = N = k = 2$. The lengths of the axes of the ellipsoid are the singular values of A, and in the general case, the major and minor axes are given by s_{max} and s_{min} respectively. Intuitively, the singular values of a matrix describe the extent to which multiplication by the matrix distorts the original vector. The magnitude of the singular values can be used to highlight which dimensions of the vector are most affected, and in some sense more important, as we shall see next in the discussion of SVD applications.

3.2 SVD and Matrix Rank

Fundamental to linear algebra is the notion of rank. Numerous theorems begin with the condition "If matrix A is of full rank, then the following property holds". However, if the matrix is rank deficient(or nearly so), then small perturbations of the matrix values (from round-off errors or fuzzy data), will yield a matrix which is of full rank. Hence, determining the rank of a matrix is non-trivial. The SVD lends us a practical definition of rank, as well as allows us to quantify the notion of near rank deficiency. The familiar definition of rank is the number of linearly independent columns of a matrix. Let the matrix A have the SVD

$$A = U\Sigma TV^T .$$

Since multiplication by orthogonal matrices preserves linear independence, the rank of A is precisely the rank of the diagonal matrix Σ or equivalently, the number of non-zero singular values. If A is nearly rank deficient (singular) then the singular values will be small. Moreover, suppose that $Rank(A) = m$ and we wish to approximate A by a matrix B of lower rank k. Then we can use the singular values of A to compute a matrix with the best approximation, and to determine if the approximation is unique. Let s_i be the diagonal entries of Σ and let u_i and v_i be the column vectors of U and V respectively. Then

$$\min_{Rank(B)=k} \|A - B\|_E = \|A - A_k\|_E = s_{k+1}$$

where $A_k \sum_{i=1}^{k} s_i u_i v_i^T$. The solution BA_k will be unique when $s_{k+1} < s_k$. Proofs of these facts can be found in [2], [5]. We see then that the SVD of A produces a sequence of approximations to A of successive ranks $A_i =$

$U\Sigma_i V^T$, where Σ_i is the rank i version of Σ obtained by setting the last $m-i$ singular values to zero. Also, A_i is the best rank i approximation to A in the sense of Euclidean distance. The use of SVD for matrix approximation has a number of practical advantages. First, applications which encounter round-off errors or fuzzy data typically use the effective rank of a matrix, i.e. the number of singular values greater than some ε, where ε reflects the accuracy of the data. Hence, decisions are made only about the negligibility of a few singular values, rather than vectors or sets of vectors. Second, storing the approximation of a matrix often results in a significant savings over storing the whole matrix. Note that we can express a matrix A as

$$A = s_1 u_1 {v_1}^T + s_2 u_2 {v_2}^T + ... + s_m u_m {v_m}^T .$$

Each outer product $u_i {v_i}^T$ is a simple matrix of rank 1, and can be stored in $M \times N$ numbers, versus $M \times N$ of the original matrix. Additionally, multiplication of $u_i v_i^T$ with a vector x requires only $M \times N$ operations, instead of $M * N$ [4].

3.2 SVD and Linear Independence

Another use of the SVD provides a measure, called a condition number, which is related to the measure of linear independence between the column vectors of the matrix. The condition number (with respect to the Euclidean norm) of a matrix A is

$$cond(A) = \frac{s_{max}}{s_{min}}$$

where s_{max} and s_{min} are the largest and smallest singular values of A. If A is rank deficient, then $s_i = 0$ and we consider $cond(A) = \infty$. Using the condition number, we can quantify the independence of the columns of A. Note that $cond(A) \geq 1$. If $cond(A)$ is close to 1, then the columns of A are very independent. When the condition number is large, the columns of A are nearly dependent. Returning to the geometric interpretation of singular values, we see that the condition number is related to the axes of the hyper-ellipsoid associated with the matrix. Since $cond(A)$ is defined by the extreme singular values and these values are the lengths of the major and minor axes, the condition number describes the eccentricity of the hyper-ellipsoid. As we will see in the next section, the notion of a condition number becomes important in solving linear systems, where

$cond(A)$ in some sense measures the sensitivity of the system to noise in the data.

4 Applications of SVD

4.1 Solutions to Linear Equations

Numerous practical problems can be expressed in the language of linear algebra. A linear system involves a set of equations in N variables. For example consider the following linear system

$$\begin{aligned} x_1 &+ 2\,x_2 &+ x_3 &= 8 \\ 10\,x_1 &+ +18\,x_2 &+ 12\,x_3 &= 78 \\ 20\,x_1 &+ 22\,x_2 &+ 40\,x_3 &= 144c \end{aligned}$$

This problem can be expressed in terms of a coefficient matrix A, a vector $\mathfrak{x}$ of variables, and a vector $\mathfrak{b}$, such that a solution to the linear system $A\mathfrak{x} = \mathfrak{b}$ is an assignment to the values of the vector x. For the above example $A, \mathfrak{x}$, and $\mathfrak{b}$ are

$$A\mathfrak{x} = \begin{pmatrix} 1 & 2 & 1 \\ 10 & 18 & 12 \\ 20 & 22 & 40 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 8 \\ 78 \\ 144 \end{pmatrix} = \mathfrak{b}$$

Using the SVD of A, we can determine if a solution exists, as well as the general form of the possible solutions $\mathfrak{x}$.

If $U\Sigma V^T$ is the SVD of the $M \times N$ matrix A ($M > N$), then the system $A\mathfrak{x} = \mathfrak{b}$ becomes

$$U\Sigma V^T\mathfrak{x} = \mathfrak{b}\,.$$

Substituting $\mathfrak{z} = V^T\mathfrak{x}$ and $\mathfrak{d} = U^T\mathfrak{b}$, we have $\Sigma\mathfrak{z} = \mathfrak{d}$.. Let $Rank(A) = k$ =the number t of non-zero singular values s_i. Studying the linear equations of the diagonal system $\Sigma\mathfrak{z} = \mathfrak{d}$, we can determine whether or not there is a solution. A solution exists if and only if $d_j = 0$ whenever $s_j = 0$ or $j > N$. If $k < N$ then the z_j associated with a zero s_j can be set to any value and still yield a solution. A general form of the possible solutions can then be expressed in terms of these arbitrary components of $\mathfrak{z}$ when transformed back to the original coordinates by $\mathfrak{x} = V\mathfrak{z}$.

The condition number of a matrix can also describe the sensitivity of solutions of linear systems to inaccuracies in the data. Suppose we want to measure the maximal increase in relative inaccuracy for the worst position of $\mathfrak{b}$ and error $\mathfrak{db}$, when solving for $\mathfrak{x}$ in the system $A\mathfrak{x} = \mathfrak{b}$. The answer is precisely the condition number [9]

$$E = cond(A) = \max_{\mathfrak{b},\mathfrak{db}} \frac{\|\mathfrak{dx}\|/\|\mathfrak{x}\|}{\|\mathfrak{dy}\|/\|\mathfrak{y}\|} = \frac{s_{max}}{s_{min}}$$

For the above reason, matrices with large condition numbers are said to be ill-conditioned.

As an extension of solving linear systems, suppose we wish to find a solution where $A\mathfrak{x}$ is approximately equal to $\mathfrak{b}$. By this we mean the least-squares solution $\mathfrak{x}$ to minimise

$$\|A\mathfrak{x} - \mathfrak{b}\|^2$$

or equivalently to minimise the length $\|A\mathfrak{x} - \mathfrak{b}\|$. The advantage of using the SVD for this problem is that it can reliably handle the rank deficient case as well as the full rank case. Since orthogonal matrices preserve norm,

$$\|U^T(AV^T\mathfrak{x} - \mathfrak{b})\| = \|\Sigma\mathfrak{z} = \mathfrak{d}\|.$$

Using the SVD, the least squares problem is now in terms of a diagonal matrix, where the vector $\mathfrak{z}$ that minimises the length $\|A\mathfrak{x} - \mathfrak{b}\|$ is given by

$$z_j = \begin{cases} \dfrac{d_j}{s_j}, & \text{if } s_j = 0 \\ anything & \text{otherwise.} \end{cases}$$

Hence, k of the equations have exact solutions and the remaining ones yield a possibly non-zero residual vector of length $\left(\sum d_i^2\right)^{\frac{1}{2}}$, where the sum is over all i for which $s_i = 0$ or $i > N$. The solution to the original problem is then $\mathfrak{x} = V\mathfrak{z}$. [4].

4.2 Noisy Signal Filtering

Problems in signal processing often use linear models for signals. In ideal (noise-free conditions) the measurement data can be arranged in a matrix, where the matrix is known to be rank-deficient. By this, we mean that the

signal is assumed to lie in a proper subspace of Euclidean space. However, the presence of noise, either from rounding error or instrument error, results in a measurement matrix that is often of full rank. Usually, the models assume that the error can be separated from the data, in that the noise component is that which lies in a subspace orthogonal to the signal subspace. For this reason, the SVD is used to approximate the matrix, decomposing the data into an optimal estimate of the signal and the noise components. Suppose A is the measurement matrix, where each column consists of a signal component $\mathfrak{x}$ and a noise component n.

$$A = (C_1|C_2|\cdots|C_N)$$

where each $C_i = x_i + n_i$. The vector $\mathfrak{x}$ representing the signal is known to lie in a rank k subspace, though the precise subspace is not known. Therefore, let $\mathfrak{x} = H\mathfrak{c}$ for a coefficient vector $\mathfrak{c}$ and a matrix H whose columns are the basis vectors of some rank k subspace. The (least-squared) error between A and $H\mathfrak{c}$ is minimised by choosing H to be the optimal k rank approximation A_k to A. Then the k columns of U, corresponding to the k largest singular values, span the rank k subspace H. The resulting error is $e^2 = \sum_{k+1}^{N} s_i^2$. Using the SVD as above, we see that the original data matrix A is decomposed into the orthogonal components $U\Sigma_k V^T$, which is the rank k subspace corresponding to the signal subspace, and $U\Sigma_{n-k}V^T$,which corresponds to the orthogonal subspace defining the noise components [7].

4.3 Time Series Analysis

The technique of delay coordinate embedding, used by [6] for time series analysis, also uses the SVD. The algorithm constructs a multidimensional model of the data from a sequence of one dimensional observations. An M-dimensional vector is constructed by sliding a window of length M over consecutive observations in the data sequence. The vectors are then filtered using the Discrete Fourier Transform to remove signal noise. Each vector $\mathfrak{b} = \{b_1, b_2, ..., b_M\}$ represents a state of the underlying dynamical system. The object is to find the best (least-squares distance) L-dimensional linear space $L \leq M$ that passes through the centre of mass c of the K nearest neighbours of b. We construct a matrix A whose rows consist of the vectors

$b_1 - c, b_2 c, ..., b_k - c$ and calculate the SVD $U\Sigma V^T$. Taking the first L columns of the orthogonal matrix V gives us the desired basis for the L-dimensional subspace [3)]

5 Discussion and Conclusion

By providing an approximation to rank deficient matrices, and exposing the geometric properties of the matrix, the singular value decomposition of a matrix is a powerful technique in matrix computations. Despite its usefulness, however, there are a number of drawbacks, as mentioned by [8]. For problems that can be solved by simpler techniques, such as the Fourier Transform, or QR decomposition, use of the SVD may be unduly expensive computationally. Secondly, the SVD operates on a fixed matrix, hence it is not amenable to problems, that require adaptive algorithms. A host of active research efforts address these problems. Further examples of the use of SVD in the field of Signal Processing, as well as discussions of implementation algorithms and architectures, can be found in [8, 3].

[3)] The first L columns of V a basis of $NullSpace(A) = Range(A^T)$ which is consistent with our previous discussion since the vector $\mathfrak{b}_i - \mathfrak{c}$ constitute the row of A, rather than the columns as in the other examples.

Literaturverzeichnis

[1] Fobert F. V. Anderson. *Introduction to Linear Algebra.* Holt, Rinehart, and Winston, New York, 1986.

[2] P. Dewilde and Ed. F. Deprettere. *Singular value decomposition. An introduction* In Ed. F. Deprettere, editor, *SVD and Signal Processing: Algorithms, Applications, and Architectures,* pages 3-41 Elsevier Science Publishers, North Holland, 1988.

[3] Ed. F. Deprettere, editor. *SVD and Signal Processing: Algorithms, Analysis, and Applications.* Elsevier Science Publishers, North Holland, 1988.

[4] George E. Forsythe, Michael A.Malcolm, and Cleve B. Moler. *Computer Methods for Mathematical Computations,* pages 201-235, Prentice Hall, Englewood Cliffs, 1977.

[5] Gene H. Golub and Charles F. Van Loan. *Matrix Computations,* pages 16-21, 293. Johns Hopkins University Press, Baltimore, Maryland, 1983.

[6] Tim Sauer. *Time series prediction by using delayed coordinate embedding.* In Andreas S. Weigend and Neil A. Gershenfeld, editors. *Time Series Prediction, Forecasting the Future and Understanding the Past.* Adgdison-Wesley, 1994

[7] Louis L. Scharf. *The SVD and reduced-rank signal processing.* In R. Vaccaro, editor, *SVD and Signal Processing II, Algorithms, Applications, and Architectures,* pages3-31, Elsevier Science Publishers, North Holland, 1991.

[8] R. Vaccaro, editor, *SVD and Signal Processing II, Algorithms Analysis, and Applications.* Elsevier Science Publishers, North Holland, 1991.

[9] Joos Vandewalle and Bart De Moor. *A variety of applications of singular value decomposition in identification and signal processing.* In Ed. F. Deprettere, editor, *SVD and Signal Processing, Algorithms, Applications, and Architectures,* pages 43-91. Elsevier Science Publishers, North Holland, 1988.

[10] Andreas S. Weigend and Neil A. Gershenfeld. *Time Series Prediction: Forecasting the Future and Understanding the Past.* Addison-Wesley, Reading, Massachusetts, 1994.

Stichwortverzeichnis

Notizen zur Algebra

Bruno Bosbach

2010

C.F. GAUß

1777 -1855

Inhaltsverzeichnis

Kapitel 1

Ein Wort vorweg

Ziel und Inhalt dieser Lecture Note sind leicht und schnell beschrieben. Der Lehramtskandidat ist in der Schule u.a. mit dem Aufbau des Zahlbereichs befasst sowie im Wechselspiel hiermit mit der jeweiligen Gleichungstheorie.

Seine *Mittelstufenalgebra* ist i.w. die *Körperalgebra,* mithin ist es wünschenswert, dass er vertraut gemacht wird auch mit *endlichen Körpern* und ihren *transzendenten Erweiterungen.*

Grundsätzlich wäre auch die Geometrie über diesen Körpern eine reizvolle Einübung „seiner Algebra".

In dieser Note spielen wir vom höheren Standpunkt alles durch, was „ins Lehramtsmetier fällt". Das bedeutet, auf den Punkt gebracht: Unser Ziel ist die Herleitung des *Fundamentalsatzes der Algebra* so algebraisch wir möglich unter Berücksichtigung besonderer Aspekte der Gymnasialmathematik. Dieser Weg erfordert als eine erste Zwischenstation den *Satz von Steinitz,* der besagt:

Ist $\mathfrak{K}$ ein Körper und $f(x)$ ein Polynom über $\mathfrak{K}$, so gibt es einen Oberkörper $\mathfrak{L}$ von $\mathfrak{K}$, in dem $f(x)$ in Linearfaktoren zerfällt.

Dieser Satz wiederum erfordert die Herleitung der *Euklidischen Teilbarkeitslehre* – hier in einem Guss für $\mathfrak{Z}$ und $\mathfrak{K}[x]$ sowie eine Entwicklung der Theorie algebraischer Erweiterungen vorgegebener Körper – unter Einschluss des abelschen *Satzes vom primitiven Element.*

Für eine Entwicklung der *Galoistheorie* reicht der Rahmen einer 4-stündigen Veranstaltung natürlich nicht, wir berücksichtigen aber die klassischen Probleme der *Würfelverdoppelung* und der *Winkeldreiteilung* wie sie in [10] behandelt werden, dabei zurückgehend bis auf DESCARTES, der gezeigt hat,

dass sich jeder Winkel mittels Lineal und Normal-Parabel *3-teilen* lässt. Um diesem Anliegen zu genügen, werden wir auch Teile der *klassischen Gleichungstheorie,* insbesondere der *Theorie der kubischen Gleichungen* vorstellen, alles spannend für jeden Liebhaber der Mathematik.

Schließlich fügen wir als zwei Addita ein Kapitel über den Satz von Wedderburn und ein Kapitel über Hauptidealringe – als einen „Beitrag des Hauses für Liebhaber" – hinzu.

Parallel zur Veranstaltung des Autors liefen die Übungen von Herrn Jörg Binder, in dessen eigener Regie und Verantwortung. So kommt es, dass nach Symbolik und Inhalt Vorlesung und Übungen gelegentlich divergieren, doch waren die Übungserfolge außerordentlich erfreulich. Grund genug, die „Binder'schen Blätter" hier „anzuheften".

Kapitel 2

Allgemein Algebraisches

2.1 Homomorphie

2. 1. 1 Definition. Sei M eine *nicht leere Menge.* Dann versteht man unter einer *n-stelligen Operation* jede *Funktion* vom Typ $f : M^n \longmapsto M$.

Ist insbesondere $n = 1$, so nennt man f auch einen *Operator.*

Schließlich bezeichnet man als 0-stellige Operation jede konstante Operation.

Eine 0-stellige Operation wäre beispielsweise auf $\mathbf{N}$ die Operation $0(b) = 0 \cdot b = 0$.

Einstellige Operationen, also Operatoren, begegnen uns u. a. in der Geometrie, beispielsweise als *Abbildungen*, oder auch in der linearen Algebra, beispielsweise als *Skalar-Multiplikation,* kurz s-Multiplikation, wenn wir notieren $s\mathfrak{a} := f_s(\mathfrak{a})$. Ist f zweistellig, wählt man in der Regel *Operationssymbole* der Art $\cdot$, $+$, $*$, $-$, $\cap$, $\cup$, $\wedge$, $\vee$, $\circ$... und schreibt dann etwa $a * b = c$ statt $f(a, b) = c$.

Offenbar lässt sich jede 2-stellige Operation auffassen als eine *Familie* von 1-stelligen Operationen, definiere $f_a(b) := ab$.

Trivial, aber fundamental, ist die Beobachtung, dass sich jede Menge auch auffassen lässt als ein *Operativ,* man setze $f(a) := a$.

2. 1. 2 Definition. Sei $(G, \cdot)$ ein Paar, gebildet aus einer nicht leeren Menge G und einer Operation $\cdot$ *auf* G. Dann nennen wir das Paar $(G, \cdot) =: \mathfrak{G}$ auch ein *Gruppoid.*

Gilt zusätzlich für alle *Tripel* (a, b, c) die Gleichung

$$\text{(A)} \qquad a \cdot (b \cdot c) \;=\; (a \cdot b) \cdot c\,,$$

so heißt $\cdot$ *assoziativ* und $\mathfrak{G}$ eine *Halbgruppe*. Ist $\mathfrak{H}$ sogar eine Halbgruppe mit *Eins*, d.h. existiert in $\mathfrak{H}$ ein Element 1 mit

$$\text{(E)} \qquad a \cdot 1 = \;a\; = 1 \cdot a$$

für alle a, so sprechen wir von einem *Monoid*.

Schließlich heißt $\cdot$ *kommutativ*, wenn für alle Paare a, b die nachfolgende Gleichung (K) erfüllt ist, nämlich:

$$\text{(K)} \qquad a \cdot b \;=\; b \cdot a\,.$$

Ist $\mathfrak{G}$ ein Gruppoid, so folgt offenbar aus $ea = a \;\; (\forall a \in G)$ und $af = a \;\; (\forall a \in G)$ die *Gleichheit* $e = ef = f$, weshalb insbesondere jedes Gruppoid höchstens eine Eins besitzen kann.

Das klassischste aller Monoide ist das Monoid aller Funktionen $f : M \longmapsto M$ einer festen Menge M in sich, betrachtet bezüglich der *Komposition*, man erinnere sich der *Endomorphismen* und ihrer Verkettung bzw. der Multiplikation von Matrizen in der Linearen Algebra oder auch der Verkettung von Funktionen in der Analysis.

2. 1. 3 Proposition. *Ist* $\mathfrak{S} := (S, \cdot)$ *eine Halbgruppe, so ist der Wert eines jeden Wortes unabhängig von der Klammerung, in Worten:*

Ändert man in $\ldots\; (((a_1 \cdot a_2) \cdot a_3) \ldots) \cdot a_n$ *die Klammerung sinnvoll, so ändert sich der Wert nicht.*

BEWEIS. Die Behauptung gilt für $n = 1, 2$ und 3. Sie sei nun schon bewiesen für alle $k \leq n$. Dann folgt für jedes Wort w der Länge $n + 1$ mit den Komponenten $b_1, \ldots, b_n, b_{n+1}$ und dem Wert b nach Induktionsvoraussetzung

$$\begin{aligned} b &= (b_1 \cdot \;\cdots\; \cdot b_m) \cdot\; (b_{m+1} \cdot \;\cdots\; \cdot b_n \cdot b_{n+1}) \\ &= (b_1 \cdot \;\cdots\; \cdot b_m) \cdot ((b_{m+1} \cdot \;\cdots\; \cdot b_n) \cdot b_{n+1}) \\ &= ((b_1 \cdot \;\cdots\; \cdot b_m) \cdot\; (b_{m+1} \cdot \;\cdots\; \cdot b_n)) \cdot b_{n+1} \\ &= (b_1 \cdot \;\cdots\; \cdot b_n) \;\cdot b_{n+1}. \end{aligned}$$

□

Somit dürfen wir in einer Halbgruppe auf Klammerungen verzichten. Wie üblich definieren wir als a^1 das Element a und als a^n mit $n \geq 2$ das Produkt

bestehend aus n gleichen Faktoren a. Ist $\mathfrak{S}$ sogar ein Monoid, so setzen wir wie üblich $a^0 := 1$. Mit Blick auf diese Festsetzungen ergibt sich fast unmittelbar:

$$a^p \cdot a^q = a^{p+q} \quad \& \quad (a^p)^q = a^{p \cdot q}$$

und im kommutativen Fall zusätzlich

$$a^p \cdot b^p \;=\; (a \cdot b)^p.$$

Unmittelbar klar ist:

2. 1. 4 Lemma. *Sei $\mathfrak{G}$ ein Gruppoid und seien A,B Teilmengen aus G. Dann liefert das Komplexprodukt*

$$A \cdot B := \{x \,\big|\, x = a \cdot b,\;\; a \in A, b \in B\}$$

eine Operation $\cdot$ auf der Potenzmenge G^* von G, und diese ist assoziativ bzw. kommutativ; falls $\cdot$ assoziativ respektive kommutativ ist.

2. 1. 5 Definition. Seien $\mathfrak{U} = (\mathfrak{U}, \circ)$ und $\mathfrak{G} = (\mathfrak{G}, \cdot)$ zwei Gruppoide. Dann heißt $\mathfrak{U}$ ein *Untergruppoid* von $\mathfrak{G}$, wenn gilt:

$$U \subseteq G \;\&\; a, b \in U \Longrightarrow a \circ b = a \cdot b\,.$$

In diesem Falle bezeichnen wir $\circ$ auch als die *Restriktion* von $\cdot$ auf U, symbolisiert *via* $\cdot\,\big|_U$.

2. 1. 6 Proposition. *Sei $\mathfrak{G} = (\mathfrak{G}\,, \cdot)$ ein Gruppoid. Ist dann $\mathfrak{U}_i$ $(i \in I)$ eine Familie von Untergruppoiden, so ist der Durchschnitt dieser U_i abgeschlossen bezüglich $\cdot$, d.h. dann gilt*

$$a, b \in D := \bigcap U_i \Longrightarrow a \cdot b \in D$$

Denn:

$$\begin{aligned} a, b \in D &\Longrightarrow a, b \in U_i \quad (\forall i \in I) \\ &\Longrightarrow a \cdot b \in U_i \quad (\forall i \in I) \\ &\Longrightarrow a \cdot b \in D\,. \end{aligned}$$

□

Der Durchschnitt D darf also leer sein. Als Beispiel kann hier das Gruppoid $(\mathbf{N}, +)$ dienen mit Blick auf die Untergruppoide $\mathfrak{U}_n = (\{x \,\big|\, x \geq n\}, +)$, deren Durchschnitt offenbar verschwindet. Ist der Durchschnitt nicht leer, so bildet das Paar $(D, \cdot|_D)$ offenbar ein Untergruppoid von $\mathfrak{G}$. Dies liefert uns die

Möglichkeit, jeder nicht leeren Teilmenge von G als *Erzeugnis* (A) dasjenige Gruppoid zuzuordnen, dessen Trägermenge gebildet wird vom Durchschnitt $[A]$ aller *abgeschlossenen* Untermengen, die A umfassen, und dessen Operation bezogen auf $[A]$ übereinstimmt mit der Multiplikation $\cdot$.

Man beachte, dass $[A]$ hiernach eine Teilmenge von G ist, (A) hingegen als ein Untergruppoid definiert wurde.

Natürlich bleibt alles Bisherige gültig, wenn wir ausgehen von einer Halbgruppe oder einem Monoid. Doch ist bei einem Monoid zu trennen nach Unterhalbgruppen und Untermonoiden, d.h. Unterhalbgruppen, die auch die *Eins* des vorgegebenen Monoids enthalten.

Damit können wir auch hier jeder Familie $\mathfrak{U}_i \ \ (i \in I)$ von Unterhalbgruppen bzw. Untermonoiden ein eindeutig bestimmtes Erzeugnis zuordnen, nämlich

$$\bigvee \mathfrak{U}_i := \Big(\bigcup U_i \ \ (i \in I) \Big) ,$$

was uns insbesondere *zu je zwei* Untergruppoiden $\mathfrak{A}$, $\mathfrak{B}$ deren Erzeugnis $\mathfrak{A} \vee \mathfrak{B}$ liefert, gelesen als $\mathfrak{A}$ *verbunden* $\mathfrak{B}$.

Erinnert sei in diesem Zusammenhang etwa an das Erzeugnis zweier Unterräume $\mathfrak{A}, \mathfrak{B}$ eines linearen Raumes $\mathfrak{V}$.

Klar ist, dass das Halbgruppenerzeugnis $[A]$ aus genau denjenigen Elementen besteht, die sich darstellen lassen als ein *Produkt* von Elementen aus A, also als ein $a_1 \cdot \ldots \cdot a_n \ \ (a_i \in A)$, sofern man die Elemente $a \in A$ als einstellige Produkte betrachtet, und dass das Monoiderzeugnis von A gleich $(A \cup \{1\})$ ist.

Von nun an sei vereinbart, das Multiplikationssymbol nur noch zur besonderen Markierung einzusetzen, ansonsten aber – wie üblich – statt $a \cdot b$ knapper ab zu schreiben, also auch Ua statt $U \cdot a$.

2. 1. 7 Definition. Seien $\mathfrak{G} := (\mathfrak{G}, \circ)$ und $\mathfrak{H} := (\mathfrak{H}, \star)$ zwei Gruppoide und sei f eine Abbildung von G auf H. Dann heißt f ein *Homomorphismus* von $\mathfrak{G}$ auf $\mathfrak{H}$, wenn gilt:

$$f(a \circ b) = f(a) \star f(b) .$$

Ist f zudem *bijektiv*, so heißt f ein Isomorphismus, ist darüber hinaus $\mathfrak{G} = \mathfrak{H}$, so sprechen wir von einem *Automorphismus*.

Schließlich heißt das Gruppoid $\mathfrak{H} := (\mathfrak{H}, \star)$ ein homomorphes Bild des Gruppoids $\mathfrak{G} := (\mathfrak{G}, \circ)$, wenn es zumindest einen Homomorphismus h von $\mathfrak{G} := (\mathfrak{G}, \circ)$ auf $\mathfrak{H} := (\mathfrak{H}, \star)$ gibt. In diesem Falle sagen wir dann auch, es sei $\mathfrak{H} := (H, \star)$ homomorphes Bild von $\mathfrak{G} := (G, \circ)$ *unter* h.

Als klassischer Homomorphismus sei erwähnt: die Abbildung der ganzen Zahlen auf die „Uhr" modulo n.

Als klassischer Isomorphismus (von $(\mathbf{R}, +)$ auf $(\mathbf{R}^+, \cdot)$) sei erwähnt: die Logarithmusfunktion

Als klassische Automorphismen seien erwähnt die linearen Abbildungen endlich erzeugter Vektorräume vermöge regulärer Matrices! [1)]

Offenbar spiegelt sich der Begriff des Homomorphismus in der Darstellung:

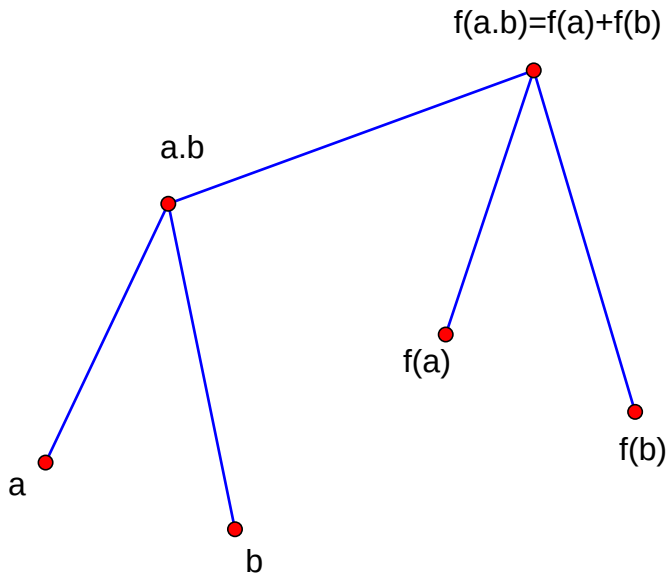


Abbildung 2.1: Zum Homomorphismus

Homomorphie bedeutet also:

Das Produkt der Bilder ist gleich dem Bild des Produktes

was wir griffiger formulieren mittels:

Homomorphismen nehmen Produkte mit.

[1)] umgangssprachlich auch bezeichnet als Matrizen

Schreiben wir statt $f(a)$ knapper $\overline{a}$ und statt $\star$ alternativ $\overline{\circ}$ so liest sich die Homomorphiebedingung als

$$\overline{a \circ b} = \overline{a}\,\overline{\circ}\overline{b} = \overline{a} \star \overline{b}\,.$$

Diese Lesart liefert fast unmittelbar den wichtigen Satz:

Homomorphismen nehmen Gleichungen mit.

Zur Wiederholung: Eine *2-stellige Relation* ρ auf der Menge M ist eine Teilmenge von $M \times M$. Gilt $(a, b) \in \rho$, so schreiben wir auch $a\,\rho\,b$. Statt griechischer Buchstaben verwendet man für die Bezeichnung solcher Relationen auch Symbole wie $\sim$, $\perp$, $\|$, $|$, $\subseteq$, $\geq$ .... Eine 2-stellige Relation $\sim$ heißt eine *Äquivalenzrelation*, wenn sie den Bedingungen genügt:

(R) $a \sim a$
(S) $a \sim b \Rightarrow b \sim a$
(T) $a \sim b \;\&\; b \sim c \Longrightarrow a \sim c\,.$

Ist $\sim$ eine Äquivalenzrelation, so liefert $\overline{a} = \{x \,\big|\, x \sim a\}$ eine *Klassenzerlegung* von M, d. h. eine Zerlegung von M in Klassen K_i mit $\bigcup_{i\in I} K_i = M$ und $K_i \neq K_j \Longrightarrow K_i \cap K_j = \emptyset\,.$

Ist nun umgekehrt K_i $(i \in I)$ eine Klassenzerlegung von M, so liefert

$$(a \sim b) \iff (a \in K_i \Leftrightarrow b \in K_i)$$

eine Äquivalenzrelation, und es entsprechen die *Klassenzerlegungen von M* und die *Äquivalenzrelationen auf M* einander umkehrbar eindeutig. □

Sei hiernach f ein Homomorphismus von $\mathfrak{G}$ auf $\mathfrak{H}$ (wie oben). Dann liefert

$$a \sim_f b \iff f(a) = f(b)$$

eine Äquivalenzrelation, und es gilt für diese Äquivalenzrelation

$$a \sim_f a' \;\&\; b \sim_f b' \implies a \circ b \sim_f a' \circ b'$$

wegen

$$\begin{aligned} a \sim_f a' \;\&\; b \sim_f b' &\implies f(a) = f(a') \;\&\; f(b) = f(b') \\ &\implies f(a) \star f(b) = f(a') \star f(b') \\ &\implies f(ab) = f(a'b') \\ &\implies ab \sim_f a'b'\,. \end{aligned}$$

2. 1. 8 Definition. Sei $\mathfrak{G} := (\mathfrak{G}, \circ)$ ein Gruppoid. Dann heißt $\equiv$ eine *Kongruenzrelation,* wenn gilt:

(i) $\equiv$ ist eine Äquivalenzrelation.
(ii) $a \equiv a' \;\&\; b \equiv b' \Longrightarrow a \circ b \equiv a' \circ b'$.

Ist nun $\equiv$ eine Kongruenzrelation, so *zerfällt* G in Klassen $\overline{a}$, und wir können mit diesen Klassen *rechnen* vermöge

$$\overline{a} * \overline{b} \;:=\; \overline{a \circ b}\,,$$

Denn, man beachte:

Das Ergebnis von $\overline{a} * \overline{b}$ ist unabhängig von der Wahl der Repräsentanten

und damit eine Funktion.

Das bedeutet aber, dass wir in kanonischer Weise ein Gruppoid $(\overline{G}, \overline{\circ})$ mit $\overline{\circ} := *$ der Klassen $\overline{a}$ erhalten, üblicherweise bezeichnet als *Restklassengruppoid* und symbolisiert mittels $\mathfrak{G}/\equiv$.

Im obigen Sonderfall der Relation $\sim_f$ erhalten wir offenbar das Restklassengruppoid $\mathfrak{G}/\sim_f$. Für dieses Restklassengruppoid $\mathfrak{G}/\sim_f$ gilt weiter:

$$\phi : a \mapsto \overline{a} \textbf{ ist ein Homomorphismus von } \mathfrak{G} \textbf{ auf } \mathfrak{G}/\sim_f ,$$

Denn: ϕ ist eine Funktion, und es gilt

$$\begin{aligned} \phi(a \circ b) &= \overline{a \circ b} \\ &= \overline{a} * \overline{b} = \phi(a) * \phi(b)\,. \end{aligned}$$

Doch, tatsächlich gilt mehr, nämlich die Isomorphie von $\overline{\mathfrak{G}}$ und $\mathfrak{H}$, was der nächste Satz genauer formuliert.

2. 1. 9 Proposition. *Sei f ein Homomorphismus des Gruppoids $\mathfrak{G} = (\mathfrak{G}, \circ)$ auf $\mathfrak{H} = (\mathfrak{H}, \star)$. Dann liefert $\sim_f$ eine Kongruenzrelation auf $\mathfrak{G}$ mit Restklassengruppoid $\overline{G} := \mathfrak{G}/\sim_f$, und es ist $\overline{\mathfrak{G}}$ isomorph zu $\mathfrak{H}$ unter*

$$\psi : \overline{a} \;\mapsto\; f(a)\,.$$

BEWEIS. Wir symbolisieren die Operation von $\mathfrak{G}$ mittels $\circ$, die Operation von $\mathfrak{H}$ mittels $\star$ und die Operation von $\overline{\mathfrak{G}}$ mittels $*$. Dann gelten nacheinander:

(i)

$$\begin{aligned} \overline{a} = \overline{a'} &\Longrightarrow a \sim_f a' \\ &\Longrightarrow f(a) = f(a') \\ &\Longrightarrow \psi(\overline{a}) = \psi(\overline{a'}) \end{aligned}$$

(ii)
$$\begin{aligned} \overline{a} \neq \overline{b} &\implies a \not\sim_f b \\ &\implies f(a) \neq f(b) \\ &\implies \psi(\overline{a}) \neq \psi(\overline{b}) \end{aligned}$$

(iii)
$$\begin{aligned} \psi(\overline{a} * \overline{b}) &= \psi(\overline{a \circ b}) \\ &= f(a \circ b) \\ &= f(a) \star f(b) \\ &= \psi(\overline{a}) \star \psi(\overline{b})\,. \end{aligned}$$

Somit ist ψ wegen (i) eine Funktion, wegen (i) und (ii) eine Bijektion und wegen (i) bis (iii) ein Isomorphismus. □

Aus 2.1.9 resultiert der

2. 1. 10 Der Homomorphiesatz. *Sei $\mathfrak{G}$ ein Gruppoid. Dann besitzt $\mathfrak{G}$ i. w. keine anderen homomorphen Bilder als seine Restklassengruppoide bzw.*

Homomorphe Bilder suchen und finden
bedeutet
Kongruenzrelationen suchen und finden!

Wie der Leser leicht erkennt, hat das Gruppoid bislang lediglich als Substrat gedient und wir hätten völlig analog ausgehen können von eine $\big(G, f_i \ (i \in I)\big)$, also mit mehreren Operationen simultan arbeiten können, und es hätten die einzelnen Operationen eben so gut n-stellig gewählt werden dürfen, u.a. also auch 1-stellig.

Dies folgt fast unmittelbar, wenn wir $a \cdot b$ ersetzen durch $f(a, b)$ und dann statt $f(a, b)$ ganz allgemein schreiben $f(x_1, \ldots, x_n)$.

Das bedeutet aber u.a., dass wir auch den Vektorraum und zwar als Algebra vom Typ $(G, +, f_s \ (s \in K))$ mit $f_s(\mathfrak{x}) := s\mathfrak{x}$ berücksichtigt haben.

Beispiele

(A) Man betrachte $(\{2^n\}, \cdot)$ und $(\mathbf{N}, +)$ bezüglich $2^n \mapsto n$.

(B) Man betrachte $(\mathbf{R}^+, \cdot)$ und $(\mathbf{R}, +)$ bezüglich $a \mapsto \log(a)$.

(C) Man betrachte $(\mathbf{R}, \cdot)$ bezüglich $a \mapsto |a|$.

(D) Man betrachte $(\mathbf{R}^n, +)$ bezüglich $x \mapsto x_i$.

(E) Man betrachte die multiplikative Halbgruppe der reellen Matrizen und die Halbgruppe $(\mathbf{R}, \cdot)$ bezüglich der Abbildung $f : A \mapsto |A| := det(A)$.

(F) Man betrachte $(\mathbf{Z}, +)$ bezüglich $a \equiv b :\Longleftrightarrow m \mid (a - b)$.

(G) Man betrachte $(\mathbf{N}, \cdot)$ bei vorgegebener Primzahl p bezüg lich der Relation $a \equiv b :\Longleftrightarrow p^n \mid a \Leftrightarrow p^n \mid b$.

(H) Man betrachte bei vorgegebenem $N \in \mathbf{N}$ den Polynom bereich $(\mathbf{R}[x], +)$ bezüglich $f \equiv g :\Longrightarrow a_i = b_i \ \ (i \geq N)$.

(I) Man setze auf $(\mathbf{R}, +)$ $a \equiv b :\Longleftrightarrow a - b$ ist rational.

(J) Man definiere einen Isomorphismus zwischen der Potenzmenge zu $\{1, 2, 3\}$ und der Teilermenge zu 30 bezüglich $\cup$ und $\vee$ $\big($erklärt vermöge $a \vee b := \mathrm{KGV}(a, b)\big)$.

(K) Man bearbeite die beiden soeben betrachteten Mengen in Bezug auf $\cap$ und $\wedge$ (als Symbol für den GGT).

(L) Man bearbeite die beiden soeben betrachteten Mengen in Bezug auf die Komplementbildung $\overline{A} := \{1, 2, 3\} - A$ und die Residuation $a' := 30/a$.

Kapitel 3

Gruppen

3.1 Über allgemeine Gruppen

3. 1. 1 Definition. Sei $\mathfrak{G} = (G, \cdot,)$ ein Gruppoid. Dann heißt $\mathfrak{G}$ eine *Gruppe*, wenn für alle $a, b, c \in G$ gilt:

$$\begin{aligned} &\text{(A)} && a \cdot (b \cdot c) &&= (a \cdot b) \cdot c \\ &\text{(G}_r\text{)} && a \cdot G &&= G \\ &\text{(G}_\ell\text{)} && G \cdot a &&= G\,. \end{aligned}$$

Ist $\mathfrak{G}$ zudem *kommutativ,* so heißt $\mathfrak{G}$ *abelsch*.
Das klassischste aller Beispiele einer Gruppe ist die Menge aller *Permutationen* einer vorgegebenen Menge M, betrachtet bezüglich der *Komposition.*

Klassisch ist auch die Gruppe der *regulären Matrizen,* also der Matrizen A mit nicht verschwindender *Determinante.*

Offenbar besagen die beiden Bedingungen (G_r) und (G_ℓ) nichts anderes als

(G) Die Gleichungen $a \cdot x \doteq b$ und $y \cdot a \doteq b$ sind stets lösbar

bzw. als Slogan:

Eine Gruppe ist eine Halbgruppe, in der man
von überall nach überall
gelangt,
über rechts und **über links**.

Aufgrund ihrer Allgemeinheit einerseits und ihrer „power" andererseits ist die Gruppe eine der zentralsten und fundamentalsten Strukturen der Mathematik, doch besitzt sie nicht nur innermathematisch, sondern auch außermathematisch größte Bedeutung, z. B. in der Physik bzw. in der Chemie.

Ist $\mathfrak{G}$ eine Gruppe, so ist $\mathfrak{G}$ erst recht ein Monoid, denn haben wir etwa $a \cdot e = a$, so folgt im Falle $b = y \cdot a$

$$b \cdot e = (y \cdot a) \cdot e = y \cdot (a \cdot e) = y \cdot a = b\,,$$

was bedeutet, dass e eine *Rechtseins* ist zu allen $b \in G$. Dual erhält man natürlich die Existenz einer Linkseins f, und das bedeutet, wie wir schon sahen, $e = fe = f$, also die Existenz einer eindeutig bestimmten 1.

Die von uns gegebene Definition der Gruppe ist sehr suggestiv. Doch sie macht den Typ der Algebra nicht klar. Dies leistet eine andere, spätere Definition deutlicher. Sie wird dem Umstand Rechnung tragen, dass jede Gruppe ein Monoid ist, in dem zu jedem a ein *Inverses* a^{-1} mit $a \cdot a^{-1} = 1 = a^{-1} \cdot a$ existiert. Hierzu vorab:

3. 1. 2 Proposition. *Ein Gruppoid $\mathfrak{G}$ ist genau dann eine Gruppe, wenn es assoziativ ist und zudem die Bedingungen erfüllt:*

(E) $$\exists e\,:\ \forall a\,:\quad a \cdot e = a$$

(I) $$\forall a\,:\ \exists a'\,:\quad a \cdot a' = e\,.$$

BEWEIS. Wie wir schon sahen, sind die aufgestellten Bedingungen notwendig.

Wir zeigen nun, dass sie auch hinreichen, also, dass zu jedem Paar a, b ein Paar x, y existiert mit $a \cdot x = b = y \cdot a$.

Hierzu wählen wir aus der Menge der möglichen a' jeweils ein a^* aus und setzen $(a^*)^* =: a^{**}$. Dann gilt zunächst:

(E) $$a = a \cdot (a^* \cdot a^{**}) \;=\; (a \cdot a^*) \cdot a^{**} = e \cdot a^{**}\,,$$

und hieraus folgt:

(3.7) $$a^* \cdot a = a^* \cdot (e \cdot a^{**}) \;=\; (a^* \cdot e) \cdot a^{**} = a^* \cdot a^{**} = e\,,$$

was uns weiter zu der Gleichung führt:

$$e \cdot a = (a \cdot a^*) \cdot a \;=\; a \cdot (a^* \cdot a) = a \cdot e = a\,. \tag{3.8}$$

Somit ist die geforderte *Rechtseins* sogar eine *Eins* und jedes *Rechtsinverse* a' zu a auch ein *Linksinverses,* denn es wurde a^* ja beliebig (!) gewählt. Damit sind wir dann am Ziel wegen:

$$\underline{a} \cdot (\underline{a'b}) = (a \cdot a')b = eb = \underline{b} \text{ und } (\underline{ba'}) \cdot \underline{a} = b(a'a) = be = \underline{b}\,. \qquad \square$$

In unserer Definition wurde lediglich die Existenz eines e, nicht aber seine Eindeutigkeit gefordert, und ganz entsprechend haben wir lediglich die *Existenz* eines a', nicht aber dessen *Eindeutigkeit* gefordert.

Tatsächlich aber sind e und a' eindeutig bestimmt. Dies ist klar für e, siehe oben, gilt aber auch für das geforderte a', wegen der *Kürzungsregel*:

$$\begin{array}{rcrcl} a \cdot x = a \cdot y & \Longrightarrow & a' \cdot (a \cdot x) & = & a' \cdot (a \cdot y) \\ & \Longrightarrow & (a' \cdot a) \cdot x & = & (a' \cdot a) \cdot y \\ & \Longrightarrow & x & = & y\,. \end{array}$$

Hiernach ist es berechtigt, das geforderte e als *Eins* zu bezeichnen und mittels 1 zu symbolisieren sowie das geforderte a' als *Inverses* zu bezeichnen und mittels a^{-1} (gesprochen: *a invers*) zu symbolisieren, worin sich jeweils neben der geforderten Funktion auch die Eindeutigkeit bzw. der *Operatorcharakter* ausdrückt.

Insbesondere haben unsere bisherigen Ausführungen mit ergeben:

3. 1. 3 Proposition. *Sei $\mathfrak{G} = (G, \cdot,)$ ein Gruppoid. Dann ist $\mathfrak{G}$ eine Gruppe, gdw. für alle $a, b, c \in G$ gilt:*

$$\text{(A)} \qquad a \cdot (b \cdot c) \;=\; (a \cdot b) \cdot c$$

$$\text{(EE)} \qquad \exists\, 1 \,:\, \forall a \,:\qquad a \cdot 1 = a = 1 \cdot a$$

$$\text{(INV)} \qquad \forall a \,:\, \exists\, !a^{-1} \,:\quad a \cdot a^{-1} = 1 = a^{-1} \cdot a\,.$$

Dieser Sachverhalt lässt sich – wie oben angekündigt – ein wenig „gelehrter" formulieren vermöge:

3. 1. 4 Korollar. *Die Gruppe lässt sich auffassen als eine Algebra $(G, \cdot, ^{-1}, 1)$ vom Typ $(2, 1, 0)$, die den Gesetzen* (A), (EE) *und* (INV) *genügt.*

Mit ergeben haben sich am Rande noch die Regeln:

$$(3.12) \qquad \begin{aligned} (a^{-1})^{-1} &= a \\ \& \quad (a \cdot b)^{-1} &= b^{-1} \cdot a^{-1} . \end{aligned}$$

Ferner halten wir fest:

$$(3.13) \qquad \begin{aligned} a^0 &:= 1 \\ \& \quad a^{-n} &:= (a^{-1})^n . \end{aligned}$$

Analog zum Begriff des Untergruppoids lässt sich der Begriff der *Untergruppe* formulieren, zu bedenken ist hierbei aber, dass wir als abgeschlossene Mengen nur *multiplikativ* abgeschlossene Mengen betrachten, die mit jedem a auch a^{-1} enthalten, die also nicht nur im Blick auf die Operation $\cdot$, sondern auch im Blick auf den Operator $^{-1}$ abgeschlossen sind, insbesondere also auch die 1 enthalten.

Dann aber können wir wie bei Gruppoiden jedem $A \subseteq G$ ein $[\, A \,]$ und ein (A) zuordnen, dabei verlaufen alle Betrachtungen wie oben.

Somit besitzt jedes $A \subseteq G$ ein *Gruppen–Erzeugnis* (A), und wir können auch hier jeder Familie $\mathfrak{U}_i \ \ (i \in I)$ ein eindeutig bestimmtes Erzeugnis zuordnen.

Als eine spezielle Untergruppe sei etwa die Untergruppe der *Potenzen* eines a aus G genannt.

Wie wir schon sahen, haben wir in Gruppen zu unterscheiden zwischen dem *Halbgruppen*-Erzeugnis und dem *Gruppen*-Erzeugnis von $A \subseteq G$. Dies werden wir derart regeln, dass wir ausdrücklich vom Halbgruppenerzeugnis sprechen, wenn dieses gemeint sein soll.

Sei hiernach A eine nicht leere Teilmenge von G. Dann ist $[\, A \,]$ zunächst von außen her erklärt, doch interessiert natürlich auch die Frage, wie sich $[\, A \,]$ von innen her aufbaut.

Offenbar gilt $[\, \emptyset \,] = \{1\}$, also $(\emptyset) = (\{1\}, \cdot, ^{-1})$.

Ist aber A nicht leer, so erhalten wir $[\, A \,]$ als die Menge aller Produkte

$$a_1 \cdot {a_2}^{-1} \cdot \ldots \cdot a_n \cdot {a_{n+1}}^{-1}, \ \ (a_i \in A \cup \{1\}) =: H(A) .$$

Denn $A \subseteq H(A)$ ist evident, und es ist $H(A)$ natürlich Teilmenge einer jeden abgeschlossenen Untermenge von G, die A enthält. Darüber hinaus ist aber

$H(A)$ auch abgeschlossen, denn es gehört ja *per definitionem* $1 \cdot 1 = 1$ zu $H(A)$ und wie man unmittelbar sieht mit jedem a auch a^{-1} und mit je zwei Elementen a, b auch $a \cdot b$.

Das bedeutet aber, dass $(H(A), \cdot, ^{-1})$ die *engste* A enthaltende Untergruppe ist, also gleich dem Erzeugnis (A) von A.

Insbesondere ist demnach $[\, a \,] = \{a^n \mid n \in \mathbf{Z}\}$.

Wir steuern nun auf den zentralen Begriff des *Normalteilers* zu. Hierzu beginnen wir mit der *Zerlegung* einer Gruppe $\mathfrak{G}$ nach einer Untergruppe $\mathfrak{U}$.

3. 1. 5 Proposition. *Sei $\mathfrak{G}$ eine Gruppe und $\mathfrak{U}$ eine Untergruppe von $\mathfrak{G}$. Dann gilt für alle $a, b \in G$ bezüglich der unter 2.1.4 erklärten Komplexoperation:*

$$Ua = Ub \iff Ua \subseteq Ub$$

DENN:

$$\begin{aligned} Ua = Ub &\implies Ua \subseteq Ub \\ &\implies a \in Ub \\ &\implies a = ub \ (\exists u \in U) \\ &\implies Ua = Uu \cdot b \\ &\implies Ua = Ub\,. \end{aligned}$$

□

3. 1. 6 Lemma. *Sei $\mathfrak{G}$ eine Gruppe und $\mathfrak{U}$ eine Untergruppe von $\mathfrak{G}$. Dann gilt*

$$Ua = Ub \implies Ua \cap Ub \neq \emptyset\,.$$

DENN: $Ua = Ub$ bedeutet wegen $Ua \neq \emptyset$ trivialer weise $Ua \cap Ub \neq \emptyset$, und es gilt:

$$\begin{aligned} x \in Ua \cap Ub &\implies u_1 a = x = u_2 b \ (\exists\, u_1, u_2 \in U) \\ &\implies a = (u_1)^{-1} u_2 \cdot b \in Ub \\ &\implies Ua \subseteq Ub \end{aligned}$$

und damit aus Gründen der Symmetrie

$$Ua \subseteq \ Ub \ \subseteq Ua\,.$$

□

Ist $\mathfrak{U}$ Untergruppe von $\mathfrak{G}$, so liefert die Abbildung $f_{a,b} : \ ua \mapsto ub$ eine Bijektion von Ua auf Ub. Denn $f_{a,b}$ ist eine Funktion, da $u_1 \cdot a = u_2 \cdot a$

zu $u_1 = u_2$ führt, evidenterweise surjektiv und schließlich injektiv wegen $u_1 \cdot a \neq u_2 \cdot a \Longrightarrow u_1 \neq u_2 \Longrightarrow u_1 \cdot b \neq u_2 \cdot b$. Das bedeutet insbesondere

$$\text{card}\,(Ua) = \text{card}\,(U) = \text{card}\,(Ub)\,. \tag{3.14}$$

Hiernach kommen wir zu dem zentralen Begriff des *Normalteilers:*

3. 1. 7 Definition. Sei $\mathfrak{G}$ eine Gruppe. Dann nennen wir $\mathfrak{N}$ einen *Normalteiler* von $\mathfrak{G}$, wenn gilt:

(N1) $\mathfrak{N}$ ist Untergruppe von $\mathfrak{G}$.

(N2) $aN = Na \;\; (\forall a \in G)\,.$

Offenbar ist $\mathfrak{N}$ ein Normalteiler gdw. $x \cdot N \cdot x^{-1} = N \;\; (\forall x \in G)$ erfüllt ist. Doch es genügt schon $x \cdot N \cdot x^{-1} \subseteq N \;\; (\forall x \in G)$ zu fordern, denn dann gilt ja auch $x^{-1} \cdot (xNx^{-1}) \cdot x = N \subseteq x^{-1} \cdot N \cdot x \;\; (\forall x \in G)$, also mit x^{-1} in der Rolle von x auch $N \subseteq x \cdot N \cdot x^{-1}$.

Ist eine Gruppe kommutativ, so ist natürlich jede Untergruppe ein Normalteiler. Nicht triviale Beispiele werden in den Übungen vorgestellt. Ein simples Beispiel für die Gruppe der $n \times n$–Matrizen etwa über $\mathbf{C}$ wäre die Untergruppe der Diagonalmatrizen mit konstanter Diagonale.

3. 1. 8 Proposition. *Sei $\mathfrak{N}$ Normalteiler zu $\mathfrak{G}$. Dann bildet die Menge aller Klassen Na bezüglich $Na \circ Nb := Na \cdot Nb$, aufgefasst als Komplexprodukt, eine Gruppe $\mathfrak{G}/\mathfrak{N}$, und es ist $\mathfrak{G}/\mathfrak{N}$ unter $a \mapsto Na$ homomorphes Bild zu $\mathfrak{G}$.*

BEWEIS. Wie man leicht sieht gilt für alle Halbgruppen die Gleichung $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ also auch

$$\begin{aligned} Na \circ (Nb \circ Nc) &= Na \cdot (Nb \cdot Nc) \\ &= (Na \cdot Nb) \cdot Nc \\ &= (Na \circ Nb) \circ Nc\,, \end{aligned} \tag{A}$$

und wir haben schon in Monoiden für Untermonoide $\mathfrak{U}$ die Gleichung $UU = U$, wegen $UU \supseteq 1U = U \supseteq UU$. Das liefert dann weiter

$$Na \circ Nb = NaNb = NNab = Nab$$

und damit die beiden Gruppenbedingungen

$$Na \circ N1 = Na1 = Na\,. \tag{E}$$

$$\text{(I)} \qquad Na \circ Na^{-1} \;=\; N(aa^{-1}) = N1\,.$$

Somit fungiert $N1$ als *Eins*, und es fungieren die Na^{-1} als *Inverse*. Damit ist alles gezeigt. □

Es definiert also jeder Normalteiler von $\mathfrak{G}$ eindeutig ein homomorphes Bild zu $\mathfrak{G}$ nämlich $\mathfrak{G}/\mathfrak{N}$.

Als Übung betrachte der Leser etwa die Gruppe der Kongruenzbewegungen des gleichseitigen Dreiecks und studiere hier die Normalteiler und die entsprechenden Zerlegungen nach diesen Normalteilern.

Normalteiler zeichnen sich u.a. dadurch aus, dass sie $x \cdot N \cdot x^{-1} = N$ erfüllen. Aus diesem Grunde nennt man Normalteiler auch *invariante* Untergruppen. Natürlich ist nicht jede Untergruppe invariant, doch stets ist mit U auch $x \cdot U \cdot x^{-1}$ abgeschlossen, also *Träger* einer Untergruppe, die man üblicherweise mittels $x\,\mathfrak{U}\,x^{-1}$ symbolisiert.

Wie man leicht sieht, sind $\mathfrak{U}$ und $x\mathfrak{U}x^{-1}$ stets isomorph. Untergruppen vom Typ $x\mathfrak{U}x^{-1}$ heißen konjugiert zu $\mathfrak{U}$. Man mache sich klar, dass die Relation konjugiert eine Äquivalenzrelation ist. Weiter haben wir:

3. 1. 9 Proposition. *Sei $\mathfrak{G} = (G, \circ)$ eine Gruppe und sei $\mathfrak{H} = (H, \star)$ ein Gruppoid. Ist dann f ein Homomorphismus von $\mathfrak{G}$ auf $\mathfrak{H}$, so ist auch $\mathfrak{H}$ eine Gruppe.*

BEWEIS. Zur Wiederholung: Homomorphismen nehmen Gleichungen mit, damit wäre alles gezeigt. Doch sei aus didaktischen Gründen an dieser Stelle ausführlich demonstriert, wie dies gemeint ist:

Wir bezeichnen die Bilder aus H *unter* f mit $\overline{a}, \overline{b}$, etc. Dann gelten nacheinander:

$$\text{(A)} \qquad \begin{aligned} \overline{a} \star (\overline{b} \star \overline{c}) \;&=\; \overline{a \circ (b \circ c)} \\ &=\; \overline{(a \circ b) \circ c} = (\overline{a} \star \overline{b}) \star \overline{c} \end{aligned}$$

$$\text{(E)} \qquad \overline{a} \star \overline{1} \;=\; \overline{a \circ 1} = \overline{a}$$

$$\text{(I)} \qquad \overline{a} \star (\overline{a^{-1}}) \;=\; \overline{a \circ a^{-1}} = \overline{1}\,. \qquad \square$$

Hiernach kommen wir zurück auf das Zusammenspiel von *Kongruenzen* und *Homomorphismen*.

3. 1. 10 Proposition. *Sei $\mathfrak{G}$ eine Gruppe. Dann entsprechen die Kongruenzen von $\mathfrak{G}$ umkehrbar eindeutig den Normalteilern von $\mathfrak{G}$ vermöge der Zuordnung:*

$$(\equiv \ \mapsto \mathfrak{N}) \iff (a \equiv b \Longleftrightarrow Na = Nb)\,.$$

BEWEIS. Sei $\equiv$ eine Kongruenz und $\overline{1} =: N$ die Kongruenzklasse der 1. Dann ist $\overline{1}$ offenbar abgeschlossen wegen

$$a \equiv 1 \equiv b \implies ab \equiv 1 \cdot 1 = 1$$

und

$$a \equiv 1 \implies a^{-1} = a^{-1} \cdot 1 \equiv a^{-1} \cdot a = 1\,.$$

Es ist aber $\overline{1} = N$ nicht nur abgeschlossen, sondern es gilt auch $x \cdot N \cdot x^{-1} \subseteq N$ wegen $n \in N \Longrightarrow n \equiv 1 \Longrightarrow x \cdot n \cdot x^{-1} \equiv x1x^{-1} = 1 \in \overline{1} = N$.

Weiter haben wir

$$\begin{aligned} a \equiv b &\iff ab^{-1} \equiv 1 \\ &\iff ab^{-1} \in N \\ &\iff Nab^{-1} = N \\ &\iff Na = Nb\,. \end{aligned}$$

Somit existiert zu jedem $\equiv$ ein Normalteiler im gewünschten Sinne, und es gehören zu verschiedenen Kongruenzen natürlich verschiedene Normalteiler.

Schließlich wurde schon im ersten Teil des Beweises gezeigt, dass jeder Normalteiler als 1-Klasse einer Kongruenz erfasst wird. □

Mit anderen Worten sagt uns der letzte Satz nichts anderes als:

Normalteiler sind Kongruenzen
und
Kongruenzen sind Normalteiler

Entsprechend dem Untergruppenerzeugnis einer Teilmenge $A \subseteq G$ existiert auch das Normalteilererzeugnis $\langle A \rangle$ der Teilmengen A. Denn, wie man sofort bestätigt ist natürlich $\mathfrak{G}$ selbst ein Normalteiler und mit jeder Familie $\mathfrak{N}_i$ $(i \in I)$ ist auch der Durchschnitt dieser Familie ein Normalteiler.

Wir fragen nach dem Aufbau der Normalteiler von innen her. Hier gilt:

Bilden wir zunächst zu dem Untergruppenerzeugnis (A) von A die Menge $\mathrm{I}(A)$ aller xax^{-1} $(x \in G, a \in [\,A\,])$, so erkennen wir sofort, dass diese

Menge in jedem Normalteiler enthalten ist, der A umfasst, man beachte, dass eine Untergruppe normal ist gdw. sie für alle $x \in G$ die Bedingung $x \cdot U \cdot x^{-1} \subseteq U$ erfüllt. Auch wurde schon erwähnt, dass mit U auch $x \cdot U \cdot x^{-1}$ eine Untergruppe ist. Und schließlich haben wir $y \cdot \mathrm{I}(A) \cdot y^{-1} \subseteq \mathrm{I}(A)$ wegen $y \cdot (xax^{-1}) \cdot y^{-1} = (yx) \cdot U(yx)^{-1}$.

3.2 Über endliche Gruppen

Ist eine Gruppe endlich, so dürfen wir Besonderheiten erwarten, die sich aus der endlichen Anzahl der Elemente ergeben. Von diesen Besonderheiten erwähnen wir hier lediglich einige Sachverhalte, wie sie für spätere Betrachtungen von Bedeutung sein werden.

Als erstes beobachten wir

3. 2. 1 Proposition. *Eine endliche Halbgruppe ist schon dann eine Gruppe, wenn sie kürzbar ist, d.h. wenn sie der Implikation genügt:*

$$\text{(K)} \qquad ax = ay \Longleftrightarrow x = y \Longleftrightarrow xa = ya$$

BEWEIS. Jede Gruppe ist kürzbar, wie wir schon sahen. Und wegen der Endlichkeit folgt nach der Kürzungsregel, das aG und G gleich viele Elemente haben, dass also jedes g ein $a \cdot g'$ ist. Damit ist aus Gründen der Dualität alles gezeigt. □

Als nächstes beobachten wir, dass es bei vorgegebenem $a \in G$ unter den Potenzen von a mindestens ein Paar a^m, a^ℓ mit $m > \ell$, aber $a^m = a^\ell$ geben muss. Das bedeutet, dass $a^{m-\ell} = 1$ mit einem $m - \ell > 0$ erfüllt ist. Dies halten wir fest.

3. 2. 2 Definition. Ist $\mathfrak{G}$ eine *endliche Gruppe,* so versteht man unter der *Ordnung* von $\mathfrak{G}$ die Anzahl $O(\mathfrak{G})$ der Elemente von G und unter der Ordnung $o(a)$ von $a \in G$ die kleinste Zahl k mit $0 < k \;\&\; a^k = 1$.

3. 2. 3 Lemma. *Sei $\mathfrak{G}$ eine endliche Gruppe und a aus G. Dann gilt $a^n = 1 \Longrightarrow \exists x_n : o(a) \cdot x_n = n$.*

BEWEIS. Sei $n = o(a) \cdot x_n + r$ im Sinne der Division mit Rest.[1)] Dann folgt $(a^{o(a)})^q \cdot a^r = a^r = 1$ mit $0 \leq r < o(a)$, also, wegen der Minimalität von $o(a)$, mit $r = 0$. Das liefert dann $n = o(a) \cdot x_n$, was zu beweisen war. □

Später werden wir auch sagen $0(a)$ *teilt* n, auch $0(a)$ *ist ein Teiler* von n.

3. 2. 4 Der Satz von Lagrange. *Sei* $\mathfrak{G}$ *eine endliche Gruppe und* $\mathfrak{U}$ *eine Untergruppe von* $\mathfrak{G}$*. Dann ist die Ordnung von* $\mathfrak{U}$ *ein Teiler der Ordnung von* $\mathfrak{G}$*.*

DENN: Man zerlege G nach U. Dann ist die Vereinigungsmenge aller Ua gleich G, und demzufolge wegen $|Ua| = |U| =: m$ die Anzahl der Elemente von G ein Vielfaches von m. □

Insbesondere haben wir demzufolge:

3. 2. 5 Korollar. *Ist* $\mathfrak{G}$ *eine endliche Gruppe, so teilen die Ordnungen der einzelnen Elemente jeweils die Ordnung von* $\mathfrak{G}$*.*

DENN: Die Menge der Potenzen $a^1, \ldots, a^{o(a)}$ bildet jeweils eine Untergruppe. □

Wir kommen nun zum Begriff der *zyklischen Gruppe.*

3. 2. 6 Definition. Ein Gruppe $\mathfrak{G}$ heißt *zyklisch,* wenn sie von einem einzigen Element *erzeugt* wird, also vom Typ (a) ist.

Hieraus folgt natürlich

3. 2. 7 Korollar. *Jede zyklische Gruppe ist abelsch.*

Als einen Struktursatz für zyklische Gruppen erhalten wir fast unmittelbar:

3. 2. 8 Theorem. *Es gibt im wesentlichen, d. h. bis auf Isomorphie, keine anderen zyklischen Gruppen als die additiven Restklassengruppen* $(\mathbf{Z}_m, \oplus)$ *unter Einschluss von* $(\mathbf{Z}, +)$ *als* $(\mathbf{Z}_0, \oplus)$*.*

BEWEIS. Sei $\mathfrak{G}$ eine zyklische Gruppe. Existiert dann ein m mit $a^m = 1$, so folgt unmittelbar für den kleinsten Exponenten k dieser Art $a^m = a^n \Longleftrightarrow k \mid m - n$.

[1)] Für den Anfänger: Subtrahiere o(a) so oft von n, „bis es nicht mehr geht". Dann bleibt ein Rest r mit $0 \leq r < n$, und es folgt:

Analog schließt man, wenn kein solches k existiert, bzw. 0 der einzige Exponent mit $a^0 = 1$ ist. □

Später werden wir im Zusammenhang mit dem Studium endlicher Körper auf der Grundlage der Teilbarkeitslehre als weitere wichtige Lemmata für endliche abelsche Gruppen beweisen:

3. 2. 9 Lemma. *In jeder endlichen, multiplikativ notierten abelschen Gruppe* $\mathfrak{G}$ *gilt:*

$$o(a) = m \perp n = o(b) \implies o(ab) = o(a) \cdot o(b)\,.$$

3. 2. 10 Lemma. *In jeder endlichen multiplikativ notierten abelschen Gruppe* $\mathfrak{G}$ *gilt:*

$$o(a) = m \cdot n \implies o(a^m) = n\,.$$

Kapitel 4

Ringe

4.1 Grundbegriffe

Grundstruktur dieses Abschnitts ist der *Ring.* Er wurde schon in der *linearen Algebra* eingeführt, etwa als *Matrizenring.* Zur Wiederholung:

4. 1. 1 Definition. Eine *Algebra* $(R, +, \cdot) =: \mathfrak{R}$ heißt ein *Ring,* wenn gilt:

(R1) $(R, +)$ ist eine abelsche Gruppe.
(R2) $(R, \cdot)$ ist eine Halbgruppe.
(R3) $a\,(b + c) = ab + ac \quad$ und $\quad (a + b)c = ac + bc\,.$

Besitzt die Halbgruppe $(R, \cdot)$ eine 1, so sprechen wir von einem *Ring mit* 1.

Erfüllt $\mathfrak{R}$ zudem die *Kürzungsregel* $a \neq 0\ \&\ ax = ay \Longleftrightarrow x = y \Longleftrightarrow xa = ya$, so heißt $\mathfrak{R}$ ein *Integritätsbereich*, und ist darüber hinaus für alle $a \neq 0$ jede Forderung $a \cdot x \doteq b$ erfüllbar, so heißt $\mathfrak{R}$ ein *Schiefkörper.*

Ist endlich die Operation $\cdot$ zudem *kommutativ,* so heißt $\mathfrak{R}$ *ein kommutativer Ring.*

Ein kommutativer Schiefkörper heißt ein *Körper.*

Ein Ring ist also immer „auch" eine Gruppe.

Klassisches Beispiel eines nicht notwendig kommutativen Ringes ist der Ring aller $n \times n$-Matrizen etwa über $\mathbf{C}$ oder $\mathbf{R}$ oder $\mathbf{Q}$.

Wir werden uns im weiteren mit kommutativen Ringen befassen. Um jedoch wenigstens einen Satz über allgemeine Ringe mit 1 zu formulieren und zu beweisen, nämlich die beiden nachfolgenden Propositionen 4.1.2 und 4.1.3

Diesbezüglich vorweg: Ein Element a aus R heißt *Linkseinsteiler, symbolisiert durch* $a \,\big|_\ell\, 1$,wenn gilt $ax = 1 \ \ (\exists x \in R)$ und hiernach:

4. 1. 2 Proposition. *Die Menge der Linkseinsteiler eine Ringes mit* 1 *bildet eine Gruppe.*

DENN: Die Menge der Linkseinsteiler erfüllt die Bedingungen von 3.1.2 □

4. 1. 3 Proposition. *Ist* $1 - yx$ *ein Linkseinsteiler des Ringes* $(R, +, \cdot, 1)$*, so ist auch* $1 - xy$ *Linkseinsteiler dieses Ringes* [1)]*.*

DENN: Aus $(1-yx)s = 1$ folgt $(1-xy)xs = x$, also $1-xy = 1-(1-xy)xs\cdot y$ und damit $(1 - xy)(1 + xsy) = 1$. □

Als ein erstes klassisches Beispiel eines kommutativen Ringes sei der Polynomring erwähnt.

Als ein weiteres klassisches Beispiel eines kommutativen Ringes mit hoch interessanten Eigenschaften sei der Ring der *stetigen reellen Funktionen* $f : \mathbf{R} \longmapsto \mathbf{R}$ bezüglich der üblichen Addition und Multiplikation von Funktionen erwähnt.

Als erstes stellt sich die Frage nach den Regeln der elementaren *Arithmetik* in Ringen, insbesondere nach den *Vorzeichenregeln.*

Erinnern wir uns: da $(R, +)$ eine abelsche Gruppe ist, bedeutet $-a$ dasselbe wie a^{-1}. Weiter können wir eine *Subtraktion* einführen, vermöge $a - b := a + (-b)$. Hierfür erhalten wir dann:

4. 1. 4 Proposition. *In jedem Ring* $\mathfrak{R}$ *gelten die Multiplikationsregeln:*

$$
\begin{aligned}
(i) \qquad a \cdot 0 &= 0 \\
(ii) \qquad a \cdot (-b) &= -(ab) = (-a) \cdot b \\
(iii) \qquad (-a) \cdot (-b) &= ab \\
(iv) \qquad a \cdot (b - c) &= ab - ac \\
\& \quad (a - b) \cdot c &= ac - bc\,.
\end{aligned}
$$

BEWEIS.

[1)] Dieses Problem wurde von Jörg Binder im Internetforum entdeckt, wo eine Lösung mittels eines Potenzreihenansatzes diskutiert wurde.

Zu $(i) : a0 = a \cdot (0+0) = a0 + a0 = a0 + 0 \rightsquigarrow a0 = 0\,.$

Zu $(ii) : ab + a(-b) = a \cdot (b + (-b)) = a0 = 0 \rightsquigarrow a(-b) = -(ab)\,.$

Zu $(iii) : (-a)(-b) = -((-a)b) = -(-(ab)) = ab\,.$

Zu $(iv) : a \cdot (b-c) = a \cdot ((b + (-c)) = ab + (-ac) = ab - ac\,.$ □

4. 1. 5 Definition. $a \neq 0 \in R$ heißt ein *Nullteiler* von $\mathfrak{R}$, wenn es ein $x \neq 0$ gibt mit $a \cdot x = 0 \vee xa = 0$.

Besitzt $\mathfrak{R}$ wenigstens einen Nullteiler, so nennt man $\mathfrak{R}$ einen *Ring mit Nullteilern*, besitzt $\mathfrak{R}$ hingegen keinen Nullteiler, so heißt $\mathfrak{R}$ *nullteilerfrei.*

Der Leser mache sich klar: Im Ring der stetigen Funktionen von $\mathbf{R}$ nach $\mathbf{R}$ sind exakt die Funktionen ohne Nullstellen invertierbar, also Einsteiler, und genau diejenigen Funktionen Nullteiler, die in mindestens einem offenen Intervall verschwinden.

4. 1. 6 Lemma. $\mathfrak{R}$ *ist genau dann ein Intregritätsbereich, wenn* $\mathfrak{R}$ *nullteilerfrei ist.*

Denn: Ist $\mathfrak{R}$ ein Integritätsbereich und gilt $a \neq 0$ und $ax = 0$, so folgt $ax = a0 \Longrightarrow x = 0$, und ist umgekehrt $\mathfrak{R}$ nullteilerfrei, so folgt $a \neq 0$ & $ax = ay \Longrightarrow a(x-y) = 0 \rightsquigarrow x = y$. Damit sind wir aus Gründen der *Rechts-/Links-Dualität am Ziel.* □

Ist $\mathfrak{R}$ sogar ein Körper, so verifizieren wir leicht die Regeln der Buchstabenrechnung. Dies sei exemplarisch erläutert an der Addition von *Brüchen.*

Nach den Regeln für das Rechnen in Körpern haben wir zunächst im Falle $b \neq 0 \neq d$ die Werte $ab^{-1},\ cd^{-1}$ oder in der vertrauteren Schreibweise $\frac{a}{b},\ \frac{c}{d}$. Wir fragen nach deren Summe $\frac{a}{b} + \frac{c}{d}$ und erhalten die Regel:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \tag{4.1}$$

wegen

$$\left(\frac{a}{b} + \frac{c}{d}\right) \cdot bd = ab^{-1}bd + cd^{-1}bd = \frac{ad + bc}{bd} \cdot bd$$

und der Kürzungsregel für Gruppen.

Als nächstes interessieren wir uns für die *Restklassenstrukturen von Ringen,* kurz für alle *Restklassenringe* bei vorgegebenem Ring $\mathfrak{R}$.

Wir wissen schon, dass alle Restklassenringe von einer Untergruppe von $(R,+)$ erzeugt werden, da jedes Restklassensystem von $\mathfrak{R}$ auch ein Restklassensystem von $(R,+)$ ist, aber wir wissen natürlich noch nicht, welche Zusatzbedingungen eine Untergruppe von $(R,+)$ erfüllen muss, damit die Festsetzung

$$a \equiv b \ \ (N) \Longleftrightarrow N + a = N + b$$

eine Kongruenz auch bezüglich der Multiplikation liefert. Hier hilft die folgende Überlegung weiter:

Soll eine Untergruppe das Gewünschte leisten, so muss sie wegen

$$a \in N \Longrightarrow a \equiv 0 \Longrightarrow as \equiv 0s = 0$$

mit jedem a auch alle sa und dual alle at enthalten, und dies ist nicht nur notwendig, sondern auch hinreichend, wie wir sehen werden. Hierbei beschränken wir uns auf Ringe mit 1, doch bedeutet dies nicht wirklich eine Einschränkung, was der Leser hinnehmen möge.

4. 1. 7 Definition. Sei $\mathfrak{R}$ ein Ring mit 1. Dann nennen wir $\mathfrak{i} \subseteq R$ ein *Ideal* aus $\mathfrak{R}$, wenn gilt:

(i) $\mathfrak{i}$ ist nicht leer.

(ii) $\mathfrak{i} \pm \mathfrak{i} \subseteq \mathfrak{i}$

(iii) $R \cdot \mathfrak{i} \cdot \mathfrak{R} \subseteq \mathfrak{i}$.

Offenbar ist die dritte Bedingung gleich bedeutend damit, dass mit jedem Element auch alle *Links-* und alle *Rechtsvielfachen* zu $\mathfrak{i}$ gehören, denn man wähle das eine Mal 1 als linken Faktor, das andere Mal 1 als den rechten Faktor.

Ferner sieht man unmittelbar, dass die Teilmenge R aller Elemente ein Ideal bildet, auch bezeichnet mit $\mathfrak{e}$ und dass ebenso die Teilmenge, gebildet aus dem Element 0 ein Ideal bildet, bezeichnet als das Nullideal $\mathfrak{o}$. Hiernach erhalten wir ganz leicht:

4. 1. 8 Proposition. *Sei $\mathfrak{R}$ ein Ring mit 1. Dann erhält man (bis auf Isomorphie) alle homomorphen Bilder von $\mathfrak{R}$ als Restklassenringe von $\mathfrak{R}$ und*

diese gewinnt man durch Zerlegung von R nach Idealen $\mathfrak{i}$ via

$$a \equiv b \ \ (\mathfrak{i}) \Longleftrightarrow \mathfrak{i} + a = \mathfrak{i} + b \Longleftrightarrow a - b \in \mathfrak{i}\,.$$

BEWEIS. Vorweg: Gilt $\mathfrak{i} + \mathfrak{a} = \mathfrak{i} + \mathfrak{b}$, so folgt $i_1 + a = i_2 + b$, also $a - b = i_2 - i_1 \in \mathfrak{i}$, und gilt $a - b \in \mathfrak{i}$, so folgt $a - b = i \rightsquigarrow a + 0 = b + i$.

Hiernach kommen wir zum eigentlichen Beweis:

Auf der einen Seite kann es keine anderen Restklassenringe geben, wie wir schon sahen.

Auf der anderen Seite liefert unsere Definition aber eine Kongruenz bezüglich der Gruppe $(R, +)$, was im Abschnitt über Gruppen unter 3.1.10 gezeigt wurde, und es liefert unsere Definition auch eine Kongruenz auf $(R, \cdot)$ wegen

$$a \equiv b \Longrightarrow a - b \in \mathfrak{i} \Longrightarrow s\,(a - b) \in \mathfrak{i} \Longrightarrow sa - sb \in \mathfrak{i} \Longrightarrow sa \equiv sb \ \ (\mathfrak{i})$$

und der hierzu rechtsdualen Aussage. □

Ideale spielen in der Ringtheorie nicht nur eine wichtige Rolle im Blick auf Kongruenzen, sondern viel mehr noch im Blick auf *Zerlegungen*, wie schon erwähnt, insbesondere *ideale Faktorzerlegungen*. Und hierher rührt auch ihr Ursprung. Ja, man darf sagen, dass es das Zusammenspiel der Teilbarkeitseigenschaften der Primideale mit ihren Kongruenzmerkmalen ist, das eine *effektive algebraische Zahlentheorie* erst ermöglicht. In diesem Zusammenhang sind vor allem gewisse *Idealoperationen* von Bedeutung. Hier nur einige Beispiele

(1) Sei $\mathfrak{a}_i \ \ (i \in I)$ eine Familie von Idealen. Dann ist auch $\bigcap_{i\in I} \mathfrak{a}_i$ ein Ideal, und dies bedeutet, dass zu jeder Teilmenge A aus R ein *ideales* Erzeugnis (A) existiert.

(2) Sei $A \subseteq B$. Dann ist das von A erzeugte Ideal (A) gleich der Menge aller Elemente, die sich mit Koeffizienten aus R linear über A kombinieren lassen.
Ist insbesondere $A = \{a\}$, so nennen wir $(A) =: (a)$ ein *Hauptideal.*

(3) Sei $\mathfrak{a}_i \ \ (i \in I)$ eine Familie von Idealen. Dann ist auch

$$\textstyle\sum_{i\in I} \mathfrak{a}_i := \{x \,|\, x = a_{i_1} + \ldots + a_{i_n}\} \ \left(a_{i_j} \in \bigcup_{i\in I} \mathfrak{a}_i\right)$$

ein Ideal, das man im Sonderfall zweier Ideale $\mathfrak{a}, \mathfrak{b}$ als die Summe $\mathfrak{a} + \mathfrak{b}$ dieser beiden Ideale bezeichnet.

(4) Seien $\mathfrak{a}, \mathfrak{b}$ zwei Ideale. Dann bildet auch die Menge aller Summen $\sum_1^n a_i b_i$ mit $a_i \in \mathfrak{a}, b_i \in \mathfrak{b}$ ein Ideal, bezeichnet als das *Produkt* $\mathfrak{a} \cdot \mathfrak{b}$ von $\mathfrak{a}$ und $\mathfrak{b}$.

(5) Seien $\mathfrak{a}, \mathfrak{b}$ zwei Ideale. Dann bildet auch die Menge aller x mit $\mathfrak{a}x \subseteq \mathfrak{b}$ ein Ideal, genannt der *Rechts-* Quotient $\mathfrak{a} * \mathfrak{b}$ von $\mathfrak{a}$ und $\mathfrak{b}$, und man erklärt natürlich dual den *Links*-Quotienten $\mathfrak{b} : \mathfrak{a}$ von $\mathfrak{a}$ und $\mathfrak{b}$.

Der aufmerksame Leser wird bemerkt haben, dass Ideale im Gegensatz zu Normalteilern nicht als Unterstrukturen, sondern als Teilmengen erklärt wurden. Dies hat seinen Grund darin, dass Ideale zunächst einmal als *ideale Objekte* hinzugenommen wurden, um die Teilbarkeitsverhältnisse gewisser Ringe aufzubessern.

Sehr wohl aber gibt es Autoren, die Ideale als Unterstrukturen einführen.

Der Leser beachte auch, dass ein Ideal in gewisser Weise einem Vektorraum gleichkommt, wenn man die Operation $\cdot$ des Ringes aufspaltet in eine Familie von Operatoren f_s, g_t mit $f_s(a) := sa$ und $g_t(a) = at$.

Betrachtet man den Ring in dieser Weise, so sind die Ideale des Ringes exakt die abgeschlossenen Teilmengen von $\mathfrak{R}$.

Von Bedeutung sind natürlich auch die Fragen, unter welchen Bedingungen ein Restklassenring ein Integritätsbereich ist und unter welchen Bedingungen ein Körper. Hierzu vorweg

4. 1. 9 Definition. Ein Ideal $\mathfrak{p}$ heißt ein *Primideal,* auch kurz *prim,* wenn $\mathfrak{p}$ der Bedingung genügt

$$ab \in \mathfrak{p} \implies a \in \mathfrak{p} \vee \mathfrak{b} \in \mathfrak{p}\,.$$

Ein Ideal $\mathfrak{m}$ heißt *maximal,* wenn kein Ideal zwischen $\mathfrak{m}$ und $\mathfrak{e}$ liegt.

Als Beispiele für Primideale erwähnen wir etwa die Teilmengen $p\mathbf{Z}$ als Primideale aus $(\mathbf{Z}, +, \cdot)$, als Beispiele maximaler Ideale etwa die Teilmengen I_x aller stetigen Funktionen, die an der Stelle x verschwinden.

Damit folgt

4. 1. 10 Proposition. *Sei* $\mathfrak{R}$ *ein Ring und* $\mathfrak{i}$ *ein Ideal aus* $\mathfrak{R}$*. Ist* $\mathfrak{i}$ *dann maximal, so ist* $\mathfrak{i}$ *auch prim, und es ist* $\mathfrak{R}/\mathfrak{i}$ *genau dann ein Integritätsbereich, wenn* $\mathfrak{i}$ *ein Primideal ist, und genau dann ein Körper, wenn* $\mathfrak{i}$ *ein maximales Ideal ist.*

BEWEIS. Die zu betrachtenden Restklassen sind von der Form $\mathfrak{i}+\mathfrak{a}$, d. h. sie entstehen dadurch, dass man „sukzessive" zu a die Elemente von $\mathfrak{i}$ addiert. Summe und Produkt zweier Klassen erhalten wir demzufolge vermöge $(\mathfrak{i} + a) \cdot / + (\mathfrak{i} + b) = \mathfrak{i} + (a \cdot / + b)$. Hiernach gilt dann:

$$(\mathfrak{i} + a)(\mathfrak{i} + b) \;=\; \mathfrak{i} + ab\,.$$

Sei nun zunächst $\mathfrak{p}$ ein Primideal. Dann haben wir

$$\begin{aligned}(\mathfrak{p} + a)(\mathfrak{p} + b) = \;\; \mathfrak{p} + 0 \;\; &= \mathfrak{p} + ab \\ &\Longrightarrow \quad ab \in \mathfrak{p} \\ &\Longrightarrow \quad a \in \mathfrak{p} \;\vee\; b \in \mathfrak{p} \\ &\Longrightarrow \quad \mathfrak{p} + a = \mathfrak{p} \;\vee\; \mathfrak{p} + b = \mathfrak{p}\,,\end{aligned}$$

und ist umgekehrt $\mathfrak{R}/\mathfrak{i}$ nullteilerfrei, so folgt

$$\begin{aligned}ab \in \mathfrak{i} \;\; &\Longrightarrow \;\; (\mathfrak{i} + a)(\mathfrak{i} + b) \subseteq \mathfrak{i} = \overline{0} \\ &\Longrightarrow \;\; \mathfrak{i} + a = \overline{0} \;\vee\; \mathfrak{i} + b = \overline{0} \\ &\Longrightarrow \;\; a \in \mathfrak{i} \;\vee\; b \in \mathfrak{i}\end{aligned}$$

Sei hiernach $\mathfrak{m}$ ein maximales Ideal.

Gilt dann $a, b \notin \mathfrak{m}$, so folgt $\mathfrak{m} + (a) = (1) = \mathfrak{e}$, also für geeignete Elemente $m \in \mathfrak{m}$, $x \in R$ die Beziehung $m + ax = 1 \rightsquigarrow 1 - ax \in \mathfrak{m}$ bzw. $\overline{a} \cdot \overline{x} = \overline{1}$, wie behauptet.

Andererseits besitzt jeder Körper nur zwei Ideale, da jedes vom *Nullideal* verschiedene Ideal mit jedem $a \neq 0$ auch alle Vielfachen zu a enthalten muss, also auch die 1. Daraus folgt aber unmittelbar, dass $\mathfrak{i}$ maximal sein muss, wenn $\mathfrak{R}/\mathfrak{i}$ ein Körper ist. □

4.2 Die transzendente Ringerweiterung

4. 2. 1 Definition. Sei $\mathfrak{R} := (\mathfrak{R}, +, \cdot)$ ein kommutativer Ring mit 1. Dann definieren wir R_f als die Menge aller fast überall verschwindenden Folgen

(a_n) $(n \in \mathbf{N}^0)$, d. h. aller Folgen, in denen höchstens endlich viele Glieder nicht verschwinden. Weiter erklären wir

$$\begin{aligned} (a_n) \oplus (b_n) &:= (a_n + b_n) \\ \text{und} \quad (a_n) \circ (b_n) &:= \sum a_i \cdot b_k \quad (i + k = n) \end{aligned}$$

Mit dieser Festsetzung folgt:

4. 2. 2 Theorem. *$(R_f, \oplus, \circ)$ bildet einen kommutativen Ring mit 1.*

BEWEIS. Wir überlassen den Beweis im wesentlichen dem Leser und beschränken uns auf ein typisches Exempel:

$$\begin{aligned} (a_n) \circ \big((b_n) \circ (c_n) \big) &= (a_n) \circ \big(\sum b_k c_\ell \quad (k + \ell = n) \big) \\ &= \sum a_i b_k c_\ell \quad (i + k + \ell = n) \\ &= \big((a_n) \circ ((b_n) \big) \circ (c_n) \,. \end{aligned}$$

□

4. 2. 3 Definition. Wir bezeichnen die Elemente $(a, 0, 0, \ldots)$, also die Folgen deren erstes Glied gleich a ist und deren weiteren Elemente alle verschwinden, mit $\overline{a}$ sowie darüber hinaus die Folge $(0, 1, 0, 0, \ldots)$ mit x.

Dann folgt durch Nachrechnen:

4. 2. 4 Proposition. *In $\mathfrak{R}_f := (R_f, \oplus, \circ)$ besitzt jedes Element eine Darstellung*

$$\overline{a}_0 \oplus \overline{a}_1 \circ x^1 \oplus \overline{a}_2 \circ x^2 \oplus \ldots \oplus \overline{a}_n \circ x^n$$

und wir erhalten ferner fast unmittelbar:

4. 2. 5 Proposition. *$(R, +, \cdot) \cong \big(\{ \overline{a} \,\big|\, a \in R \}, \oplus, \circ \big)$ via $a \mapsto \overline{a}$.*

Somit lässt sich $(R, +, \cdot)$ *einbetten* in $(R_f, \oplus, \circ)$, denn wir können ja die Elemente $\overline{a}$ austauschen gegen die Elemente a aus R. Gilt nach diesem Prozess nämlich $a = b$, so hatten wir $\overline{a} = \overline{b}$ in $\mathfrak{R}_f$ und damit auch $a = b$ in $\mathfrak{R}$.

4. 2. 6 Definition. Im folgenden bezeichnen wir die eindeutig bestimmten Summen $\sum_0^n a_i x^i$ als *Polynome* über $\mathfrak{R}$ und entsprechend $\mathfrak{R}_f =: \mathfrak{R}[x]$ auch als *Polynomring* über $\mathfrak{R}$.

Weiter symbolisieren wir die Summen $\sum_0^n a_i x^i$ durch Abkürzungen der Form $f(x), g(x)$ etc. oder auch kurz durch $f, g, \ldots$, wenn klar ist, dass f bzw. g aus $\mathfrak{R}[x]$ stammen.

Schließlich bezeichnen wir den höchsten in f effektiv auftretenden Exponenten als den *Grad* von f, i. Z. grad (f).

Fazit: Ist $\mathfrak{R}$ ein kommutativer Ring mit 1, so existiert ein $x \notin R$ derart, dass man x mit den Elementen aus $\mathfrak{R}$ *verknüpfen* kann, als gehöre x zu $\mathfrak{R}$, ohne dass irgendein Paar $a \neq b$ *kollabiert* und derart, dass $\sum_0^n a_i x^i = 0$ genau dann erfüllt ist, wenn $a_i = 0$ erfüllt ist für alle $0 \leq i \leq n$.

Im weiteren werden wir wie üblich kurz $f+g$ statt $f \oplus g$ schreiben und analog fg statt $f \circ g$.

Es sei nun $\mathfrak{R}'$ ein Oberring zu $\mathfrak{R}$ und $\alpha \in R'$. Dann lässt sich jedem $f(x)$ eindeutig das Element $f(\alpha)$ zuordnen, und man sieht fast unmittelbar, dass sich unter dieser Abbildung, also unter $x \mapsto \alpha$ und $r \mapsto r \quad (r \in R)$

$$\begin{array}{rrcl} & f(x)+g(x) & \mapsto & f(\alpha)+g(\alpha) \\ \text{und} & f(x)\cdot g(x) & \mapsto & f(\alpha)\cdot g(\alpha) \end{array}$$

einstellt. Dies halten wir fest:

4. 2. 7 Proposition. *Der Ring aller Polynome $f(x)$ lässt sich homomorph abbilden auf jeden Ring $\mathfrak{R}[\alpha]$, gebildet aus allen Formen $\sum_1^n a_i \alpha^i$.*

Aus diesem Grunde gilt:

4. 2. 8 Proposition. *Ist $\mathfrak{S}$ ein Oberring von $\mathfrak{R}$ und die 0 aus $\mathfrak{S}$ nur trivial darstellbar, also jedes Element eindeutig darstellbar als $\sum_1^n a_i y^i$, so ist $\mathfrak{S}$ isomorph zu $\mathfrak{R}_f$.*

Denn: die Abbildung

$$\sum_1^n a_i x^i \longmapsto \sum_1^n a_i y^i$$

liefert einen Homomorphismus und gilt $\sum_1^n a_i y^i = 0$, so müssen alle a_i verschwinden, weshalb $\mathfrak{R}_f$ und $\mathfrak{S}$ sogar isomorph sind. □

Implizit ist damit dann auch gezeigt, dass $\mathfrak{R}[x]$ durch die Eigenschaft, auf jedes $\mathfrak{R}[\alpha]$ homomorph abbildbar zu sein, bis auf Isomorphie eindeutig bestimmt ist.

Dies rechtfertigt es, $\mathfrak{R}[x]$ als die *transzendente Erweiterung* von $\mathfrak{R}$ zu bezeichnen, wobei das Wort transzendent für die Eigenschaft steht, dass nur

die triviale *lineare R-Kombination* über den Potenzen von x verschwindet, d. h. den Wert 0 liefert, alle übrigen Kombinationen hingegen Werte „jenseits" von R.

Man beachte: Ist $\mathfrak{Q}$ der Ring der rationalen Zahlen, so ist etwa π transzendent über $\mathfrak{Q}$. Das bedeutet, dass $\mathfrak{Q}[\pi]$ isomorph ist zu $\mathfrak{Q}[x]$, also aus algebraischer Sicht kein Unterschied auszumachen ist zwischen $\mathfrak{Q}[x]$ und $\mathfrak{Q}[\pi]$, insbesondere also auch, dass $\mathfrak{Q}[x]$ *total geordnet* angenommen werden darf.

Im Gegensatz zu transzendent nennt man ein Element α *algebraisch* über einem Ring $\mathfrak{R}$, wenn α Nullstelle eines Polynoms über $\mathfrak{R}$ ist, also mit seinen Potenzen eine nicht triviale lineare R-Kombination der 0 zulässt.

Ist $\mathfrak{R}$ sogar ein Integritätsbereich, so gilt offenbar die Gradformel

$$\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g).$$

Deshalb ist mit $\mathfrak{R}$ auch $\mathfrak{R}[x]$ ein Integritätsbereich.

Somit können wir formulieren:

Mit $\mathfrak{R}$ ist auch $\mathfrak{R}[x]$ ein Ring bzw. ein Integritätsbereich. Demzufolge können wir in der Konstruktion transzendenter Ringerweiterungen fortschreiten, also von $\mathfrak{R}[x_1]$ zu $\big(\mathfrak{R}[x_1]\big)[x_2] =: \mathfrak{R}[x_1, x_2]$ gelangen usf. Auf diese Weise erhalten wir dann Polynome in mehreren – etwa in n – Veränderlichen, und es ist diese Erweiterung von $\mathfrak{R}$ genau dann ein Integritätsbereich, wenn $\mathfrak{R}$ ein Integritätsbereich ist.

Wir betrachten $\mathfrak{R}[x_1, \ldots, x_n]$. Hier „begegnen" uns Glieder der Form

$$r \cdot x_1^{e_1} \cdot \ldots \cdot x_n^{e_n} \quad (r \in R),$$

und wir können diese Summanden *lexikographisch ordnen*, d. h.

$$r \cdot x_1^{a_1} \cdot \ldots \cdot x_n^{a_n} \text{ vor } s \cdot x_1^{b_1} \cdot \ldots \cdot x_n^{b_n}$$

genau dann setzen, wenn an der ersten Stelle i, an der a_i und b_i differieren, der Exponent a_i von dem Exponenten b_i übertroffen wird. Das Glied, welches nach dieser Ordnung am weitesten rechts steht, nennen wir auch das höchste Glied.

4. 2. 9 Definition. Ist f aus $\mathfrak{R}[x_1, \ldots, x_n]$ so verstehen wir unter dem Grad von f, i. Z. $\operatorname{grad}(f)$, das Maximum der Exponentensummen $e_1 + \ldots + e_n$.

Wie man erneut sofort sieht, gilt die oben formulierte Grad-Formel für Integritätsbereiche auch im mehrdimensionalen Fall. Folglich ist auch hier das „höchste Glied" eines Produktes gleich dem Produkt der „höchsten Glieder" der Faktoren.

Ferner mache man sich klar, dass ein f genau dann nicht verschwindet, wenn das eindeutig bestimmte höchste Glied nicht verschwindet.

Schließlich beachte man, dass ein Polynom f aus $\mathfrak{K}[x_1, \ldots, x_n]$ genau dann den Wert 0 annimmt, wenn seine sämtlichen Koeffizienten verschwinden, was sich fast unmittelbar ergibt.

Das bedeutet dann u.a., dass jedes Element aus $K[x_1, \ldots, x_n] - K$ transzendent ist über $\mathfrak{K}$.

4. 2. 10 Definition. Sei $f(x_1, \ldots, x_n)$ aus $\mathfrak{R}[x_1, \ldots, x_n]$. Dann heißt f symmetrisch in $x_1, \ldots, x_n$, wenn sich der Wert von f unter den Permutationen π von $(1, \ldots, n)$ nicht ändert.

Beispiele für symmetrische Funktionen sind zunächst die sogenannten *elementarsymmetrischen* Funktionen:

$$\begin{aligned}
\sigma_1(x_1, \ldots, x_n) &:= x_1 + x_2 + \ldots\ldots + x_n \\
\sigma_2(x_1, \ldots, x_n) &:= x_1x_2 + x_1x_3 + \ldots\ldots + x_{n-1}x_n \\
\sigma_3(x_1, \ldots, x_n) &:= x_1x_2x_3 + \ldots\ldots + x_{n-2}x_{n-1}x_n \\
&\vdots \quad \vdots \quad \vdots \\
\sigma_n(x_1, \ldots, x_n) &:= x_1x_2 \cdot \ldots \cdot x_n .
\end{aligned}$$

Ferner sind natürlich die Funktionen $(\sigma_i)^n$ symmetrisch und selbstverständlich auch alle Polynome in symmetrischen Funktionen, also Polynome vom Typ $p(f_1, \ldots, f_n)$ mit symmetrischen Polynomen $f_i \ \ (1 \leq i \leq n)$.

Andererseits ist die Klasse der symmetrischen Funktionen sehr eng. Denn es gilt:

4. 2. 11 Der Hauptsatz über symmetrische Funktionen.

Sei $f(x_1, \ldots, x_n)$ symmetrisch in $x_1, \ldots, x_n$. Dann ist $f(x_1, \ldots, x_n)$ darstellbar als Polynom in den elementar-symmetrischen Funktionen $\sigma_1, \ldots, \sigma_n$ und diese Darstellung ist eindeutig.

BEWEIS. (a) Wir beginnen mit der Darstellbarkeit.

Der Beweis erfolgt durch Reduktion. Sei zunächst $a \cdot x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$ der nach der oben eingeführten Ordnung *höchste Summand* von $f(x_1, \ldots, x_n)$. Dann gilt $a_1 \geq a_2 \geq \ldots \geq a_n$, denn mit $a \cdot x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$ gehört auch jedes $a \cdot x_1^{a_{\pi(1)}} \cdot \ldots \cdot x_n^{a_{\pi(n)}}$ als Summand zu f.

Wir beachten nun, dass $\sigma_1^{a_1 - a_2}$ als höchsten Summanden $x^{a_1 - a_2}$ liefert, $\sigma_2^{a_2 - a_3}$ als höchsten Summanden $x_1^{a_2 - a_3} x_2^{a_2 - a_3}$, weiterhin $\sigma_3^{a_3 - a_4}$ als höchsten Summanden $x_1^{a_3 - a_4} x_2^{a_3 - a_4} x_3^{a_3 - a_4}$ usf., weshalb dann $a \cdot \sigma_1^{a_1 - a_2} \cdot \sigma_2^{a_2 - a_3} \cdot \ldots \cdot \sigma_n^{a_n}$ als höchsten Summanden $a \cdot x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$ von f liefert. Das bedeutet aber: Bilden wir das Polynom

$$g_1(x_1, \ldots, x_n) := a \cdot \sigma_1^{a_1 - a_2} \cdot \sigma_2^{a_2 - a_3} \cdot \ldots \cdot \sigma_n^{a_n}$$

und hiernach $f - g_1 =: f_1$, so ist mit f und g_1 auch $f - g_1$ symmetrisch, und es liegt das höchste Glied von f_1 echt unter dem höchsten Glied von f.

Somit lässt sich f sukzessive abbauen bis

$$f - g_1 - g_2 - \ldots - g_m = 0$$

also

$$f = g_1 + g_2 + \ldots + g_m$$

eintritt, f also als Polynom in $\sigma_1, \ldots, \sigma_n$ dargestellt ist.

(b) Wir kommen nun zur Eindeutigkeit.

Es genügt zu zeigen, dass mit $f(x_1, \ldots, x_n)$ auch $f(\sigma_1, \ldots, \sigma_n)$ nicht verschwindet.

Sei also ein $f(x_1, \ldots, x_n)$ und hier ein beliebiges Glied gegeben. Dann können wir zunächst dieses Glied in der Form

$$a \cdot {x_1}^{k_1 - k_2} \cdot \ldots \cdot {x_n}^{k_{n-1} - k_n} \cdot {x_n}^{k_n} \quad (k_1 \geq \ldots \geq k_n) \tag{4.2}$$

schreiben. Wie schon oben angemerkt ist aber das höchste Glied eines Produktes gleich dem Produkt der höchsten Glieder. Folglich ist dann:

$$a \cdot {x_1}^{k_1 - k_2} \cdot (x_1 x_2)^{k_2 - k_3} \cdot \ldots \cdot (x_1 \cdot \ldots \cdot x_{n-1})^{k_{n-1} - k_n} \cdot (x_1 \cdot \ldots \cdot x_n)^{k_n}$$

das höchste Glied von $a \cdot {\sigma_1}^{k_1 - k_2} \cdot \ldots \cdot {\sigma_{n-1}}^{k_{n-1} - k_n} \cdot {\sigma_n}^{k_n}$.

Andererseits ist der Wert dieses Gliedes gleich

$$a \cdot {x_1}^{k_1} \cdot \ldots \cdot {x_n}^{k_n}. \tag{4.3}$$

Folglich hebt sich für den Fall, dass $a x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$ als das lexikographisch höchste Glied von f gewählt wurde, (4.3) nicht weg. Also gilt $f(\sigma_1, \ldots, \sigma_n) \neq 0$. □

Kapitel 5

Einbettungen

5.1 Quotientengruppen

5. 1. 1 Definition. Als Halbgruppe mit 0 bezeichnen wir jede Halbgruppe mit Nullelement. Als kürzbare Halbgruppe mit 0 bezeichnen wir jede Halbgruppe mit 0, die zusätzlich der Implikation $a \neq 0 \;\&\; ax = ay \Longrightarrow x = y$ genügt. Analog definieren wir den Begriff Gruppe mit 0.

Anschaulich entsteht also die Gruppe mit 0 durch Adjunktion eines Elements 0 zur Trägermenge G und die hiernach erfolgende Festsetzung $a{\cdot}0 := 0 =: 0{\cdot}a$.

5. 1. 2 Proposition. *Sei* $(H^0, \cdot)$ *eine kommutative kürzbare Halbgruppe mit* 0. *Dann lässt sich* $(H^0, \cdot)$ *einbetten in eine Gruppe mit* 0.

BEWEIS.

(a) Wir bezeichnen $H^0 \backslash \{0\}$ mit H und bilden $H^0 \times H$.

(b) Wir definieren auf $H^0 \times H$ die Operation $\circ$ vermöge

$$(a|b) \circ (c|d) := (ac \,\big|\, bd)$$

und sehen

(c) $\circ$ ist assoziativ und kommutativ.

(d) Wir definieren

$$(a \,\big|\, b) \sim (c \,\big|\, d) :\Longleftrightarrow ad = bc$$

und sehen:

(e) $\sim$ ist eine Äquivalenzrelation, denn: $\sim$ ist offenbar reflexiv und symmetrisch, und es gilt ferner

$$\begin{array}{rrcl|rcl} & (a\,|\,b) & \sim & (c\,|\,d) & \& & (c\,|\,d) & \sim & (g\,|\,h) \\ \Longrightarrow & ad & = & bc & \& & ch & = & dg \\ \Longrightarrow & adh & = & bch & \& & bch & = & bdg \\ \Longrightarrow & ah & = & & bch & & = & bg \\ \Longrightarrow & (a|b) & \sim & (g|h) & & & & & \end{array}$$

(f) $\sim$ ist eine Kongruenzrelation auf $(H^0 \times H, \circ)$, denn:

$$\begin{array}{rrcl} (a,b) \sim (c|d) & \Longrightarrow & ad & = & bc \\ & \Longrightarrow & au \cdot dv & = & bu \cdot cv \\ & \Longrightarrow & (a\,|\,b)(u|v) & \sim & (c\,|\,d) \cdot (u\,|\,v). \end{array}$$

(g) Es gelten die Äquivalenzen:

$$\begin{array}{rcl} (0\,|\,x) & \sim & (0\,|\,y) \\ (x\,|\,x) & \sim & (y\,|\,y) \\ (ax\,|\,ax) & \sim & (a\,|\,a) \\ (ax\,|\,x) & \sim & (ay\,|\,y) \end{array}$$

sowie

$$(ax\,|\,x) \circ (by\,|\,y) \sim (ab \cdot x\,|\,x)$$

(h) Wir bezeichnen die durch $(ax\,|\,x)$ bestimmte $\sim$-Klasse mit $\overline{a}$ und die durch $(a\,|\,b)$ bestimmte $\sim$-Klasse mit $\overline{(a\,|\,b)}$. Dann folgt sofort

$$\overline{a} \circ \overline{b} = \overline{a \cdot b},$$

und somit die Isomorphie von $(H, \cdot)$ und $\big(\{\overline{a} \mid a \in H\}, \circ\big)$, und es gilt ferner:

$$\begin{array}{rcl} \overline{(a\,|\,b)} \circ \overline{(0\,|\,x)} & = & \overline{(0\,|\,x)} \\ \big(\overline{(a\,|\,b)} \circ \overline{(c\,|\,d)}\big) \circ \overline{(g\,|\,h)} & = & \overline{(a\,|\,b)} \circ \big(\overline{(c\,|\,d)} \circ \overline{(g\,|\,h)}\big) \\ \overline{(a\,|\,b)} \circ \overline{(c\,|\,d)} & = & \overline{(c\,|\,d)} \circ \overline{(a\,|\,b)} \\ \overline{(a\,|\,b)} \circ \overline{(x\,|\,x)} & = & \overline{(a\,|\,b)} \end{array}$$

sowie

$$a \neq 0 \Longrightarrow \overline{(a\,|\,b)} \circ \overline{(b\,|\,a)} = \overline{(x\,|\,x)}\,.$$

(i) Daher ist $(H^0 \times H, \circ)/\!\sim$ eine Halbgruppe mit $\overline{(0\,|\,x)}$ als Null, $\overline{(x\,|\,x)}$ als Eins – und mit $\overline{(b\,|\,a)}$ als $\overline{(a\,|\,b)}^{-1}$, falls $a \neq 0$. Das bedeutet aber, dass

die Klassen $(\overline{a \,\big|\, b})$ mit $a \neq 0 \neq b$ eine abelsche Gruppe bilden, da die Menge dieser Klassen $\circ$-abgeschlossen ist. Man beachte:

$$(a \,\big|\, b) \circ (c \,\big|\, d) \sim (0 \,\big|\, x) \Longrightarrow (ac \,\big|\, bd) \sim (0 \,\big|\, x) \Longrightarrow acx = 0. \qquad \square$$

Mit 5.1.1 haben wir die Einbettbarkeit bewiesen. Wir demonstrieren nun ihre Eindeutigkeit.

5. 1. 3 Proposition. *Sei $(H^0, \cdot)$ Unterhalbgruppe mit 0 einer abelschen Gruppe mit 0. Damit ist die Menge Q_G aller Quotienten ab^{-1} mit $a \in H^0$, $b \in H$ abgeschlossen bezüglich $\circ$, und es gilt:*

$$\big(Q_G^o, \cdot\big) \;\cong\; \big(H^0 \times H, \circ\big)\big/ \sim$$

BEWEIS. (a) Q_G^o ist abgeschlossen bezüglich $\cdot$. Denn es gilt die Gleichung $ab^{-1} \cdot cd^{-1} = (ac) \cdot (bd)^{-1}$.

(b) Wir definieren nun:

$$\phi : (\overline{a \,\big|\, b}) \mapsto ab^{-1}.$$

Dann folgt:

(c) ϕ ist eine Funktion, denn

$$\begin{aligned} (a \,\big|\, b) = (c \,\big|\, d) &\Longrightarrow ad = bc \\ &\Longrightarrow ab^{-1} = cd^{-1}. \end{aligned}$$

(d) ϕ ist surjektiv, denn

$$ab^{-1} \;=\; \phi(\overline{a \,\big|\, b})$$

(e) ϕ ist injektiv, denn

$$\begin{aligned} (\overline{a \,\big|\, b}) \neq (\overline{c \,\big|\, d}) &\Longrightarrow ad \neq bc \\ &\Longrightarrow ab^{-1} \neq cd^{-1}. \end{aligned}$$

(f) ϕ ist ein Homomorphismus, denn

$$\begin{aligned} \phi\big((\overline{a \,\big|\, b}) \circ (\overline{c \,\big|\, d})\big) &= \phi(ac \,\big|\, bd) \\ &= (ac)(bc)^{-1} \\ &= (ab^{-1}) \cdot (cd^{-1}) \\ &= \phi(a \,\big|\, b) \cdot \phi(c \,\big|\, d). \end{aligned}$$

$\square$

5.2 Quotienten- und Differenzen-Ringoide

Im folgenden wollen wir die hergeleiteten Regeln auch auf komplexere Strukturen anwenden. Hierzu:

5. 2. 1 Definition. Unter einem kommutativen *Ringoid* verstehen wir jede Algebra $(R, \cdot, \oplus)$ die sowohl bezüglich $\cdot$ als auch bezüglich $\oplus$ eine kommutative Halbgruppe bildet und zudem die Distributivgesetze

$$a(b \oplus c) = ab \oplus ac \quad \text{und} \quad (a \oplus b)c = ac \oplus bc$$

erfüllt.

Als klassische Beispiele, die nicht schon Ring sind, seien genannt $(\mathbf{N}, \cdot, +)$ und $(\mathbf{N}, \cdot, \wedge)$ mit $\wedge$ als Symbol für den *größten gemeinsamen Teiler* , abgekürzt durch GGT.

Das Ringoid ist sehr allgemein gefasst, erfüllt aber wegen des Distributivgesetzes aus kombinatorischen Gründen immerhin stets die binomische Formel

$$(a+b)^n = \sum_1^n \binom{n}{k} a^{n-k} b^k$$

5. 2. 2 Proposition. *Sei $(R^0, \cdot, \oplus)$ ein Ringoid, sei $(R^0, \cdot)$ eine kürzbare abelsche Halbgruppe mit 0, sei $(R, \oplus)$ eine abelsche Halbgruppe. Dann lässt sich $(R^0, \cdot, \oplus)$ einbetten in ein Ringoid $(S^0, \cdot, \oplus)$ mit den Eigenschaften:*

- *(i)* $(S^0, \cdot)$ *ist eine abelsche Gruppe mit* 0 .
- *(ii)* $(S^0, \cdot, \oplus)$ *ist eine abelsche Halbgruppe.*

BEWEIS. Es genügt zu zeigen, dass die Operation $\oplus$ sich ausdehnen lässt auf $(R^0 \oplus R)/\sim$, so dass die Gleichungen gelten:

$$\begin{aligned}
&\text{(E)} && (\overline{ax \mid x}) \oplus (\overline{bx \mid x}) &&= \big(\overline{(a \oplus b)x^2 | x^2}\big) \\
&\text{(K)} && (\overline{a \mid b}) \oplus (\overline{c \mid d}) &&= (\overline{c \mid d}) \oplus (\overline{a \mid b}) \\
&\text{(A)} && \big((\overline{a \mid b}) \oplus (\overline{c \mid d})\big) \oplus (\overline{g \mid h}) &&= (\overline{a \mid b}) \oplus \big((\overline{c \mid d}) \oplus (\overline{g \mid h})\big) \\
&\text{(D)} && (\overline{a \mid b}) \circ \big((\overline{c \mid d}) \oplus (\overline{g \mid h})\big) &&= (\overline{a \mid b}) \circ (\overline{c \mid d}) \oplus (\overline{a \mid b}) \circ (\overline{g \mid h}).
\end{aligned}$$

Zu diesem Zweck definieren wir

$$(\overline{a \,|\, b}) \oplus (\overline{c \,|\, d}) := (\overline{ad} \oplus \overline{bc} \,\big|\, \overline{bd})$$

und erhalten:

(a) $\oplus$ ist eine Operation, denn:

$$\begin{aligned} (c \,|\, d) \sim (g \,|\, h) \implies & (a \,|\, b) \oplus (c \,|\, d) = (ad \oplus bc \,|\, bd) \\ \& \quad & (a \,|\, b) \oplus (g \,|\, h) = (ah \oplus bg \,|\, bh) \\ \implies & (a \,|\, b) \oplus (c \,|\, d) \sim (a \,|\, b) \oplus (g \,|\, h), \end{aligned}$$

wegen

$$ch = dg \implies adbh \oplus bcbh = ahbd \oplus bgbd \ .$$

(b) $\oplus$ erfüllt die aufgeführten Gesetze (E), (K), (A), (D),

BEWEIS: Übung. □

Satz 5.2.2 liefert zwei klassische Korollare und zwar zum einen

(i) $(\mathbf{Z}, +, \cdot)$ besitzt mit $(\mathbf{Q}, +, \cdot)$ eine im wesentlichen eindeutige Quotienten-Erweiterung,

und zum anderen

(ii) $(\mathbf{N}, \wedge, \cdot)$ besitzt eine eindeutige Quotienten-Erweiterung in die *Verbandsgruppe* (der Leser nehme diese Bezeichnung hier hin), nämlich in

$$(\mathbf{Q}^+, 1, \cdot) \text{ mit } \frac{p}{q} \wedge \frac{r}{s} := \frac{ps \wedge rq}{qs} \,.$$

Insbesondere haben wir

5. 2. 3 Korollar. *Sei $(R, +, \cdot)$ ein Integritätsbereich. Dann lässt sich $(R, +, \cdot)$ einbetten in einen Quotientenkörper und dieser ist i.w. eindeutig bestimmt.*

DENN: man verfahre wie im Falle des Eindeutigkeitsbeweises für Quotientengruppen. □

DENN: Es ist die Existenz eines negativen Elements zu $(\overline{a \,|\, b})$ nachzuweisen, was sich mit $-(\overline{a \,|\, b}) := (\overline{-a \,|\, b})$ erledigt. □

Wir sind bislang ausgegangen von Ringoiden $(R, \oplus, \cdot)$ mit kürzbarer Multiplikation und haben Quotientenerweiterungen betrachtet.

Sei nun $(R, \oplus)$ eine kürzbare abelsche Halbgruppe. Dann lässt sich $(R, \oplus)$ natürlich einbetten in eine abelsche Gruppe von Differenzen, und es stellt sich die Frage, ob sich in diesem Falle die Multiplikation $\cdot$ zufrieden stellend von R auf $(R \oplus R, \oplus)/\!\sim$ ausdehnen lässt. Hier gilt:

5. 2. 4 Proposition. *Sei $(R, \oplus, \cdot)$ ein assoziatives und kommutatives Ringoid mit kürzbarer Halbgruppe $(R, \oplus)$. Dann lässt sich $(R, \oplus, \cdot)$ einbetten in ein Oberringoid $(S, \oplus, \cdot)$, dessen $(S, \oplus)$ sogar Gruppe ist.*

HINWEIS:

(i) Definiere: $(\overline{a \mid b}) \circ (\overline{c \mid d}) := (\overline{ac \oplus bd \,\big|\, ad \oplus bc})$

(ii) und zeige:

(a) $\circ$ ist assoziativ

(b) $\circ$ ist kommutativ

(d) $\circ$ und $\oplus$ sind distributiv gekoppelt.

5. 2. 5 Proposition. *Die unter 5. 2. 4 angegebene Differenzenerweiterung ist – so wie die unter 5. 2. 2 angegebene Quotientenerweiterung – im wesentlichen eindeutig bestimmt.*

BEWEIS. Übung □

Kapitel 6

Teilbarkeitsaspekte

6.1 Die Teilerrelation

6. 1. 1 Definition. Sei $\mathfrak{S}$ ein *abelsches Monoid.* Dann setzen wir:

$$\begin{aligned} a \mid b &:\Longleftrightarrow a \cdot x = b \ (\exists x) \\ a \parallel b &:\Longleftrightarrow a \mid b \ \& \ b \nmid a \\ a \sim b &:\Longleftrightarrow a \mid b \ \& \ b \mid a \\ a \equiv b &:\Longleftrightarrow a = b \cdot \varepsilon = b \ (\varepsilon \mid 1) \end{aligned}$$

und nennen a einen *Teiler* von b, wenn $a \mid b$ erfüllt ist, a einen *echten* Teiler von b, wenn $a \parallel b$ erfüllt ist, a *äquivalent* zu b, wenn $a \sim b$ erfüllt ist, und a *assoziiert* zu b, wenn $a \equiv b$ erfüllt ist.

Ist insbesondere a ein Teiler der 1, so nennen wir a einen *Einsteiler*

Statt „a ist Teiler von b" sagen wir auch „b ist *Vielfaches von a".*

6. 1. 2 Proposition. *Sei $\mathfrak{S}$ ein abelsches Monoid. Dann bildet die Menge aller Einsteiler aus $\mathfrak{S}$ eine Gruppe.*

Denn: dies ist fast evident. □

6. 1. 3 Proposition. *Sei $\mathfrak{S}$ ein abelsches Monoid. Dann gilt:*

(*i*) *Die Relation $\mid$ ist* reflexiv und transitiv.
(*ii*) *Die Relation $\sim$ ist eine Kongruenzrelation.*
(*iii*) *die Relation $\equiv$ ist eine Kongruenzrelation.*
(*iv*) *Ist $\mathfrak{S}$ sogar kürzbar, so gilt $\sim \ = \ \equiv$.*

BEWEIS. Zu (i) :

$$\begin{array}{rcl} a = a \cdot 1 & \rightsquigarrow & a \,|\, a \\ & \& & \\ a \,|\, b \;\&\; b \,|\, c & \Longrightarrow & c = b \cdot y \;\&\; b = a \cdot x \;\; (\exists x, y) \\ & \Longrightarrow & c = a(xy) \\ & \Longrightarrow & a \,|\, c\,. \end{array}$$

Zu (ii) : Zunächst folgen die Eigenschaften der Äquivalenz aus (i). Es ist aber $\sim$ auch *verträglich*, wegen:

$$\begin{array}{rcl} a \sim b & \Longrightarrow & ax = b \;\&\; by = a \;\; (\exists x, y) \\ & \Longrightarrow & (ca)x = cb \;\&\; (cb)y = ca \\ & \Longrightarrow & ca \sim cb\,. \end{array}$$

Zu (iii) : Es gilt $a \cdot 1 = a$, also ist $\equiv$ reflexiv, und es gilt die Implikation $a\varepsilon = b \Longrightarrow a = b \cdot \varepsilon^{-1}$. Also ist $\equiv$ symmetrisch. Weiter haben wir $a \cdot \varepsilon_1 = b \;\&\; b \cdot \varepsilon_2 = c \Longrightarrow a \cdot (\varepsilon_1\varepsilon_2) = c$.

Schließlich folgt die Verträglichkeit von $\equiv$ mit der Multiplikation unmittelbar.

Zu (iv) : Ist $\mathfrak{S}$ kürzbar und gilt $ax = b \;\&\; by = a$, so folgt $a(xy) = a$, also $xy = 1$. □

6. 1. 4 Lemma. *Bezeichnen wir die Klassen von $\mathfrak{S}$ bezüglich $\sim$ mit $\overline{a}, \overline{b}, \ldots$, so gilt*

$$a \,|\, b \Longleftrightarrow \overline{a} \,|\, \overline{b}\,.$$

DENN: $a \,|\, b \Longrightarrow b = ax \,(\exists x) \Longrightarrow \overline{b} \,|\, \overline{ax} \Longrightarrow a(xz) = b \Longrightarrow a \,|\, b\,.$ □

6. 1. 5 Proposition. *Sei $\mathfrak{S}$ ein abelsches Monoid. Dann gilt:*

$$\overline{a} \,|\, \overline{b} \;\&\; \overline{b} \,|\, \overline{a} \Longrightarrow \overline{a} = \overline{b}\,.$$

DENN: $\overline{a} \,|\, \overline{b} \;\&\; \overline{b} \,|\, \overline{a} \Longrightarrow a \,|\, b \;\&\; b \,|\, a \Longrightarrow a \sim b \Longrightarrow \overline{a} \,|\, \overline{b}\,.$ □

Dass die Relationen$\sim$ und $\equiv$ auch in kommutativen Ringen mit 1 nicht übereinstimmen müssen, zeigt uns der *Ring der stetigen Funktionen* von $\mathbf{R}$ nach $\mathbf{R}$.

Erklären wir hier Funktionen f und g, indem wir sie links von 0 vermöge $f(x) = x$ und $g(x) = |x|$ festlegen, auf dem *Einheitsintervall* $f(x) = g(x) = 0$

wählen und rechts vom Einheitsintervall irgendwie $f(x) = g(x) \neq 0$ definieren, so sind diese beiden Funktionen in dem von uns betrachteten Ring der stetigen Funktionen zwar äquivalent, nicht aber assoziiert.

Für das weitere vereinbaren wir

$$T(a) := \{t \,\big|\, \ t|a\} \quad \text{und} \quad V(a) := \{v \,\big|\, \ a|v\}\,.$$

Mit dieser Bezeichnung können wir formulieren:

6. 1. 6 Definition. Seien a, b zwei Elemente aus S. Dann bezeichnen wir c als einen GGT *(größten gemeinsamen Teiler)* zu a, b, wenn gilt $T(a) \cap T(b) = T(c)$, und wir bezeichnen d als ein KGV (*kleinstes gemeinsames Vielfaches*) zu a, b wenn gilt $V(a) \cap V(b) = V(d)$.

Der Leser beachte, dass alle bisherigen Vereinbarungen natürlich auch für die multiplikative Halbgruppe eines kommutativen Ringes gelten. Hier resultieren dann insbesondere idealtheoretische Zusammenhänge. So folgt beispielsweise unmittelbar:

6. 1. 7 Lemma. *Sei $\mathfrak{R}$ ein kommutativer Ring mit 1. Dann gilt*

$$a \,\big|\, b \Longleftrightarrow b \in (a) \Longleftrightarrow (a) \supseteq (b)\,.$$

oder auch

6. 1. 8 Lemma. $(a, b) = (c) \Longrightarrow$ *c ist ein GGT zu a und b.*

Denn: Gilt die Prämisse, so ist c natürlich ein Teiler zu a, b, und es folgt $c = ax + by \ \ (\exists x, y \in R)$. Dies liefert aber mit geeigneten Elementen u, v

$$\begin{aligned} t \,\big|\, a, b \ &\Longrightarrow \ tu = a, tv = b \\ &\Longrightarrow \ c = t \cdot ux + t \cdot vy = t \cdot (ux + vy)\,. \end{aligned}$$

□

Wie man leicht induziert ist schon dann jedes *endlich erzeugte* Ideal eines Ringes ein Hauptideal, wenn jedes 2-*erzeugte* Ideal ein Hauptideal ist. Ringe mit dieser Eigenschaft werden zu Ehren des französischen Mathematikers Bézout als *Bézout–Ringe* bezeichnet. Sie haben eine extrem starke Theorie. Noch stärker ist natürlich die Theorie der so genannten *Hauptidealringe*, denen wir uns im übernächsten Abschnitt zuwenden wollen.

Hierzu an dieser Stelle nur

6. 1. 9 Korollar. *Sei $\mathfrak{R}$ ein Hauptidealring. Dann erhält man exakt alle Kongruenzen von $\mathfrak{R}$ als Kongruenzen modulo einem Element m via*

$$a \equiv b \ mod\ m :\Longleftrightarrow: m \,\Big|\, a - b\,.$$

6.2 Euklidische Ringe

6. 2. 1 Definition. Sei $\mathfrak{R}$ ein kommutativer Ring mit 1. Dann heißt $\mathfrak{R}$ ein *Euklidischer Ring*, wenn sich auf R eine Normfunktion

$$\phi: \ R \mapsto \mathbf{N}^0$$

erklären lässt, mit

(E1) $\quad \phi(a) = 0 \Longleftrightarrow a = 0$

(E2) $\quad \phi(a \cdot b) = \phi(a)\phi(b)$

(E3) $\quad \forall a, b \neq 0\, \exists\, q, r: \ \ a = b \cdot q + r$ mit $\big(\phi(r) < \phi(b)\big)$.

Eine Normfunktion ist also stets ein *multiplikativer* Homomorphismus. Als eine erste unmittelbare Konsequenz aus (E1) bis (E3) erhalten wir:

6. 2. 2 Proposition. *Jeder euklidische Ring ist nullteilerfrei.*

Denn:

$$\begin{aligned} ab = 0 \ &\Longrightarrow \ \phi(ab) = 0 \\ &\Longrightarrow \ \phi(a)\phi(b) = 0 \\ &\Longrightarrow \ \phi(a) = 0 \ \vee \ \phi(b) = 0 \\ &\Longrightarrow \ a = 0 \vee b = 0\,. \end{aligned}$$ □

Es ist also jeder euklidische Ring ein Integritätsbereich. Weiter gilt für euklidische Ringe:

6. 2. 3 Lemma. $\quad \phi(a) = 1 \Longleftrightarrow a \,\Big|\, 1\,.$

Denn: zunächst haben wir für beliebige Elemente a

$$\phi(a) = \phi(a \cdot 1) = \phi(a) \cdot \phi(1) \rightsquigarrow \phi(1) = 1$$

und hieraus folgt

$$\begin{aligned}
\phi(a)=1 &\implies 1=aq+r \\
&\quad \text{mit } \phi(r)<1 \rightsquigarrow \phi(r)=0 \\
&\implies 1=aq+0 \\
&\implies a \,\big|\, 1 \\
&\implies 1=ax \ \ (\exists x) \\
&\implies \phi(a)\phi(x)=1 \\
&\implies \phi(a)=1\,,
\end{aligned}$$

was zu beweisen war. □

Euklidische Ringe sind benannt nach EUKLID (ca 300 v. Chr.) aufgrund des von ihm formulierten Verfahrens zur Bestimmung des GGT in $\mathbf{N}$.

6. 2. 4 Der euklidische Algorithmus. *Sind a und $b \neq 0$ aus R, so folgt sukzessive:*

$$\begin{array}{rcll}
a & = & b\cdot q + a_1 & \textit{mit} \quad \phi(a_1)<\phi(b) \\
b & = & a_1\cdot q_1 + a_2 & \textit{mit} \quad \phi(a_2)<\phi(a_1) \\
a_1 & = & a_2\cdot q_2 + a_3 & \textit{mit} \quad \phi(a_3)<\phi(a_2) \\
\vdots & & \ldots\ldots\ldots\ldots & \vdots \\
\vdots & & \ldots\ldots\ldots\ldots & \vdots \\
a_{n-1} & = & a_n\cdot q_n + a_{n+1} & \textit{mit} \quad \phi(a_{n+1})=0 \rightsquigarrow a_{n+1}=0\,,
\end{array}$$

und es ist a_n zum einen GGT zu a und b und zum andern Linearkombination von a und b.

BEWEIS. Teil 1 ist klar nach (E3). Weiter haben wir

$$\begin{aligned}
T(a)\cap T(b) &= T(b)\cap T(a_1) \\
&= T(a_1)\cap T(a_2) \\
&= T(a_2)\cap T(a_3) \\
&\ \ \vdots \\
&= T(a_n)\,,
\end{aligned}$$

denn ein t teilt schon dann alle Summanden einer n-gliedrigen Summe, wenn es die Summe und $n-1$ Summanden dieser Summe teilt. Somit ist a_n GGT zu a und b.

Ganz analog erhalten wir mit $\ell(\ )$ als Symbol für *Linearformen* (von unten nach oben):

$$\begin{aligned} a_n &= \ell_n(a_{n-1}, a_{n-2}) \\ a_{n-1} &= \ell_{n-1}(a_{n-2}, a_{n-3}) \\ a_{n-2} &= \ell_{n-2}(a_{n-3}, a_{n-4}) \\ &\vdots \\ a_1 &= \ell_1(a, b)\,. \\ &\rightsquigarrow \\ a_n &= \ell(a, b)\,. \end{aligned}$$

Damit sind wir am Ziel. □

Hiernach formulieren wir den alles entscheidenden Satz für Euklidische Ringe:

6. 2. 5 Theorem. *Jeder Euklidische Ring ist ein Hauptidealring.*

BEWEIS. Sei $\mathfrak{i}$ ein Ideal. Dann gibt es in $\mathfrak{i}$ unter den Elementen von nicht verschwindendem Betrag eines von kleinstem Betrag, etwa b. Das bedeutet für alle anderen Elemente $a = bq + r$ mit $\phi(r) < \phi(b)$. Nun liegt aber mit a, b auch $a - bq$, also r in $\mathfrak{i}$ und hieraus resultiert $\phi(r) = 0 \rightsquigarrow r = 0$, also $b \,\big|\, a$. □

Entwicklung einer Teilbarkeitslehre für Hauptidealbereiche bedeutet also u.a. auch ein Studium der Teilbarkeitsverhältnisse in Euklidischen Ringen. Aus diesem Grunde werden wir uns im nächsten Paragraphen von vorne herein mit Hauptidealbereichen befassen.

Doch zuvor noch einige Beispiele für Euklidische Ringe.

BEISPIEL 1: Sei $\mathfrak{Z}$ der Ring der ganzen Zahlen. Wir setzen

$$\phi(a) := |a|\,.$$

Dann ist ϕ eine Normfunktion, wie der Leser leicht bestätigt.

BEISPIEL 2: Sei $\mathbf{Q}[x]$ der Ring der Polynome über $\mathbf{Q}$ oder allgemeiner $\mathfrak{K}[x]$ der Ring der Polynome über irgendeinem Körper $\mathfrak{K}$. Wir setzen

$$\phi(0) := 0 \text{ und } \phi(f(x)) := 2^{\operatorname{grad}(f)} \text{ sonst}\,.$$

Dann ist ϕ eine Normfunktion.

DENN: (E1) und (E2) sind *per definitionem* erfüllt.

Weiter erhalten wir:

$$\forall\, f, g \,\exists\, q, r \,:\;\; f = g \cdot q + r \text{ mit } \phi(r) < \phi(g)\,.$$

Um dies zu zeigen verfahren wir wie folgt:

1. Gilt $\phi(f) < \phi(g)$, so haben wir

$$f = g \cdot 0 + f \text{ mit } \phi(f) < \phi(g)\,,$$

und sind damit am Ziel.

2. Gilt aber $\phi(f) \geq \phi(g)$, so haben wir $\text{grad}(f) \geq \text{grad}(g)$, also

$$\begin{array}{rcll} f & = & a_o + a_1 x + \ldots + a_n x^n & \\ g & = & b_o + b_1 x + \ldots + b_m x^m & \text{mit } n \geq m\,, \end{array}$$

und es gilt mit $\text{grad}(f) = n$

$$f - g\frac{a_n}{b_m}x^{n-m} =: f_1 \text{ mit } \text{grad}(f_1) < \text{grad}(f)\,.$$

Ist nun $\text{grad}(f_1) < \text{grad}(g)$, also $\phi(f_1) < \phi(g)$, so sind wir am Ziel. Sonst aber können wir wegen $\phi(f_1) > \phi(g)$ das Verfahren fortsetzen und so sukzessive zu einer Kette

$$\begin{array}{rcl} f - g \cdot q_1 & =: & f_1 \\ f_1 - g \cdot q_2 & =: & f_2 \\ f_2 - g \cdot q_3 & =: & f_3 \\ \vdots \quad \vdots & & \vdots \end{array}$$

gelangen, die wegen $\text{grad}(f) > \text{grad}(f_1) > \text{grad}(f_2) \ldots$ nach endlich vielen Schritten zu einem f_n mit $\text{grad}(f_n) < \text{grad}(g)$ führt. Das liefert dann $\phi(f_n) < \phi(g)$ und damit

$$f - gq_1 - gq_2 - \ldots - gq_n = f_n$$

$$\rightsquigarrow \;\; f = g(q_1 + \ldots q_n) + f_n \text{ mit } \phi(f_n) < \phi(g)\,.$$

Schließlich geben wir als

BEISPIEL 3: Sei $\mathbf{Z}(i)$ der Ring der *ganzen* GAUSS*'schen Zahlen*, also der Zahlen vom Typ $a + bi$ $(a, b \in \mathbf{Z})$. Wir setzen

$$\phi(a) := a^2 + b^2\,.$$

Dann ist ϕ eine Normfunktion.

DENN: Der Leser bestätigt leicht die Bedingungen (E1) und (E2).

Seien hiernach $a+bi$ und $c+di$ zwei ganze *Gauß*'sche Zahlen. Bilden wir dann den Quotienten

$$\frac{a+bi}{c+di} = \frac{a+bi}{c+di} \cdot \frac{c-di}{c-di} = \frac{ac+bd}{c^2+d^2} + \frac{(bc-ad)}{c^2+d^2} i \,,$$

so liegen die beiden Komponenten, wie man leicht sieht, von mindestens einer ganzen Zahl dem Betrag nach um höchstens $\frac{1}{2}$ entfernt, d.h. wir dürfen in dem oben betrachteten Bruch in der Form $(u+vi)+(r+si)$ mit $u, v \in \mathbf{Z}$, $r, s \in \mathbf{Q}$ und $r^2+s^2 < 1$ annehmen. Das bedeutet dann aber

$$a+bi = (c+di)(u+vi) + (r+si)(c+di) \,,$$

worin $(r+si)(c+di)$ eine ganze GAUSS 'sche Zahl ist, von kleinerer Norm als $c+di$.

6.3 Hauptidealbereiche

6. 3. 1 Definition. Ein Ring $\mathfrak{R}$ heißt ein *Hauptidealring*, wenn jedes Ideal ein Hauptideal, d.h. vom Typ (a) ist.

Ziel dieses Paragraphen ist eine gewisse Klärung der Struktur von Hauptidealbereichen, also nullteilerfreien Hauptidealringen.

Als eine erste *Evidenz* formulieren wir:

6. 3. 2 Proposition. *Ist $\mathfrak{R}$ ein Hauptidealring, so besitzen je zwei Elemente a, b einen GGT und ein KGV.*

DENN: es gilt mit geeigneten Elementen d, v

$$(a,b) = (d) \quad \text{und} \quad (a) \cap (b) = (v) \,. \qquad \square$$

Als nächstes erinnern wir an die Begriffe *Primelement* und *irreduzibles Element.* Schließlich erklären wir:

6. 3. 3 Definition. Sei $\mathfrak{R}$ ein kommutativer Ring. Dann heißt $\mathfrak{R}$ – zu Ehren von EMMY NOETHER – ein *Noetherscher Ring,* wenn jedes Ideal endlich erzeugt ist, wofür man auch sagt, wenn $\mathfrak{R}$ *den Basisatz erfüllt.*

6. 3. 4 Definition. Sei $\mathfrak{R}$ ein kommutativer Ring. Dann sagt man, $\mathfrak{R}$ erfülle die *aufsteigende Kettenbedingung,* wenn jede Kette von Idealen

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \mathfrak{a}_4 \subset \mathfrak{a}_5 \subset \ldots$$

nach endlich vielen Schritten abbricht.

Hiernach beweisen wir nacheinander:

6. 3. 5 Proposition. *Ein Ring $\mathfrak{R}$ erfüllt genau dann die aufsteigende Kettenbedingung, wenn er noethersch ist.*

BEWEIS. (a) Gelte zunächst der Basissatz.

Es folgt unmittelbar, dass $\mathfrak{a} := \bigcap \mathfrak{a}_i \ \ (n \in \mathbf{N})$ ein Ideal ist.

Nun ist aber $\mathfrak{a}$ vom Typ $(c_1, \ldots, c_k)$. Folglich gibt es ein erstes $\mathfrak{a}_m$ mit $c_1, c_2, \ldots, c_k \in \mathfrak{a}_m$. Und das bedeutet dann

$$\mathfrak{a} = (c_1, \ldots, c_k) \subseteq \mathfrak{a}_m \subseteq \mathfrak{a}_{m+k} \subseteq \mathfrak{a},$$

womit die erste Aussage bewiesen ist.

(b) Gelte hiernach die aufsteigende Kettenbedingung und sei $\mathfrak{a}$ ein beliebiges Ideal. Wählen wir dann sukzessive $a_1, a_2, a_3 \ldots$, so erhalten wir eine Kette $(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \ldots$, die nach dem Basissatz abbrechen muss. Folglich ist $\mathfrak{a}$ unter der gemachten Voraussetzung in der Tat endlich erzeugt. □

6. 3. 6 Proposition. *Sei $\mathfrak{R}$ ein noetherscher Integritätsbereich. Dann zerfällt jedes von 0 verschiedene Element, das kein Einsteiler ist, in irreduzible Elemente.*

BEWEIS. Gäbe es ein Element der angegebenen Art, das nicht in irreduzible Elemente zerfällt, so wäre die Menge aller Hauptideale (x) zu Elementen x dieser Art nicht leer, und sie erfüllte zudem die aufsteigende Kettenbedingung. Also gäbe es ein maximales (c) in dieser Menge.

Dieses Element c könnte dann aber nicht irreduzibel sein. Folglich gäbe es ein u mit $1 \parallel u \parallel c$ und $uv = c$. Damit müsste dann aber auch $1 \parallel v \parallel c$ erfüllt sein, da $v \sim 1$ unmittelbar und $v \sim p$ mittelbar zum Widerspruch führen würde, wegen $v = yc \rightsquigarrow c = uy \cdot c \rightsquigarrow uy = 1 \rightsquigarrow u \,\big|\, 1$.

Somit wären u und v zerlegbar und also auch c, mit Widerspruch zur Annahme. □

Der letzte Satz sichert jedem Element eine Darstellung

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n \,.$$

Diese Darstellung lässt sich noch verfeinern. Hierzu beachten wir, dass in Integritätsbereichen $a \sim b \Longleftrightarrow a \equiv b$ erfüllt ist. Dies gibt uns die Möglichkeit im Falle $p_1 \sim p_2$ das Element p_2 in der Form $p_1 \cdot \varepsilon_1$ mit Einsteiler ε_1 zu schreiben.

Konsequente Durchführung dieses Aspekts liefert uns dann

6. 3. 7 Korollar. *In einem noetherschen Integritätsbereich besitzt jedes $a \in R$ eine Darstellung*

$$a = \varepsilon \cdot \textstyle\prod_1^s p_i^{e_i} \text{ mit irreduziblen } p \text{ und } i \neq j \Longrightarrow p_i \nmid p_j \,.$$

Der obige Beweis hat noch mit ergeben, dass Elemente b mit der Eigenschaft $1 \parallel a \parallel b$ stets zerlegbar sind. Unzerlegbare Elemente haben also in Integritätsbereichen stets nur Einsteiler und assoziierte Elemente zu Teilern. Daher erfüllen irreduzible Elemente hier stets $(p, a) = (p) \vee (p, a) = 1$. Das liefert dann

6. 3. 8 Das Euklidische Lemma. *In einem Hauptidealbereich ist jedes irreduzible p sogar prim.*

BEWEIS. Sei p irreduzibel und sei $p \cdot c = a \cdot b$ erfüllt. Hätten wir dann weder $p \mid a$ noch $p \mid b$, so ergäbe sich $(p, a) = 1 = (p, b)$ und damit für geeignete x, y, u, v

$$\begin{aligned} px + ay = 1 = pu + bv \;&\rightsquigarrow\; p^2xu + pxbv + aypu + aybv = 1 \\ &\rightsquigarrow\; p \cdot (pxu + xbv + ayu + cyv) = 1 \\ &\rightsquigarrow\; p \mid 1 \,, \end{aligned}$$

mit Widerspruch. □

Als eine unmittelbare Folge des letzten Lemmas erhalten wir

6. 3. 9 Lemma. *Sind $p_1 \cdot p_2 \cdot \ldots \cdot p_k = a = q_1 \cdot q_2 \cdot \ldots \cdot q_\ell$ Primfaktorzerlegungen desselben Elementes a, so gilt $m = n$, und es ist jedes p_i $(1 \leq i \leq m)$ assoziiert zu einem q_j und umgekehrt.*

BEWEIS. Offenbar ist nichts zu zeigen im Falle $m = 1$.

Sei unsere Behauptung nun schon bewiesen für alle $n \leq k-1$.

Dann ist p_1 Teiler eines q_j, etwa o.B.d.A. Teiler von q_1. Nun ist aber p_1 kein Einsteiler, also *assoziiert* zu q_1, was $q_1 = \varepsilon_1 p_1$ bedeutet und nach Kürzung

$$p_2 \cdot p_3 \cdot \ldots \cdot_n = (\varepsilon_1 q_2) \cdot q_3 \cdot \ldots \cdot q_m$$

impliziert.

Damit ist dann induktiv alles gezeigt. □

Zusammenfassend haben wir also erhalten:

6. 3. 10 Theorem. *Sei $\mathfrak{R}$ ein euklidischer Ring. Dann ist $\mathfrak{R}$ ein Hauptidealbereich.*

Sei $\mathfrak{R}$ ein Hauptidealbereich, dann existiert a fortiori zu je zwei – und damit auch zu je endlich vielen Elementen aus R ein GGT und ein KGV, und es zerfällt darüber hinaus jedes $a \in R$ i.w. eindeutig in irreduzible Primelemente.

Ganz allgemein nennt man zwei Elemente eines Ringes *teilerfremd*, in Zeichen $a \perp b$, wenn jeder ihrer gemeinsamen Teiler auch 1 teilt. Das bedeutet in einem Hauptidealring natürlich nichts anders als $(a, b) = (1)$, und dies wiederum führt analog zur obigen Herleitung des Euklidischen Lemmas zu

6. 3. 11 Lemma. $a \perp b \Longrightarrow (a \cdot b) = (a) \cap (b)$

und führt somit für Polynomringe über Körpern zu

6. 3. 12 Proposition. *Hat $f(x)$ den Grad n, so hat $f(x)$ in keiner Körpererweiterung mehr als n Nullstellen.*

Denn: man beachte, dass α Nullstelle zu f genau dann ist, wenn sich f als $(x-\alpha) \cdot f_1(x)$ darstellen lässt und dass zwei Polynome $x-\alpha$ und $x-\beta$ fremd sind, wenn α und β verschieden sind. □

Aus den bisherigen Resultaten ergibt sich als eine wesentliche Konsequenz:

6. 3. 13 Proposition. *Sei $\mathfrak{R}$ ein Hauptidealring, also nicht notwendig integer und sei p irreduzibel. Dann liefert die Festsetzung $a \equiv b :\Longleftrightarrow p \,\big|\, a - b$*

eine Kongruenz, deren zugehöriger Restklassenring sogar ein Körper ist, d.h. der Bedingung genügt:

$$\forall\, \overline{a} \neq \overline{0}\ \exists\, \overline{a}' :\ \ \overline{a} \cdot \overline{a}' = \overline{1}.$$

BEWEIS. Man beachte $\overline{a} \neq \overline{0}$ bedeutet $p \nmid a$, also $(p, a) = (1)$ und damit

$$px + ay = 1 \quad (\exists :\ x, y \in R)\,,$$

also
$$\overline{p} \cdot \overline{x} + \overline{a} \cdot \overline{y} = \overline{1}\,.$$

Es ist aber $\overline{p} = \overline{0}$ und damit dann wie behauptet:

$$\overline{a} \cdot \overline{y} = \overline{1}\,. \qquad \square$$

Wir beenden diesen Abschnitt mit einem fast evidenten, aber doch ganz wesentlichen Resultat.

6. 3. 14 Das Teilbarkeitslemma. *Sei $\mathfrak{K}$ ein Körper, $p(x)$ irreduzibel über $\mathfrak{K}$ und gelte in einem Oberkörper $p(\beta) = 0$ und auch $h(\beta) = 0$. Dann folgt $p(x) \,\big|\, h(x)$.*

Denn: andernfalls erhielten wir für geeignete u, v den Widerspruch:

$$0 = p(\beta) \cdot u(\beta) + h(\beta) \cdot v(\beta) = 1\,. \qquad \square$$

Dieser letzte Satz ist natürlich ein Sonderfall von 4.1.10, da jedes Primelement p ein Primideal (p) erzeugt. Doch greift der Beweis unmittelbar zurück auf die Definition des Hauptidealringes und erspart dadurch überflüssige theoretische Anleihen.

6.4 Ein Satz von Gauß

Wir beginnen dieses Kapitel mit einem Satz, der im Kern zurück geht auf C. F. Gauss.

6. 4. 1 Proposition. *Sei $\mathfrak{R}$ ein faktorieller Integritätsbereich, d.h. ein Integritätsbereich mit eindeutiger Faktorzerlegung. Dann ist auch $\mathfrak{R}[x]$ faktoriell.*

BEWEIS. Wir vereinfachen die Verhältnisse aus didaktischen Gründen zunächst unwesentlich, indem wir den klassischen Satz beweisen:

$$\mathfrak{Z}[x] \text{ ist ein Gauß'scher Ring.}$$

Zunächst gehen wir von $\mathfrak{Z}$ über zum Quotientenkörper $\mathfrak{Q}$ und von $\mathfrak{Z}[x]$ zu $\mathfrak{Q}[x]$.

In $\mathfrak{Q}[x]$ besitzt jedes $f(x)$ aus $\mathfrak{Z}[x]$ eine eindeutige Primfaktorzerlegung $\prod_1^s p_i(x)^{e_i}$. Wir werden nun zeigen, dass sich hieraus eine eindeutige Primfaktorzerlegung in $\mathfrak{Z}[x]$ gewinnen lässt. Die Hauptidee wird dabei sein, ausgehend von den Primfaktoren in $\mathfrak{Q}[x]$ solche in $\mathfrak{Z}[x]$ zu gewinnen.

Hierzu betrachten wir den *Inhalt* $C(f)$ der einzelnen Polynome aus $\mathfrak{Z}[x]$, d. h. den positiven GGT der jeweiligen Koeffizienten $a_1, \ldots, a_n$.

Folglich sind wir am Ziel, wenn wir zeigen können, dass jedes f mit $C(f) = (1)$ in prime Polynome $p_i(x)$ zerfällt. Es gilt aber

$$C(f) = (1) = C(g) \Longrightarrow C(fg) = (1)\,, \tag{6.1}$$

da es sonst ein primes p gäbe mit $p \,\big|\, fg$ & $p \nmid f, g$.

Ist nun a der Inhalt von f und b der Inhalt von g, so haben wir bei geeigneter Wahl $f(x) = a{\cdot}f^*(x)$ und $g = b{\cdot}g^*(x)$ mit $C(f^*g^*) = 1$ also $C(fg) = ab = a{\cdot}b$.

Das liefert dann den gewünschten Beweis. Denn gilt $C(f) = 1$ und zerfällt $f(x)$ in $\mathfrak{Q}[x]$ etwa in

$$f(x) \;=\; \prod_1^s p_i(x)^{e_i}\,,$$

so können wir zunächst durch Multiplikation mit einem Hauptnenner der auf der rechten Seite auftretenden Nenner, etwa d, diese rechte Seite von ihren Koeffizientennennern befreien, was zu

$$d \cdot f(x) \;=\; \prod_1^s p_i'(x)$$

führt. Das bedeutet aber, dass wir die Primfaktoren von d sukzessive heraus kürzen können, da sie jeweils mindestens ein $p_j'(x)$ teilen, so dass am Ende

$$f(x) \;=\; \prod_1^s (p_i)^*(x)$$

eintritt, worin die einzelnen $(p_i)^*(x)$ den Inhalt 1 aufweisen.

Folglich sind wir am Ziel, wenn wir noch zeigen können, dass die $p_i^*(x)$ prim sind in $\mathfrak{Z}[x]$, denn dann lässt sich ja die gewünschte Eindeutigkeit durch sukzessive Kürzung erzielen.

Sei hierzu $p(x)$ ein solches $p_i^*(x)$. Dann ist $p(x)$ prim in $\mathfrak{Q}[x]$, da es aus einem irreduziblen Polynom durch Multiplikation mit einem Einsteiler gewonnen wurde.

Gelte hiernach weiter $p(x) \mid f(x)(g(x) \;\; (f, g \in Z[x])$. Dann ist $p(x)$ in $\mathfrak{Q}[x]$ Teiler eines der beiden Faktoren, etwa $p(x) \cdot q(x) = g(x)$, und wir können $q(x)$ schreiben als $\frac{r}{s} \cdot q^*(x)$ mit $C(q^*) = 1$, woraus weiter resultiert:

$$p(x) \cdot r \cdot q^*(x) \;\; = \;\; s \cdot g(x)$$

Das bedeutet aber, dass wir die Primfaktoren der Zerlegung von s sukzessive heraus kürzen können und zwar auf der linken Seite aus r. Das bedeutet dann $s \mid r$ und damit $p(x) \mid g(x)$ in $\mathfrak{Z}[x]$. □

Kapitel 7

Elimination

7.1 Der Stammkörper

Wir erinnern vorab – vergleiche 6.3.14 an das

7. 1. 1 Das Teilbarkeitslemma. *Sei $\mathfrak{K}$ ein Körper, $p(x)$ irreduzibel über $\mathfrak{K}$ und gelte in einem Oberkörper $p(\beta) = 0$ und auch $h(\beta) = 0$. Dann folgt $p(x) \,\big|\, h(x)$.*

Denn: Siehe oben, doch zur Erinnerung: andernfalls erhielten wir für ein geeignetes u, v

$$p(x) \cdot u(x) + h(x) \cdot v(x) = 1$$

mit Widerspruch zu

$$p(\beta) \cdot u(\beta) + h(\beta) \cdot v(\beta) = 0\,. \qquad \square$$

Ganz allgemein nennt man zwei Elemente eines Ringes *fremd*, in Zeichen $a \perp b$, wenn jeder ihrer gemeinsamen Teiler auch 1 teilt. Das bedeutet in einem Hauptidealring natürlich nichts anders als $(a, b) = (1)$, und dies wiederum führt analog zur obigen Herleitung des Euklidischen Lemmas zu

7. 1. 2 Lemma. $a \,\big|\, bc \;\&\; (a, c) = (1) \Longrightarrow a \,\big|\, b\,,$

liefert also für Polynomringe über Körpern:

7. 1. 3 Proposition. *Hat $f(x)$ den Grad n, so hat $f(x)$ in keiner Körpererweiterung mehr als n Nullstellen.*

DENN: man beachte, dass nach dem Teilbarkeitslemma α Nullstelle zu f genau dann ist, wenn sich f als $(x-\alpha)\cdot f_1(x)$ darstellen lässt und dass zwei Polynome $x-\alpha$ und $x-\beta$ fremd sind, wenn α und β verschieden sind. $\square$

Sei im folgenden sei $\mathfrak{K}$ ein Körper und $\mathfrak{K}[x]$ seine transzendente Erweiterung. Wir fragen: Unter welchen Bedingungen gibt es eine Erweiterung $\mathfrak{L}$ von $\mathfrak{K}$ in der

$$\frac{f_1(x)}{g_1(x)} \doteq \frac{f_2(x)}{g_2(x)}$$

eine Lösung besitzt. Dies ist offenbar gleich bedeutend mit der Existenz eines α mit

$$f_1(\alpha)\cdot g_2(\alpha) = f_2(\alpha)\cdot g_1(\alpha) \text{ und } g_1(\alpha)\cdot g_2(\alpha) \neq 0\,,$$

also mit

$$f_1(\alpha)\cdot g_2(\alpha) - f_2(\alpha)\cdot g_1(\alpha) = 0 \neq g_1(\alpha)\cdot g_2(\alpha)\,.$$

Natürlich ist ein solches α nicht stets in K zu erwarten, man denke an $x^2 - 2 \doteq 0$ über $\mathfrak{Q}$ oder an $x^2+1 \doteq 0$ über $\mathfrak{R}$. Wir werden aber sehen, dass jedes Polynom über $\mathfrak{K}$ in einem geeigneten Oberkörper von $\mathfrak{K}$ eine *Nullstelle besitzt.* Und hierzu genügt offenbar der Nachweis, dass es zu jedem über $\mathfrak{K}$ irreduziblen $p(x)$ einen Oberkörper $\mathfrak{L}$ von $\mathfrak{K}$ gibt mit $p(\alpha) = 0$ $(\exists\,\alpha \in L)$.

Das aber sichert

7. 1. 4 Der Satz über Stammkörper. *Sei $\mathfrak{K}$ ein Körper und*

$$p(x) = a_0 + a_1\cdot x + a_2\cdot x^2 + a_3\cdot x^3 + \ldots + a_n\cdot x^n$$

ein irreduzibles Polynom über $\mathfrak{K}$. Dann existiert ein Oberkörper $\mathfrak{L}$ zu $\mathfrak{K}$ in dem $p(x)$ mindestens eine Nullstelle besitzt.

Darüber hinaus gilt zusätzlich:

Schon der Ring $\mathfrak{K}[\alpha]$ ist ein Körper und ist β ebenfalls Nullstelle zu $p(x)$ in irgendeinem Oberköper $\mathfrak{L}'$, so gilt

$\mathfrak{K}[\alpha]$ ist isomorph zu $\mathfrak{K}[\beta]$ bezüglich der durch die Festsetzung

$$K \ni k \mapsto k \quad \textit{und} \quad \alpha \mapsto \beta$$

gestifteten Abbildung.

Hierfür sagen wir dann auch, es seien $\mathfrak{K}[\alpha]$ *und* $\mathfrak{K}[\beta]$ *elementweise isomorph, i. Z.* $\mathfrak{K}[\alpha]$ *eliso* $\mathfrak{K}[\beta]$.

BEWEIS. (a) Wie wir unter 6.3.13, ist $\mathfrak{K}[x]/p(x)$ ein Körper.

(b) Weiter gilt: Liegen a und b in K, so folgt:

$$a \equiv b \bmod p(x) \Longrightarrow a = b\,,$$

denn es teilt ja kein Polynom von einem Grad ≥ 1 ein Element aus K verschieden von 0.

(c) Es gilt aber mit den Operationssymbolen $\oplus$ bzw. $\circ$ für die Addition bzw. die Multiplikation in $\overline{\mathfrak{K}} := \mathfrak{K}/p(x)$

$$\overline{p(x)} = \overline{0} = \overline{a}_0 \oplus \overline{a}_1 \circ \overline{x} \oplus \overline{a}_2 \circ \overline{x}^2 \oplus \overline{a}_3 \circ \overline{x}^3 \oplus \ldots \oplus \overline{a}_n \circ \overline{x}^n\,,$$

und es gilt unter $a \mapsto \overline{a}$ die Kongruenz $\mathfrak{K} \cong \overline{\mathfrak{K}} := \mathfrak{K}/p(x)$.

(d) Tauschen wir hiernach $\overline{a}$ aus gegen a, $\oplus$ gegen $+$, $\circ$ gegen $\cdot$ und setzen wir $\overline{x} =: \alpha$, so erhalten wir

$$p(\alpha) = 0 = a_0 + a_1 \cdot \alpha + a_2 \cdot \alpha^2 + a_3 \cdot \alpha^3 + \ldots + a_n \cdot \alpha^n\,.$$

Folglich ist α eine Nullstelle zu $p(x)$.

Ferner ist der Ring $\mathfrak{K}[\alpha]$ isomorph zu $\mathfrak{K}[x]/p(x)$, dessen Elemente sich in der Form

$$\overline{a}_0 + \overline{a}_1 \cdot \overline{x} + \overline{a}_2 \cdot \overline{x}^2 + \overline{a}_3 \cdot \overline{x}^3 + \ldots + \overline{a}_m \cdot \overline{x}^m$$

schreiben lassen. Also ist der Ring aller „Ausdrücke"

$$a_0 + a_1 \cdot \alpha + a_2 \cdot \alpha^2 + a_3 \cdot \alpha^3 + \ldots + a_m \cdot \alpha^m$$

in der Tat schon ein Körper.

(e) Ist schließlich auch $\mathfrak{K}[\beta]$ von der gewünschten Art, so liefert:

$$\Psi: \quad f(x) \;\mapsto\; f(\beta)$$

einen Isomorphismus von $\mathfrak{K}[x]/p(x)$ auf $\mathfrak{K}[\beta]$. Denn, das Teilbarkeitslemma liefert:

$$\begin{aligned} \Psi(f) = \Psi(g) &\Longrightarrow \Psi(f-g) = 0 \\ &\Longrightarrow (f-g)(\beta) = 0 \\ &\Longrightarrow p \,\big|\, f-g \\ &\Longrightarrow f \equiv g \ mod\ p\,, \end{aligned}$$

und damit

$$\mathfrak{K}[\alpha] \cong \mathfrak{K}[x]/p(x) \cong \mathfrak{K}[\beta]\,. \qquad \square$$

Wegen des letzten Satzes sprechen wir auch von dem *Stammkörper* zu $p(x)$ über $\mathfrak{K}$.

Mittels des Eliminationssatzes sind wir nun in der Lage, das wohl bedeutendste Ergebnis dieser Vorlesung zu beweisen.

7.2 Der Zerfällungskörper

7. 2. 1 Der Satz von Steinitz. *Ist $f(x)$ ein beliebiges Polynom über $\mathfrak{K}$, so gibt es einen engsten Oberkörper von $\mathfrak{K}$, in dem f ganz in Linearfaktoren zerfällt, und es sind alle engsten Oberkörper dieser Art elementweise isomorph.*

Genauer gilt:

Ist $\mathfrak{K} \cong \overline{\mathfrak{K}}$ unter $k \mapsto \overline{k}$ und $f(x) \in \mathfrak{K}[x]$, so gibt es Körper

$$\mathfrak{K}[\alpha_1, \ldots, \alpha_n] \quad , \quad \overline{\mathfrak{K}}[\beta_1, \ldots, \beta_n]$$

mit:

$$f(x) = \prod_1^n (x - \alpha_i) \quad , \quad \overline{f} = \prod_1^n (x - \beta_i)\ ,$$

die bezüglich einer geeigneten Permutation π der β_i elementweise isomorph sind unter

$$k \mapsto \overline{k} \quad , \quad \alpha_i \mapsto \beta_{\pi(i)}\,.$$

BEWEIS. (a) Sei zunächst $\mathfrak{K}$ isomorph zu $\overline{\mathfrak{K}}$ und sei – man beachte das Teilbarkeitslemma –

$$f(x) = x - a \ \ (a \in K) \ \text{ sowie } \ \overline{f}(y) = y - \overline{a} \ \ (\overline{a} \in \overline{K})\,.$$

Dann gilt mit $\alpha := a$, $\beta := b$ evidenter weise

$$\mathfrak{K}[\alpha] \ \text{ eliso } \ \overline{\mathfrak{K}}[\beta]\,.$$

(b) Sei hiernach der Satz schon bewiesen für alle Polynome von einem Grad $\leq n-1$ und sei f vom Grad n.

Ist dann α Nullstelle des irreduziblen Polynoms $p(x)$ mit $p(x) \,\big|\, f(x)$ und etwa β Nullstelle zu $\overline{p}(y)$ mit $\overline{p}(y) \,\big|\, \overline{f}(x)$ unter $\mathfrak{K}[x]$ eliso $\overline{\mathfrak{K}}[y]$, so ist auch $\overline{p}(y)$ irreduzibel und damit nach der Konstruktion des Stammkörpers

$$\mathfrak{K}[\alpha] \;\text{ eliso }\; \overline{\mathfrak{K}}[\beta]$$

sowie, man beachte das Teilbarkeitslemma,

$$f(x) = (x-\alpha)\cdot f_1(x) \quad , \quad \overline{f}(y) = (y-\beta)\cdot \overline{f}_1(y)\,.$$

Dann ist aber auch

$$\big(\mathfrak{K}[\alpha]\big)[x] \;\text{ eliso }\; \big(\overline{\mathfrak{K}}[\beta]\big)[y]\,,$$

und es gilt

$$\frac{f(x)}{x-\alpha} = f_1(x) \implies \frac{\overline{f}(y)}{y-\beta} = \overline{f}_1(y)\,,$$

woraus dann wegen $\operatorname{grad}(f_1) = \operatorname{grad}(\overline{f}_1) \leq n-1$ unsere Behauptung induktiv resultiert. □

Wie der Satz von Steinitz konstatiert, sind bei vorgegebenem $\mathfrak{K}$, $f(x)$ je zwei Körper der oben konstruierten Art elementweise isomorph.

Man spricht deshalb auch von dem *Zerfällungskörper* zu f über dem Körper $\mathfrak{K}$.

Zerfällungskörper haben eine weitere bedeutende und deshalb nachdrücklich zu betonende Eigenschaft, die besagt, dass sie mit jedem α auch alle zu α konjugierten Elemente – also alle Wurzeln des zu α gehörenden irreduziblen Polynoms f_α enthalten.

7. 2. 2 Definition. Ein Körper $\mathfrak{L}$ heißt normal über dem Körper $\mathfrak{K}$, wenn jedes irreduzible Polynom über $\mathfrak{K}$, das mindestens 1 Nullstelle in $\mathfrak{L}$ besitzt, über $\mathfrak{L}$ sogar in Linearfaktoren zerfällt.

7. 2. 3 Proposition. *Ist $\mathfrak{L}$ ein Zerfällungskörper über $\mathfrak{K}$, so ist $\mathfrak{L}$ – sogar – normal über.*

BEWEIS. Sei $\mathfrak{L}$ Zerfällungskörper über $\mathfrak{K}$ bezüglich $f(x) \in K[x]$ und $g(x)$ ein irreduzibles Polynom über $\mathfrak{K}$ mit einer Nullstelle $\lambda \in L$. Wir haben zu zeigen, dass $g(x)$ ein Produkt von Linearfaktoren über $\mathfrak{L}$ ist. Nun ist aber

$$f(x) = (x-\vartheta_1)\cdot \ldots \cdot (x-\vartheta_n)\,, \tag{7.1}$$

und es gilt

$$\lambda = h(\vartheta_1, ..., \vartheta_n) \ \ (1 \leq i \leq n)\,. \tag{7.2}$$

Wir bilden das Polynom

$$H(x) = \prod (x - h(\vartheta_1, ..., \vartheta_n))\,, \tag{7.3}$$

erstreckt über alle Permutationen der Indizes $1, ..., n$.

Die Koeffizienten dieses Polynoms sind invariant gegenüber allen Permutationen der ϑ_i, also Polynomwerte der elementarsymmetrischen Polynome, die ihrerseits nach (7.1) die Koeffizienten von $f(x)$, also Elemente aus K liefern. Somit gilt

$$H(x) \in \mathfrak{K}[x] \tag{7.4}$$

Andererseits ist $H(\lambda) = 0$ und nach Voraussetzung $g(\lambda) = 0$. Folglich ist nach dem Teilbarkeitslemma 6.3.14 $g(x)$ ein Teiler von $H(x)$.

Nun sind aber mit $h(\vartheta_1, ..., \vartheta_n)$ auch alle durch Permutation der ϑ_i erzeugten Elemente aus L. Also zerfällt $H(x)$ über $\mathfrak{L}$ in Linearfaktoren und mit $H(x)$ dann auch $g(x)$ □

Hiernach kommen wir zu dem oben angekündigten „Kehrsatz" über Normalkörper

7. 2. 4 Proposition. *Sind $\vartheta_1, ..., \vartheta_n$ Nullstellen irreduzibler Polynome über $\mathfrak{K}$ und ist $\mathfrak{N} = \mathfrak{K}(\vartheta_1, ..., \vartheta_n)$ normal über $\mathfrak{K}$, so ist $\mathfrak{N}$ ein Zerfällungskörper über $\mathfrak{K}$.*

BEWEIS. Sind $f_1, ..., f_n$ die zu den ϑ_i gehörenden irreduziblen Polynome, so liegt die Gesamtheit aller Nullstellen der $f_i(x)$ in N. Also ist $\mathfrak{N}$ Zerfällungskörper über $\mathfrak{K}$ bezüglich des Produktpolynoms $f(x) := f_1(x) \cdot ... \cdot f_n(x)$. □

Wir kehren zurück zum Problem der Elimination. Hier kommt die natürliche Frage auf, ob sich auch über kommutativen Ringen mit 1 jedes Polynom zerfällen lässt. Dass dies nicht möglich ist, zeigt uns das Beispiel:

$$\mathfrak{Z}_4 := (\mathbf{Z}_4, +, \cdot) \quad , \quad f(x) := 2x^2 + 1\,.$$

Besäße f in irgendeiner Erweiterung von $\mathfrak{Z}_4$ eine Nullstelle α, so wäre in diesem Ring

$$(2\alpha^2) = -1 = 3 \;\rightsquigarrow\; 0 = 2 \cdot (2\alpha^2) = 2 \cdot 3 = 2\,,$$

mit Widerspruch.

Das macht klar, was ja auch nicht verwundert, dass die Existenz einer Wurzel nicht für jede Klasse von Ringen gesichert ist.

Weiter oben hatten wir gezeigt, dass ein Polynom vom Grade n über einem Körper höchstens n Nullstellen zulässt. Dass dies über Ringen ganz anders sein kann, zeigt der R^2, wenn man $(a, b) \cdot (c, d) := (ab, cd)$ erklärt.

Denn dies ist offenbar ein Ring, in dem $(1, 0)$ mit jedem $(0, b)$ den Produktwert $(0, 0)$ liefert, in dem also das Polynom $(1, 0) \cdot x$ unendlich viele Lösungen hat.

Schließlich kann über einem Ring der Fall $f(x) \,\big|\, 1$ auch für Polynome von einem Grad ≥ 1 eintreten, der ja über Integritätsbereichen ausgeschlossen ist. Man betrachte über $\mathfrak{Z}_4$ das Polynom $f(x) := 1+2x$. Dann gilt $f(x)\cdot(1-2x) = 1$.

Besinnen wir uns andererseits auf die Konstruktion, so sehen wir, dass es sich bei der *Eliminationsfrage* i. w. um ein Problem der *Allgemeinen Algebra* handelt. Denn $f(\alpha) \doteq g(\alpha)$ in einem geeigneten Oberring besagt ja nichts anderes als die Forderung $f(x) \equiv g(x)$ für ein geeignetes $\equiv$ mit $a \not\equiv b \;\; (\forall\, a \neq b \in K)$.

Genau dies aber lässt sich übertragen in die Allgemeine Algebra. Natürlich wäre auch hier zunächst eine Polynomerweiterung zu konstruieren, zum Beispiel zu einer Gruppe $\mathfrak{G}$.

Dies gelingt auf dem Wege, dass man zunächst alle „*Rechenausdrücke* mit Elementen aus der Ausgangsalgebra und dem *Platzhalter* x bildet und hiernach zwei solcher *Ausdrücke* als gleichwertig erachtet, wenn sie bei allen möglichen Homomorphismen dasselbe Bild erhalten. Danach lässt sich dann die *Eliminationsfrage* stellen, also die Frage:

Existiert ein Homomorphismus ϕ, der den Bedingungen genügt: $\phi(f) = \phi(g)$, aber $\phi(a) \neq \phi(b) \;\; (\forall a, b \in G)$.

EIN BEISPIEL: Die Polynome der abelschen Gruppe wären Ausdrücke der Form $a \cdot x^k \;\; (k \in \mathbf{N})$. Eine typisches Eliminationsproblem wäre:

$$\text{(W)} \qquad x + x \;\doteq\; a\,.$$

Problem: Ist diese *Gleichungsforderung* lösbar.

Wir betrachten den Fall $a = 1$ über $\mathfrak{G} = \mathfrak{Z}$. Offenbar lässt sich $\mathfrak{Z}$ einbetten in $\frac{1}{2} \cdot \mathfrak{Z}$, und hier lässt sich dann die vorgegebene Gleichung lösen durch $\frac{1}{2}$, womit nach Konstruktion zugleich gezeigt ist, dass sich die oben betrachtete Gleichung für jedes a lösen lässt.

Natürlich sehen wir sofort, dass $\mathfrak{Q}$ eine Erweiterung von $\mathfrak{Z}$ ist, in der sich alle Gleichungen über $(\mathbf{Z}, +)$ lösen lassen, so wie sich in $\mathfrak{C}$, wie wir noch sehen werden, alle Gleichungen über $\mathfrak{R}$ lösen lassen.

PROBLEM: Sei $\mathfrak{G}$ eine total geordnete Gruppe und sei $x^2 \doteq a$ nicht lösbar in $\mathfrak{G}$. Dann lässt sich zeigen, dass es eine Lösung in einer Erweiterung von $\mathfrak{G}$ gibt. Es ist aber bis heute offen, ob es auch eine Lösung in einer total geordneten Erweiterung von $\mathfrak{G}$ gibt.

HINWEIS: Es fehlt nicht an Beiträgen zu diesem Problem, aber es gibt derzeit niemanden, der auch nur annähernd eine Idee von einem Lösungsweg hätte.

Kapitel 8

Körper

8.1 Lineare Abhängigkeit

Im Zentrum dieses Kapitels steht das Begriffspaar *algebraisch/ transzendent.*

8. 1. 1 Definition. Sei $\mathfrak{R}$ ein *Oberintegritätsbereich* des Körpers $\mathfrak{K}$. Dann heißt $x \in R$ *transzendent* über $\mathfrak{K}$, wenn sich die Potenzen von x linear nur trivial zu 0 kombinieren lassen.

Hingegen heißt $\alpha \in R$ *algebraisch* über $\mathfrak{K}$, wenn bei geeigneter Koeffizientenwahl

$$a_0 + a_1\alpha^1 + a_2\alpha^2 + \ldots + a_n\alpha^n = 0$$

eintritt.

Im Kapitel über Ringe haben wir den Begriff der *transzendenten Erweiterung*

$$\mathfrak{R}\,[\,x_1, \ldots, x_n\,]\,,$$

d. h. die sukzessive Erweiterung um die transzendenten Elemente $x_1 \ldots, x_n$ eingeführt.

Im Kapitel über Elimination haben wir Erweiterungen der Art

$$\mathfrak{L} = \mathfrak{K}\,[\,1 = \alpha_0, \alpha_1, \ldots, \alpha_n\,]$$

studiert, wobei die Elemente α_i $(1 \leq i \leq n)$ jeweils Nullstelle eines Polynoms über $\mathfrak{K}\,[\,\alpha_0, \ldots, \alpha_{i-1}\,]$, also algebraisch waren.

Während wir aber auf der einen Seite schon gezeigt haben, dass alle Elemente aus $K\,[\,x_1, \ldots, x_n\,] \setminus K$ transzendent sind über $\mathfrak{K}$, haben wir auf der anderen Seite $\mathfrak{K}\,[\,\alpha_1, \ldots, \alpha_n\,]$ in dieser Hinsicht noch nicht genauer untersucht. Dies soll nun nachgeholt werden.

8. 1. 2 Definition. Sei $\mathfrak{L}$ ein *Oberintegritätsbereich* des Körpers $\mathfrak{K}$. Dann nennen wir $a \in L$ *linear abhängig* von $B \subseteq L$ gdw.

$$a \;=\; \textstyle\sum_1^n k_i b_i \;\; (k_i \in K, b_i \in B)$$

erfüllt ist. Gilt dies, so schreiben wir auch $a \propto_K B$.

Wie man leicht verifiziert ist dies eine lineare Abhängigkeitsrelation – vgl. Lineare Algebra 1 – so dass eine *Basis* zu $\propto_K$ existiert und alle Basen gleiche Länge haben. Dies halten wir fest unter:

8. 1. 3 Proposition. *Ist $\mathfrak{R}$ ein Oberintegritätsbereich zu $\mathfrak{K}$, so lässt sich $\mathfrak{R}$ auffassen als m-dimensionaler Vektorraum über $\mathfrak{K}$.*

Als eine fundamentale Folge hieraus resultiert, vgl. Linal,

8. 1. 4 Proposition. *Ist $\mathfrak{L}$ ein Oberkörper von $\mathfrak{K}$ und B eine Basis von L bezüglich $\propto_K$ so lässt sich jedes $a \in L$ eindeutig darstellen vermöge*

$$a \;=\; \textstyle\sum_1^n k_i b_i \;\; (k_i \in K, b_i \in B).$$

Dies liefert einen ersten Einblick in die Struktur von $\mathfrak{K}[\,\alpha\,]$.

Ist α Nullstelle des irreduziblen Polynoms $p(x)$, so ist auf der einen Seite die Menge der Elemente

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \;\;=:\;\; B$$

linear unabhängig, da es andernfalls ein Polynom $g(x)$ gäbe mit $\operatorname{grad}(g) < \operatorname{grad}(p)$, aber $p \,\big|\, g$, auf der anderen Seite hingegen die Menge der Elemente

$$1,\ \alpha,\ \alpha^2,\ \ \ldots\ \ ,\ \alpha^{n-1},\ \alpha^n$$

aber linear abhängig, was bedeutet, dass sich α^n und damit auch jedes α^{n+k} linear kombinieren lässt mittels $1 = \alpha^0$ bis α^{n-1}.

Insbesondere gilt damit unter den gemachten Voraussetzungen

$$\mathfrak{K}[\,\alpha\,] : \mathfrak{K} \;=\; \operatorname{grad}\big(p(x)\big)\,.$$

Unter anderem genügt es daher im konkreten Fall, die Elemente α^n bis α^{2n-2} über $1, \alpha, \ldots, \alpha^{n-1}$ darzustellen, was insbesondere im endlichen Fall das Aufstellen einer Multiplikationstafel zu $\mathfrak{K}[\,\alpha\,]$ außerordentlich erleichtert.

BEISPIEL: Man konstruiere ein $\mathfrak{Z}_3[\alpha]$ zu $p(x) := x^2 - 2x + 2$.

Wir kehren zurück zur allgemeinen Theorie.

8. 1. 5 Definition. Sei $\mathfrak{L}$ ein Oberkörper von $\mathfrak{K}$. Dann bezeichnen wir die Dimension von $(L, \propto_K)$ als den *Grad von* $\mathfrak{L}$ *über* $\mathfrak{K}$, i. Z. $[\mathfrak{L} : \mathfrak{K}]$.

8. 1. 6 Proposition. *Ist* $\mathfrak{K}_2$ *Oberkörper zu* $\mathfrak{K}_1$ *und* $\mathfrak{K}_1$ *Oberkörper zu* $\mathfrak{K}$*, so gilt:*

$$[\mathfrak{K}_2 : \mathfrak{K}_1] \cdot [\mathfrak{K}_1 : \mathfrak{K}] \;=\; [\mathfrak{K}_2 : \mathfrak{K}].$$

BEWEIS. Offenbar genügt es, den Beweis für endliche Grade zu führen.

Ist dann zum einen $B = \{b_1, \ldots, b_m\}$ eine Basis zu $\mathfrak{K}_1$ über $\mathfrak{K}$ und zum anderen $C = \{c_1, \ldots, c_n\}$ eine Basis zu $\mathfrak{K}_2$ über $\mathfrak{K}_1$, so ist

$$\{b_i c_j \,\big|\, b_i \in B, c_j \in C,\;\; 1 \leq i \leq m, 1 \leq j \leq n\}$$

eine Basis zu $\mathfrak{K}_2$ über $\mathfrak{K}$.

Denn ist a aus K_2, so gilt zunächst

$$a = \sum_1^n \ell_j \cdot c_j \;\; (\exists \ell_i \in K_1,\, c_j \in C),$$

und es ist jedes c_j ein

$$\sum_1^m k_i \cdot b_i \qquad (k_i \in K).$$

Darüber hinaus ist diese Darstellung sogar eindeutig, da sich die 0 nur trivial komponieren lässt. Denn, ist

$$\sum_{i,j=1}^{m,n} k_{i,j}(b_i c_j) b_i \;=\; 0$$

erfüllt, so folgt

$$\sum_i^m \Big(\sum_1^n k_{ij} \cdot c_j \Big) b_i = 0$$

und damit

$$\sum_1^n k_{ij} \cdot c_j = 0 \;\; (1 \leq i \leq k),$$

also $k_{ij} = 0$ für alle i, j . □

Wir betrachten nun Integritätsbereiche vom Typ $\mathfrak{K}[\vartheta]$. Ist ϑ hier transzendent über $\mathfrak{K}$, so handelt es sich um den Polynomring über $\mathfrak{K}$, und es gibt im Blick auf $\propto_\vartheta$ eine unendliche Basis, etwa die Basis $\vartheta^0, \vartheta^1, \vartheta^2, \ldots \vartheta^n, \ldots$, über der sich alle Elemente aus $\mathfrak{K}[\vartheta]$ als (endliche) K-Linearkombination darstellen lassen.

Ist ϑ aber nicht transzendent über $\mathfrak{K}$, sondern algebraisch, so existiert ein $\sum_1^n a_i \vartheta^i$, das den Wert 0 liefert, obwohl nicht alle Koeffizienten a_i verschwinden.

Hieraus resultiert dann der Satz, dass alle Elemente aus $\mathfrak{K}[\vartheta]$ algebraisch sind über $\mathfrak{K}$, „sobald" ϑ algebraisch ist über $\mathfrak{K}$. Denn, man argumentiere *via* $[\mathfrak{K}[\vartheta] : \mathfrak{K}]$. Ist dieser Grad gleich n und α aus $K[\vartheta]$, so ist die Menge $\{1, \alpha, \ldots \alpha^n\}$ linear abhängig, α also algebraisch.

MERKE: Ist ϑ algebraisch/transzendent über $\mathfrak{K}$, so sind auch alle übrigen Elemente aus $K[\vartheta] \setminus K$ algebraisch/transzendent.

Es gilt aber noch etwas mehr, nämlich dass zu jedem α aus K ein eindeutig bestimmtes *irreduzibles, normiertes* f_α existiert mit $f_\alpha(\alpha) = 0$, das zudem unter allen Polynomen f mit $f(\alpha) = 0$ von minimalem Grad ist.

Denn, ist f_α unter allen $g(x)$ mit Nullstelle α eines von minimalem Grad mit $a_n = 1$, so ist es natürlich irreduzibel, da es sonst nicht von minimalem Grade wäre, weil ja bei jeder Zerlegung mindestens einer der beiden Faktoren an der Stelle α verschwinden würde. Es kann aber darüber hinaus auch kein irreduzibles Polynom von höherem Grade geben, das α annulliert, da dieses irreduzible Polynom f_α teilen müsste. Schließlich ergibt sich die Eindeutigkeit daraus, dass zwei normierte Polynome einander nur teilen können, wenn sie gleich sind.

Mitgeliefert haben die letzten Ausführungen natürlich noch

8. 1. 7 Proposition. *Sei α algebraisch über $\mathfrak{K}$. Dann gilt:*

$$\mathfrak{K}(\alpha) : \mathfrak{K} = \operatorname{grad}(f_\alpha) .$$

Ist nun allgemein der Körper $\mathfrak{L} = \mathfrak{K}[\alpha_1, \ldots, \alpha_n]$ mit $n \geq 2$ und α_i algebraisch über dem Körper $\mathfrak{K}[\alpha_1, \ldots, \alpha_{i-1}]$, so können wir induktiv fortschreiten

und zeigen, dass $\mathfrak{K}[\,\alpha_1,\ldots,\alpha_n\,]$ von *endlichem Grad* über $\mathfrak{K}$ und damit auch *algebraisch* über $\mathfrak{K}$ ist.

8. 1. 8 Definition. Sei $\mathfrak{L}$ ein Oberkörper zu $\mathfrak{K}$. Dann heißt $\mathfrak{L}$ algebraisch über $\mathfrak{K}$, wenn alle $\alpha \in L$ algebraisch sind über $\mathfrak{K}$.

Hiernach ist insbesondere jede endliche Erweiterung $\mathfrak{K}[\,\alpha_1,\ldots,\alpha_n\,]$ mit algebraischen α_i algebraisch über $\mathfrak{K}$, insbesondere also auch jeder Zerfällungskörper. Weiter haben wir:

8. 1. 9 Proposition. *Sei $\mathfrak{K}_2$ Oberkörper zu $\mathfrak{K}_1$ und sei $\mathfrak{K}_1$ Oberkörper zu $\mathfrak{K}$. Ist dann $\mathfrak{K}_2$ algebraisch über $\mathfrak{K}_1$ und $\mathfrak{K}_1$ algebraisch über $\mathfrak{K}$, so ist auch $\mathfrak{K}_2$ algebraisch über $\mathfrak{K}$.*

BEWEIS. Ist ϑ ein Element aus $K_2 \setminus K_1$, so ist ϑ Nullstelle eines Polynoms f über $\mathfrak{K}_1$, d.h. so gibt es Elemente $a_0,\ldots,a_n$ derart, dass $\sum_1^n a_i\vartheta^i$ verschwindet.

Mit anderen Worten: f gehört zu $\mathfrak{K}[\,a_0,\ldots,a_n,x]$. Daher ist der Grad von $\mathfrak{K}[\,a_0,\ldots,a_n,\vartheta\,]$ über $\mathfrak{K}$ endlich und somit ϑ algebraisch über $\mathfrak{K}$. □
Der letzte Satz liefert als eine unmittelbare Anwendung

8. 1. 10 Korollar. *Sind die Elemente α und β algebraisch über $\mathfrak{K}$, so auch die Elemente $\alpha+\beta, \alpha-\beta, \alpha\cdot\beta, \alpha:\beta$.*

DENN: β ist algebraisch über $\mathfrak{K}[\,\alpha\,]$, folglich sind alle Elemente aus $\mathfrak{K}[\,\alpha,\beta\,]$ algebraisch über $\mathfrak{K}$. □

Der vorauf gegangene Beweis reduziert auf der Basis der linearen Algebra den klassischen direkten Beweis auf einen *„Einzeiler"*. Er liefert uns allerdings kein Polynom, das etwa von $\alpha\cdot\beta$ oder $\alpha+\beta$ annulliert würde.

8. 1. 11 Beispiel. Da sich – wie wir später sehen werden – der Winkel von 60° nicht mit Zirkel und Lineal dreiteilen lässt, lässt sich natürlich auch der Winkel von 1° nicht mit Zirkel und Lineal konstruieren, also auch nicht der Sinus von 1 Grad.

Dennoch ist $\sin 1^\circ$ nicht transzendent, sondern algebraisch (über $\mathfrak{Q}$), was sich fast elementar her rechnen lässt.

DENN: $\sin 1^0 + \cos 1^0 = 1$, also wäre mit $\sin 1^\circ$ auch $\cos 1^\circ$ transzendent. Es gilt aber $(\cos 1^0 + i\cdot\sin 1^0)^{360} = 1$. Das bedeutet: wären $x := \sin 1^0$ und $y := \cos 1^0$ transzendent über $\mathfrak{Q}$, so würde dies, da der imaginäre Anteil auf

der linken Seite verschwinden muss, ein Polynom in x, y über $\mathfrak{Q}$ vom Wert 1 liefern.

HINWEIS: Natürlich können wir analog schließen für jedes $\sin k$ mit $360 : k \in \mathbf{N}$

8.2 Endliche Körper

Wir beginnen mit den im Abschnitt über Gruppen angekündigten Lemmata über endliche Gruppen:

8. 2. 1 Lemma. *In jeder endlichen multiplikativ notierten abelschen Gruppe* $\mathfrak{G}$ *gilt:*

$$o(a) = m \perp n = o(b) \implies o(ab) = o(a) \cdot o(b).$$

DENN: es gilt $(ab)^{man} = (a^m)^n \cdot (b^n)^m = 1$ also $o(ab) \mid mn$, und wir haben weiter mit $k := o(ab)$ und $k = mq_1 + r \;\&\; k = nq_2 + s \quad$ mit $(0 \leq r < m,\ 0 \leq s < n)$:

$$\begin{aligned} (ab)^k = 1 &\implies a^r \cdot b^s = 1 \\ &\implies a^{rn} = 1 \\ &\implies m \mid rn \Rightarrow m \mid r \to r = 0 \\ &\implies m \mid k \;\; (\;\&\; n \mid k) \\ &\implies m \cdot n \mid k\,. \end{aligned}$$ □

8. 2. 2 Lemma. *In jeder endlichen multiplikativ notierten abelschen Gruppe* $\mathfrak{G}$ *gilt:*

$$o(a) = m \cdot n \implies o(a^m) = n\,.$$

DENN:

$$o(a) = m \cdot n \implies (a^m)^n = a^{mn} = 1$$

und

$$\begin{aligned} (a^m)^k = 1 &\implies a^{mn} = (a^m)^k \\ &\implies mn \mid mk \\ &\implies n \mid k\,. \end{aligned}$$ □

8. 2. 3 Lemma. *Ist* $\mathfrak{Z}_p$ *der Restklassenkörper von* $\mathfrak{Z}$ *modulo* p*, so gilt für jedes Element* a *dieses Körpers* $a^{p^m} = a$*.*

DENN: dies ist klar für 0, und ist $a \neq 0$, so folgt $a^{p-1} = 1$ und damit $a^p = a$, also auch $(a^p)^p = a^p = a$ und somit schließlich $a^{p^m} = a$. □

Wir fahren fort mit einigen Bemerkungen über kommutative Ringe mit 1.

8. 2. 4 Definition. Sei $\mathfrak{R}$ ein kommutativer Ring mit 1. Dann versteht man unter dem *Primring* $\mathfrak{P}$ von $\mathfrak{R}$ den von 1 erzeugten Unterring, also den Ring aller Summen, gebildet aus Summanden gleich +1 oder gleich −1.

Setzen wir nun $$\textcircled{n} := 1 + 1 + \ldots + 1 \ \ (n - mal)$$

bzw. $$-\textcircled{n} := -1 - 1 - \ldots - 1 \ \ (n - mal)$$

und $$\textcircled{0} := 0\,,$$

so muss nach diesen Erklärungen $\mathfrak{P}$ stets isomorph zu einem $\mathfrak{Z}_m$ oder aber zu $\mathfrak{Q}$, im Falle eines endlichen Körpers aber zwangsläufig isomorph zu einem $\mathfrak{Z}_p$ sein, da andernfalls aus $m = k \cdot \ell$ für die Klassen $\textcircled{k}\,\textcircled{\ell} = 0$ folgen würde $\textcircled{k} \cdot \textcircled{\ell} = 0$, mit Widerspruch.

Offenbar ist die Struktur von $\mathfrak{P}$ von größter Bedeutung für das multiplikative Verhalten der Größen

$$\operatorname{sgn}(n) \cdot \textcircled{n} := 1 + \ldots + 1 \ \ (n \text{ mal})$$

und zwar gilt genauer $\mathfrak{P} \cong \mathfrak{Z}_c \Longleftrightarrow \textcircled{c}a = 0 \ \ (\forall\, a \in R)$.

8. 2. 5 Definition. Sei $\mathfrak{R}$ ein Ring. Dann versteht man unter der *Charakteristik* von $\mathfrak{R}$, i.Z. $\operatorname{char}(\mathfrak{R})$, den Modul c desjenigen Restklassenringes $\mathfrak{Z}_c$, zu dem der Primring von $\mathfrak{R}$ isomorph ist.

Ist $\mathfrak{R}$ sogar ein Integritäsbereich, so kann die Charakteristik von $\mathfrak{R}$ natürlich nur eine Primzahl oder aber gleich 0 sein. Insbesondere ist demnach die Charakteristik eines endlichen Körpers stets eine Primzahl. Das bedeutet eine erste Einsicht in die Struktur endlicher Körper.

8. 2. 6 Proposition. *Jeder endliche Körper lässt sich als m-dimensionaler Vektorraum über seinem Primkörper auffassen und hat demzufolge p^m (p prim $m \in \mathbf{N}$) viele Elemente.*

Im weiteren wird eine Klärung der Frage von Bedeutung sein, wann ein Polynom $f(x)$ mehrfache Nullstellen hat. Hierzu definieren wir:

8. 2. 7 Definition. Sei $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ ein Polynom über dem kommutativen Ring $\mathfrak{R}$ mit 1. Dann setzen wir:

$$f'(x) := ⓪\, a_0 + ①\, a_1x^0 + \ldots + ⓝ\, a_nx^{n-1}$$

Wie der Leser sofort erkennt, ist die Funktion f' formal der Ableitung in der Analysis nachgebildet, und wie er leicht nachrechnet, gelten für die hier formal erklärte Ableitung die Summen- die Produkt- und die Ketten-Regel. Das bedeutet weiter:

8. 2. 8 Lemma. *Genau dann hat ein Polynom über einem Körper $\mathfrak{K}$ eine mehrfache Nullstelle, d.h. einen Faktor $(x-\alpha)^2$, wenn es mit seiner Ableitung eine gemeinsame Nullstelle hat.*

DENN:
$$\begin{aligned} & f(x) &=& (x-\alpha)^2 \cdot g(x) \\ \Longrightarrow \quad & f'(x) &=& ②\,(x-\alpha)\cdot g(x) + (x-\alpha)^2 \cdot g'(x) \end{aligned}$$

und gilt $f(x) = (x-\alpha)h(x)$ und $f'(x) = (x-\alpha)k(x)$, so folgt:

$$\begin{aligned} & f'(x) &=& (x-\alpha)k(x) = h(x) + (x-\alpha)h'(x) \\ \Longrightarrow \quad & h(x) &=& (x-\alpha)\big(k(x) - h'(x)\big) \\ \Longrightarrow \quad & f(x) &=& (x-\alpha)^2 \cdot \big(k(x) - h'(x)\big)\,. \end{aligned}$$ □

Das letzte Lemma hat zwei fundamentale Konsequenzen:

8. 2. 9 Proposition. *Ist $char\,(\mathfrak{K})$ gleich 0, so hat kein irreduzibles Polynom mehrfache Nullstellen.*

DENN: Hätte das irreduzible Polynom f eine mehrfache Nullstelle α, so müsste f seine Ableitung f' teilen, mit Widerspruch zu der Regel $\operatorname{grad}(f') < \operatorname{grad}(f)$. □

8. 2. 10 Proposition. *$x^n - 1$ kann über keinem Körper $\mathfrak{K}$ mit einer Charakteristik $c\!\nmid n$ eine mehrfache Nullstellen besitzen bzw. äquivalent hierzu: Gilt $char\,(\mathfrak{K}) = c\!\nmid n$, so hat $x^n - 1$ in jedem Zerfällungskörper n paarweise verschiedene Nullstellen.*

Hiernach kommen wir zu dem ersten Struktursatz über endliche Körper:

8. 2. 11 Theorem. *Es gibt i.w. keine anderen Körper als die Zerfällungskörper zu $x^{p^m} - x$ über Primkörpern vom Typ $\mathfrak{Z}_p$.*

BEWEIS. (a) Sei $\mathfrak{K}$ irgendein endlicher Körper. Dann ist $\mathfrak{K}$ eine m-dimensionale Erweiterung seines Primkörpers. Folglich gilt für alle $a \neq 0$ die Gleichheit $a^{p^m-1} - 1 = 0$, weshalb $\mathfrak{K}$ ein Zerfällungskörper zu $x^{p^m-1} - x = 0$ ist.

(b) Sei jetzt $\mathfrak{Z}_{p^m}$ der Zerfällungskörper zu $x^{p^m} - x$ über dem Primkörper $\mathfrak{P} := \mathfrak{Z}_p$. Dann erfüllen alle a aus Z_p die Gleichheit $a^{p^m} = a$ und gehören somit zur Lösungsgesamtheit der Forderung $x^{p^m} - x \doteq 0$.

Weiterhin ist die Lösungsgesamtheit abgeschlossen bezüglich der rationalen Operationen $+, -, \cdot, :$.

Dies ist klar für $\cdot$ und :, gilt aber auch für $+$ und $-$, wegen

$$p \,\Big|\, \binom{p^m}{k}_{(1\leq k\leq p^m-1)} \Longrightarrow (a+b)^{p^m} = a^{p^m} + b^{p^m} = a + b\,.$$

Somit ist die Menge der Lösungen zu $x^{p^m} - x \doteq 0$ *rational abgeschlossen*, also Trägermenge eines und damit i.S. der Algebra des Zerfällungskörpers.

(c) Das bedeutet dann insgesamt, dass es keine anderen endlichen Körper als die Zerfällungskörper i.S. des Satzes gibt und damit, dass endliche Körper in ihrer Struktur eindeutig festgelegt sind durch ihre Charakteristik p und die Anzahl ihrer Elemente. Insbesondere also, dass es zu jedem p^m einen Körper dieser Anzahl gibt, nämlich den Zerfällungskörper zu $x^{p^m} - x$ über $\mathfrak{P}$ und dass jeder endliche Körper von einer solchen Anzahl ist. □

Das soeben bewiesene Resultat darf als ein *wunderschöner* Struktursatz bezeichnet werden und doch ist es möglich, diesen Struktursatz noch zu verschärfen. Dies leistet indirekt

8. 2. 12 Der Satz über Kreisteilungspolynome. *Sei im folgenden* $char(\mathfrak{K}) \nmid m$ *und* $T_m(x) = x^m - 1$ *betrachtet über* $\mathfrak{K}$. *Dann bilden die Wurzeln von* T_m *im Zerfällungskörper* $\mathfrak{Z}_m$ *eine zyklische Gruppe der Ordnung* m.

BEWEIS. Es ist zu zeigen, dass mindestens ein ζ mit $\zeta^m = 1$ alle übrigen ζ_i mit $\zeta_i^m = 1$ „erzeugt".

Zunächst sehen wir, dass die m-ten Einheitswurzeln eine *abelsche Gruppe* bilden, und wir wissen auch, dass $x^m - 1$ m viele Lösungen hat.

Ferner existiert im Falle $o(\zeta_i) = p_j^{e_j} \cdot n_j$ mit $p_j \perp n_j$ nach 8.2.2 ein ζ_j mit $o(\zeta_j) = p_j^{e_j}$.

Wir bilden nun das KGV der (endlich vielen) $o(\zeta_j) = p^{e_j}$ und bezeichnen es mit n. Dann gibt es nach 3.2.9 auch ein ζ von der Ordnung $o(\zeta) = n$, und es gilt natürlich $o(\zeta_i) \,\big|\, n$. Folglich sind alle ζ_i auch Wurzeln zu $x^n - 1$, also alle $(x - \zeta_i)$ Linearfaktoren zu $x^n - 1$. Es sind aber je zwei verschiedene Linearfaktoren fremd. Folglich gilt

$$x^m - 1 = \prod_1^n (x - \zeta_i) \,\big|\, x^n - 1\,,$$

also insbesondere $m \leq n$ und damit $m = n$, d.h. $o(\zeta) = n = m$, was zu beweisen war. □

Zum Satz von Wedderburn

8. 2. 13 Definition. Als Schiefkörper bezeichnet man jeden Ring $\mathfrak{S} = (S, +, \cdot)$, in dem für jedes $a \neq 0$ alle Gleichungsforderungen

$$a \cdot x \doteq b \quad \text{und} \quad y \cdot a \doteq b$$

erfüllbar sind.

Der bekannteste Schiefkörper ist der Schiefkörper der *Quaternionen,* vgl. [4]. Ziel dieses Abschnitts ist es zu zeigen, dass jeder endliche Schiefkörper kommutativ ist.

Den Weg dorthin skizzieren wir durch Aufgaben, die dem Leser zuzumuten sein sollten.

8. 2. 14 Aufgabe. *Ist $\mathfrak{U}$ eine Untergruppe der Gruppe, so bildet gUg^{-1} für jedes $g \in G$ eine zu $\mathfrak{U}$ isomorphe Untergruppe von $\mathfrak{G}$.*

8. 2. 15 Definition. Zwei Untergruppen $\mathfrak{U}, \mathfrak{V}$ einer Gruppe $\mathfrak{G}$ heißen konjugiert, wenn ein $g \in G$ mit $V = gUg^{-1}$ existiert. Zwei Elemente a, b aus G heißen konjugiert, wenn ein $g \in G$ mit $b = gag^{-1}$ existiert.

Man bestätigt leicht, dass in beiden Fällen Äquivalenzrelationen definiert werden. Die Menge aller Untergruppen von $\mathfrak{G}$ zerfällt also in Klassen konjugierter, paarweise zueinander isomorpher Untergruppen, und die Menge aller Elemente von G zerfällt in Klassen paarweise konjugierter Elemente.

8. 2. 16 Definition. Es sei g ein Element der Gruppe $\mathfrak{G}$ und M die Menge aller $m \in G$ mit $mgm^{-1} = g$ bzw. – gleichwertig – $mg = gm$. Dann heißt M der *Normalisator* von $g \in G$.

8. 2. 17 Proposition. *Man zeige: Es sei $\mathfrak{G}$ eine Gruppe und M der Normalisator von $g \in G$. Dann ist M operativ abgeschlossen, und die Anzahl der Konjugierten von g ist gleich dem Index von $\mathfrak{M}$ in $\mathfrak{G}$.*

Dies bedeutet insbesondere: Ist G endlich, so ist die Anzahl der Konjugierten von $g \in G$ gleich $|\,G\,| : |\,M\,|$.

BEWEIS. Wir erhalten geradeaus, dass M abgeschlossen ist bezüglich Multiplikation und Inversenbildung, also eine Untergruppe von $\mathfrak{G}$ „trägt".

Liefern nun $x, y \in G$ dasselbe Konjugierte von g, ist also $xgx^{-1} = ygy^{-1}$, so folgt $y^{-1}xg = gy^{-1}x$, also $y^{-1}x \in M$ bzw. $x \in yM$, d.h. so liegen x und y in derselben Linksnebenklasse von M.

Und liegen andererseits zwei Elemente hm_1 und hm_2 in derselben Linksnebenklasse hM so liefern sie dasselbe Konjugierte hgh^{-1} von g, wegen

$$(hm_1)g(hm_1)^{-1} = hm_1gm_1^{-1}h^{-1} = hgm_1m_1^{-1}h^{-1} = hgh^{-1}.$$

Damit ist gezeigt: die Anzahl der Konjugierten von g ist gleich dem Index von $\mathfrak{M}$ in $\mathfrak{G}$. □

8. 2. 18 Aufgabe. *Es sei $\mathfrak{S}$ ein Schiefkörper. Dann bezeichnet man die Menge $Z \subset S$ aller Elemente $z \in S$, die mit jedem $s \in S$ vertauschbar sind, als das Zentrum von $\mathfrak{S}$. Man zeige: Das Zentrum von $\mathfrak{S}$ ist operativ abgeschlossen bzw. bildet einen Unterkörper $\mathfrak{Z}$ von $\mathfrak{K}$.*

8. 2. 19 Aufgabe. *Man zeige: Es sei $\mathfrak{S}$ ein Ober-Schiefkörper über $\mathfrak{K}$. Dann stiftet die Festsetzung*

$$a \propto A :\Longleftrightarrow a = \kappa_1 a_1 + \kappa_2 a_2 + ... + \kappa_n a_n \quad (\kappa_\nu \in K)$$

eine lineare Abhängigkeitsrelation.

8. 2. 20 Definition. Es sei $\mathfrak{S}$ ein Ober-Schiefkörper über $\mathfrak{K}$. Dann bezeichnen wir wie im Kommutativen die allen Basen zu $\propto$ gemeinsame Länge als den Grad von $\mathfrak{S}$ über $\mathfrak{K}$.

8. 2. 21 Aufgabe. *Man zeige: Ist $\mathfrak{S}$ ein endlicher Schiefkörper vom Grade n über seinem Zentrum $\mathfrak{Z}$ von der Mächtigkeit $|\,Z\,| = q$, so hat $\mathfrak{S}$ q^n viele Elemente.*

In den Beweis des Satzes von WEDDERBURN wird die Theorie der Kreisteilung wesentlich eingehen. Hierzu erwähnen wir:

Sei m eine natürliche Zahl. Wir betrachten das Polynom $x^m - 1$. Es zerfällt über jedem Oberkörper von $\mathbf{Q}$, in dem es überhaupt zerfällt, z.B. im Körper der komplexen Zahlen, aber natürlich auch in jeder sukzessiven Stammkörpererweiterung von $\mathbf{Q}$, in der $x^m - 1$ linear zerfällt, in, vgl. 8.2.12, m paarweise verschiedene Linearfaktoren:

$$x^m - 1 = (x - \zeta_1)(x - \zeta_2)\dots(x - \zeta_m).$$

Dabei sind die ζ_ν $(1 \le \nu \le m)$ die sämtlichen m-ten Einheitswurzeln und bilden nach 8.2.12 eine zyklische Gruppe, o.B.d.A. erzeugt von $\zeta := \zeta_1$ mit $\zeta_\nu = \zeta^\nu$ und damit exakt von den $\varphi(n)$ vielen ζ^ν mit $\nu \perp n$ bzw. $(\nu, n) = 1$.

Zur Erinnerung

8. 2. 22 Definition. Unter dem *m-ten Kreisteilungspolynom* versteht man das Polynom

$$\Phi_m(x) = \prod_{1 \le \nu \le m}^{(\nu,m)=1} (x - \zeta_\nu)\,, \tag{8.1}$$

8. 2. 23 Aufgabe. *Man zeige*

$$x^m - 1 = \prod_{n|m} \phi_n(x)\,. \tag{8.2}$$

8. 2. 24 Aufgabe. *Man beweise induktiv unter Einsatz der – früher aus der Mittelstufe bekannten – Polynom-Division mit Rest*

$$\Phi_m(x) \in \mathfrak{Z}[x]. \tag{8.3}$$

Hiernach lässt sich verifizieren

8. 2. 25 Theorem. Der Satz von Wedderburn: *Jeder endliche Schiefkörper ist kommutativ.*

BEWEIS. Wir führen den Beweis nach Ernst Witt.

Es sei $\mathfrak{S}$ ein endlicher Schiefkörper und $\mathfrak{Z}$ das Zentrum von $\mathfrak{S}$.

Es ist zu zeigen $Z = S$. Wir setzen

$$\mathfrak{S} : \mathfrak{Z} =: n$$

und $|\, Z \,| =: q$, dann gilt $q \geq 2$ und $|\, S \,| = q^n$.

Nun betrachten wir für ein festes $s \in S$ den Normalisator $N(s)$ von s. Man bestätigt leicht, dass $N(s) \supseteq Z$ bezüglich $+$ und $\cdot$ die Schiefkörperbedingungen erfüllt. Also ist $|\, N(s) \,| = q^{\,d}$ eine Potenz von $|\, Z \,| = q$. Da ferner $S \supseteq N(s)$ erfüllt ist, also auch eine Potenz von $|\, N(s) \,| = q^{\,d}$ ist, folgt zusätzlich $d \,\big|\, n$.

Wir zerlegen nun die multiplikative Gruppe $\mathfrak{S}_0$ von $\mathfrak{S}$ in Klassen konjugierter Gruppenelemente und zählen die Elemente der einzelnen Klassen ab. Insgesamt hat $\mathfrak{S}_0$ die Ordnung $|\, S_0 \,| = q^n - 1$. Nach 8.2.17 ist die Anzahl der Konjugierten eines $s \in S_0$ gleich dem Index des Normalisators $N_0(s) = \{x \in N(s) : x \neq 0\}$, also eine Zahl der Gestalt

$$\frac{q^n - 1}{q^d - 1} \quad \text{mit} \quad d \,\big|\, n\,. \tag{8.4}$$

Wir werden zeigen, dass die multiplikativen Gruppen von $\mathfrak{S}$ und $\mathfrak{Z}$ überein stimmen, also $S_0 = Z_0$ erfüllt ist.

Angenommen, das wäre nicht der Fall, dann wäre der Grad von $\mathfrak{S}$ über $\mathfrak{Z}$ größer als 1. Außerdem gäbe es ein $s \in S_0$, dessen Normalisator $N_0(s)$ von S_0 verschieden wäre, denn jedes $s \in S_0$, das nicht in Z_0 liegt, würde dies erfüllen. Die Klasse der Konjugierten, zu der dieses Element s gehörte, hätte

$$\frac{q^n - 1}{q^d - 1}$$

viele Elemente, mit echtem Teiler d von n. Es könnte sein, dass es mehrere solcher Klassen gäbe. Jedes der $q - 1$ Elemente des Zentrums Z_0 von S_0 aber bildet eine Klasse für sich.

Somit ergäbe sich durch Abzählen eine Gleichung der Form

$$q^n - 1 = (q - 1) + \sum \frac{q^n - 1}{q^d - 1}, \tag{8.5}$$

in der n und q von 1 verschiedene natürliche Zahlen sind und rechts über einen gewissen echten Teiler d von n summiert wird.

Nun ist aber

$$x^n - 1 = \prod_{m|n} \Phi_m(x)\,.$$

Für jeden echten Teiler d von n folgt dementsprechend

$$x^d - 1 = \prod_{m|d} \Phi_m(x)$$

und damit auch

$$\frac{x^n - 1}{x^d - 1} = \Phi_n(x) g(x) \tag{8.6}$$

in $\mathfrak{Z}[x]$.

Ersetzt man nun in (8.6) x durch q und vergleicht dann (8.6) mit (8.5), so erkennt man, dass in (8.5) sowohl $q^n - 1$ als auch die Summe rechts durch $\Phi_n(q)$ teilbar sind. Also müsste auch $q - 1$ den Teiler $\Phi_n(q)$ haben. Das aber führt zum Widerspruch!

DENN: Für $n > 1$ ist $|\,\Phi_n(q)\,| > q - 1$, man beachte die Zerlegung

$$\Phi_n(x) = \prod (x - \zeta_\nu)$$

in $\mathfrak{C}[x]$, worin die ζ_ν gerade die $\varphi(n)$ primitiven n-ten Einheitswurzeln durchlaufen. Für $n > 1$ ist keine von ihnen gleich 1, was $|\,q - \zeta_\nu\,| > q - 1 \geq 1$ impliziert und damit

$$|\,\Phi_n(q)\,| = \prod |\,q - \zeta_\nu\,| > q - 1.$$

Damit ist der Satz bewiesen. □

Kapitel 9

Klassik

9.1 Ein Satz von Abel

Als nächstes präsentieren wir einen Satz von Abel.

9. 1. 1 Der Satz vom primitiven Element. *Sei $\mathfrak{K}$ ein Körper der Charakteristik 0 oder ein endlicher Körper. Dann ist jedes $\mathfrak{K}[\,\alpha,\beta\,]$ mit algebraischen Elementen α,β ein $\mathfrak{K}[\,\vartheta\,]$.*

BEWEIS. Wir können uns auf den Fall der Charakteristik 0 beschränken, da endliche Körper, wie wir sahen, 1-erzeugt sind.

Zu α bzw. β gehört jeweils ein eindeutig bestimmtes normiertes irreduzibles Polynom f_α bzw. f_β.

Wir bilden $f_\alpha \cdot f_\beta$ und hierzu einen Zerfällungskörper $\mathfrak{Z}$ über $\mathfrak{K}[\,\alpha,\beta\,]$.

Dann zerfallen f_α und f_β in

$$\begin{aligned} f_\alpha(x) &= (x-\alpha_1)(x-\alpha_2)\cdot\ldots\cdot(x-\alpha_m) \\ f_\beta(x) &= (x-\beta_1)(x-\beta_2)\cdot\ldots\cdot(x-\beta_n)\,, \end{aligned}$$

und wir dürfen o. B. d. A. $\alpha=\alpha_1$ und $\beta=\beta_1$ annehmen. Wegen $\operatorname{char}(\mathfrak{K})=0$ haben die beiden Polynome f_α und f_β in $\mathfrak{Z}$ nur einfache Nullstellen. Folglich sind die Polynome

$$\alpha_i+\beta_j x \;=:\; \vartheta_{i,j}(x)$$

paarweise verschieden, weshalb das Polynom

$$\prod\big(\vartheta_{i,j}(x)-\vartheta_{k,\ell}(x)\big)\;\;(i,j\neq k,\ell)$$

nicht verschwindet. Dann findet sich aber ein $a \in K$ mit

$$\alpha_i + \beta_j a \;\neq\; \alpha_k + \beta_\ell a \;\; (i,j \neq k,\ell)\,.$$

Wir bilden nun

$$\vartheta \;:=\; \alpha + \beta \cdot a$$

und danach

$$\begin{aligned}\Phi(x) &= \textstyle\prod_1^m \big(\vartheta - (\alpha_i + ax)\big)\\ &= \textstyle\prod \big((\alpha+\beta a) - (\alpha_i + ax)\big)\\ &= \textstyle\prod \big((\vartheta - ax) - \alpha_i\big)\\ &= f_\alpha(\vartheta - ax)\,.\end{aligned}$$

An der letzten Zeile erkennt man, dass $\Phi(x)$ ein Polynom über $\mathfrak{K}[\vartheta]$ ist und an der zweiten Zeile , dass $\beta_1 = \beta$ und unter den β_j nur dieses β_1 Nullstelle zu $\Phi(x)$ ist.

Das bedeutet dann, dass $\Phi(x)$ und $f_\beta(x)$ nur den Linearfaktor $x - \beta$ gemeinsam haben und folglich über $\mathfrak{K}[\vartheta]$

$$x - \beta \;=\; \Phi(x)\cdot u(x) + f_\beta(x)\cdot v(x)$$

erfüllt ist. Denn man beachte: jeder GGT zu $\Phi(x)$ und $f_\beta(x)$ in $\mathfrak{K}(\vartheta)[x]$ ist vom Grad 1 und lässt sich linear kombinieren. Also ist auch der normierte GGT $x - \gamma$ linear kombinierbar Über $\mathfrak{K}(\vartheta)[x]$ und es ist β Nullstelle von $x - \vartheta$, also $\vartheta = \beta$.

Dann liegt aber β in $\mathfrak{K}[\vartheta]$, also auch βa und damit auch $\alpha = \vartheta - \beta a$. Und das bedeutet

$$\mathfrak{K}[\,\alpha,\beta\,] \;=\; \mathfrak{K}[\,\vartheta\,]$$

□

9. 1. 2 Korollar. *Sind die Elemente α_i algebraisch über $\mathfrak{K}$ und ist $\mathfrak{K}$ endlich oder aber von der Charakteristik 0, so gibt es ein ϑ mit*

$$\mathfrak{K}[\,\alpha_1,\ldots,\alpha_n\,] \;=\; \mathfrak{K}[\,\vartheta\,]\,.$$

9.2 Der Fundamentalsatz der Algebra

Endlich kommen wir nach unseren allgemeinen Betrachtungen über das Problem der Elimination zu der klassischen Frage nach Nullstellen reeller Polynome. Wie nicht anders zu erwarten, treffen wir dabei auf besonders günstige Verhältnisse. Genauer gilt das wohl klassischste Resultat dieser Notizen:

9. 2. 1 Der Fundamentalsatz der Algebra. *Sei $f(z)$ ein Polynom über dem Körper $\mathfrak{C}$ der komplexen Zahlen. Dann besitzt f in $\mathbf{C}$ mindestens eine Nullstelle.*

Dies bedeutet dann nach dem Teilbarkeitslemma, dass jedes komplexe Polynom, also auch jedes reelle Polynom, *über $\mathfrak{C}$ in Linearfaktoren $(z-\alpha_i)$ $(1 \leq i \leq n)$ zerfällt.*

BEWEIS. Zunächst erkennen wir leicht, dass das Polynom $f \cdot \overline{f}$ stets reell ist, da die Koeffizienten c_k von $f \cdot \overline{f}$ jeweils gleich ihren Konjugierten $\overline{c}_k$ sind. (Zur Erinnerung: $\overline{a+bi} = a - bi$.)

Folglich können wir uns auf reelle Polynome beschränken, da jede Wurzel von $f \cdot \overline{f}$ eine Nullstelle von f oder eine solche von $\overline{f}$ ist und $\overline{f}(\alpha) = 0$ zu $f(\overline{\alpha}) = 0$ führt.

Weiterhin stimmen außerhalb von 0 die Funktionen $f(x)$ und $\dfrac{f(x)}{x^k}$ für gerades k in ihrem Vorzeichen überein. Das bedeutet aber, dass jedes reelle Polynom von ungeradem Grad sowohl positive als auch negative Werte annimmt und daher nach dem Nullstellensatz von ROLLE mindestens eine Nullstelle hat. Denn ist n gerade, so ist $n-1$ ungerade, und es wächst

$$f_1(x) := \frac{f(x)}{x^{n-1}} = \left[\frac{a_0}{x^{n-1}} + \frac{a_1}{x^{n-2}} + \ldots + a_{n-1}\right] + a_n \cdot x\,.$$

in beide Richtungen über alle Grenzen, da der Inhalt von[ ] für $x \longmapsto \pm\infty$ nach der *Limitenregel* gegen a_{n-1} strebt.

Dies liefert als ein erstes Zwischenergebnis

(1) Alle reellen Polynome von einem Grad, der sich durch 2^0, nicht aber durch 2^1 teilen lässt , besitzen eine Nullstelle in $\mathbf{C}$.

(2) Wir induzieren nun über den Grad und nehmen zu diesem Zweck an, es sei schon bewiesen, dass alle Polynome von einem Grad, der sich durch

$2^{\kappa-1}$ teilen lässt, nicht aber durch 2^{κ}, eine Nullstelle besitzen und betrachten ein Polynom $f(x)$ vom Grade n mit $2^{\kappa} \mid n$, aber $2^{\kappa+1} \nmid n$.

Dann gibt es nach dem Satz von STEINITZ einen Zerfällungskörper [1] zu $f(x)$ über $\mathfrak{C}$, also einen Erweiterungskörper $\mathfrak{W}$ von $\mathfrak{C}$, mit

$$f(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n) \ \ (\alpha_i \in W) .$$

Obwohl die einzelnen α_i natürlich nicht in $\mathbf{C}$ liegen müssen, sind die elementarsymmetrischen Werte dieser α_i aus $\mathbf{R}$, da sie ja bis auf das Vorzeichen gleich den Koeffizienten von f sind. Dies wird von entscheidender Bedeutung sein.

(3) Wir bilden nun das Polynom

$$F\big(y, h\big) := \prod_{i<k} \big(y - (h + \alpha_i)(h + \alpha_k)\big) = \prod_{i<k} f_{i,k} .$$

Dieses Polynom ist symmetrisch in den α_i $(1 \leq i \leq n)$, d. h., es sind die Koeffizienten von F ganz-rationale Polynome in den α_i, aber invariant gegenüber allen Permutationen der α_i. Somit sind die Koeffizienten von F nach dem Hauptsatz über symmetrische Funktionen Werte von Polynomen der elementarsymmetrischen Funktionswerte $\sigma_i(\alpha_1, \ldots, \alpha_n)$ $(1 \leq i \leq n)$ und damit reell.

Das bedeutet aber, dass wir bei Einsetzen eines reellen Wertes für h ein reelles Polynom in y vom Grade

$$\binom{n}{2} = \frac{n \cdot (n-1)}{1 \cdot 2}$$

erhalten, dessen Grad teilbar ist durch $2^{\kappa-1}$, nicht aber durch 2^{κ}.

(4) Daher besitzt jedes $F(y, h)$ mit $h \in \mathbf{R}$ mindestens eine Nullstelle in $\mathbf{C}$. Nun hat aber $\mathbf{R}$ unendlich viele Elemente. Deshalb gibt es zwei Elemente h_1, h_2, derart dass für h_1 und für h_2 der gleiche Faktor $f_{i,k}$ eine komplexe Nullstelle besitzt. Das bedeutet dann nach Umnummerierung ohne Beschränkung der Allgemeinheit:

$$\begin{aligned} z_1 - (h_1 + \alpha_1)(h_1 + \alpha_2) &= 0 \\ z_2 - (h_2 + \alpha_1)(h_2 + \alpha_2) &= 0 , \end{aligned}$$

[1] Tatsächlich genügt weniger, siehe den nächsten Abschnitt

also

$$\begin{aligned}(\alpha_1+\alpha_2)\cdot h_1+\alpha_1\cdot\alpha_2 &\in \mathbf{C}\\ (\alpha_1+\alpha_2)\cdot h_2+\alpha_1\cdot\alpha_2 &\in \mathbf{C}\,,\end{aligned}$$

und damit

$$(\alpha_1+\alpha_2)\cdot(h_1-h_2)\in\mathbf{C}\,,$$

woraus dann zunächst $\alpha_1+\alpha_2\in\mathbf{C}$ und hiernach weiter $\alpha_1\cdot\alpha_2\in\mathbf{C}$ resultiert.

Daher ist das Polynom $(x-\alpha_1)(x-\alpha_2)$ komplex. Es haben aber komplexe Polynome vom Grade 2 stets eine komplexe Nullstelle. Folglich hat auch $f(x)$ eine komplexe Nullstelle, was zu beweisen war. □

9.3 Eine Retrospektive

Für den Lehramtskandidaten steht in der Algebra natürlich ein und nur ein Satz im Vordergrund: *Der Fundamentalsatz*. Nach der Erweiterung von $(\mathbf{N},+)$ zu $(\mathbf{Z},+)$ haben wir einen Zahlbereich entwickelt, in dem alle Forderungen $a+x\doteq b$ erfüllbar sind, nach der Erweiterung von $(\mathbf{Z},+,\cdot)$ zu $(\mathbf{Q},+,\cdot)$ einen Zahlbereich, in dem alle Forderungen $ax+b\doteq cx+d$ erfüllbar sind, und schließlich nach Übergang zu $(\mathbf{R},+,\cdot)$ einen Bereich, in dem alle Forderungen $f(x)\doteq 0$ mit $\operatorname{grad}(f)=2m+1$ erfüllbar sind.

Die allgemeine Frage aber stand noch aus, nämlich

> Gibt es einen $\mathbf{R}$ umfassenden Zahlbereich, in dem alle Forderungen
>
> $$\frac{f(x)}{g(x)}\doteq\frac{u(x)}{v(x)}$$
>
> erfüllbar sind

Diese Frage ist mit dem Fundamentalsatz beantwortet.

Wenngleich der Fundamentalsatz weit hinten in der Vorlesung steht, so ist er letztlich doch ein Satz der elementaren Algebra, durchaus jedem Studenten zumutbar, der Lehrer für Mathematik, welcher Stufe auch immer werden möchte.

Denn: Der Zwischenwertsatz ist äquivalent zum Axiom von der oberen Grenze, also elementar.

Die Division mit Rest ist Mittelstufenpensum, der daraus abgeleitete Euklidische Algorithmus paradigmatisch ableitbar in $(\mathbf{Z}, +, \cdot)$.

Also erhalten wir elementar-paradigmatisch die wichtige Einsicht:

Teilbarkeitslehre in $\mathfrak{K}[x]$
ist Teilbarkeitslehre in $\mathfrak{Z}$

Schauen wir weiter auf den Beweis.

Der Eliminationssatz arbeitet mit Kongruenzen, wie wir sie aus der elementaren Zahlentheorie kennen, man erinnere das Rechnen auf der Uhr. Der Ansatz:

$\mathfrak{K}[x]$ ist euklidisch, also gilt für irreduzible $p(x)$

$$p \nmid f \Longrightarrow \exists u, v : u \cdot p + v \cdot f = 1$$

und damit $\overline{f} \neq \overline{0} \Longrightarrow \overline{f} \mid \overline{1}$, d. h., $\overline{\mathfrak{K}}[\overline{x}]$ ist ein Körper mit

$$\overline{p}(\overline{x}) = \overline{0}\,.$$

Zusammen mit dem

Teilbarkeitslemma:

$$p(\alpha) = 0 = f(\alpha) \text{ führt für irreduzible } p \text{ zu } p \mid f$$

gewährleistet dies, dass man ausgehend von $\mathfrak{K}$ sukzessive zu einer Erweiterung von $\mathfrak{K}$ gelangt, in der p in Linearfaktoren zerfällt. Es besitzt aber jedes f einen irreduziblen Faktor, also finden wir zu einem beliebigen f eine Nullstelle in $\mathbf{C}$, wenn wir zu einem seiner irreduziblen Faktoren in $\mathbf{C}$ eine Nullstelle finden.

Folglich können wir auf den Satz über Zerfällungskörper verzichten, uns mit dem Eliminationssatz – ohne Isomorphiebeweis – begnügen und auf den ersten Teil des Satzes über symmetrische Funktionen beschränken, der die Darstellbarkeit sichert, ohne auf die Eindeutigkeit einzugehen.

WAS BLEIBT ist ein Rechnen mit Polynomen.

EINE DRINGENDE EMPFEHLUNG. Man mache sich noch einmal den Eliminationssatz (Satz über Stammkörper) klar, indem man das Polynom $p(x) = x^2 + x + 1$ über $\mathfrak{Z}_3$ studiert. $p(x)$ ist irreduzibel, denn sonst gäbe es

einen linearen Faktor, also eine Nullstelle in $\mathfrak{Z}_3$. Es verschwindet aber $p(x)$ für kein Element aus $\mathfrak{Z}_3$.

Hiernach bilde man alle Restklassen $\overline{f}$. Dies scheint zunächst ein hoffnungsloses Unterfangen, **jedoch**: da $x^2 \equiv -x - 1$ erfüllt ist, lässt sich zunächst jedes Polynom in ein kongruentes Polynom von einem Grad ≤ 1 überführen, weshalb wir nur diese Klassen zu berücksichtigen brauchen. Bezeichnen wir dann $\overline{x}$ mit α, so wird $\mathfrak{K}[\alpha]$ ausgeschöpft von den Elementen der Form $a+b\alpha$, mit a, b aus $\mathfrak{Z}_3$. Folglich können wir den Erweiterungskörper „hinschreiben".

Wenigstens einmal in seinem Leben sollte jeder Lehrer eine solche Elimination Schritt für Schritt vollzogen haben, denn es ist ja der Fundamentalsatz der Abschluss der Zahlbereichserweiterungen!!!

UND

Eine Didaktik, die ein solches Angebot nicht gewährleistet, sollte vielleicht ihre Praeferenzen überdenken.

Nach dem Fundamentalsatz sind alle rationalen Gleichungen über $\mathfrak{C}$ lösbar. So gesehen herrscht kein Bedarf an einem weiteren Ausbau unseres Zahlsystems.

Dennoch drängt sich natürlich die Frage auf, ob hinter dem Körper der komplexen Zahlen noch weitere „interessante Zahlbereiche" zu erwarten sind. Insbesondere drängt sich die Frage auf, ob nicht nur der $\mathbf{R}^2$, sondern auch noch weitere Vektorräume $\mathbf{R}^n$ $(n \geq 3)$ eine Körperstruktur tragen, deren Addition mit der Vektoraddition übereinstimmt.

Dies trifft wegen des Fundamentalsatzes nicht zu! Denn dieser Körper enthielte den Körper der komplexen Zahlen als Unterkörper und wäre von endlichem Grad über $\mathfrak{R}$, also algebraisch über $\mathfrak{C}$ und damit enthalten in $\mathfrak{C}$, da kein Polynom über $\mathfrak{C}$ mehr Nullstellen haben kann, als sein Grad angibt.

Allerdings lässt der $\mathbf{R}^4$ noch die Struktur eines Schiefkörpers zu, d.h. eines „Körpers" mit nicht kommutativer Multiplikation. Man bezeichnet die Elemente dieser Struktur als *Quaternionen* i. S. von *4-Tupeln.*

Quaternionen lassen sich natürlich auch auffassen als Paare, gebildet aus einer reellen Zahl (also einem Skalar) und einem dreidimensionalen Vektor. Die Multiplikation lässt sich dann über das skalare und das vektorielle Produkt von Vektoren derart beschreiben, dass physikalische Interpretationen in einem Raum-Zeit-Modell möglich werden.

9.4 Ein Projekt*)

9. 4. 1 Definition. Ein Ring $\mathfrak{S} = (S, +, \cdot)$, in dem für jedes $a \neq 0$ alle Gleichungsforderungen

$$a \cdot x \doteq b \quad \text{und} \quad y \cdot a \doteq b$$

erfüllbar sind, heißt ein Schiefkörper.

Der bekannteste Schiefkörper ist der Schiefkörper der Quaternionen, vgl. die Elementaria Mathematicae.

Ziel dieses Abschnitts ist es zu zeigen, dass jeder endliche Schiefkörper kommutativ ist.

Dem Weg dorthin skizzieren wir durch Aufgaben, die dem Leser zuzumuten sein sollten, deren Lösungen sich aber natürlich auch in jedem Buch über klassische Algebra finden, siehe etwa [8].

9. 4. 2 Aufgabe. *Man zeige: Ist $\mathfrak{S}$ ein Oberschiefkörper zu dem Schiefkörper $\mathfrak{K}$, so stiftet die Festsetzung*

$$a \propto A :\Longleftrightarrow a = \kappa_1 a_1 + \kappa_2 a_2 + ... + \kappa_n a_n \quad (\kappa_\nu \in K)$$

eine lineare Abhängigkeitsrelation.

9. 4. 3 Aufgabe. *Man zeige: Ist $\mathfrak{S}$ ein endlicher Schiefkörper vom Grade n über dem Schiefkörper $\mathfrak{E}$, d.h. haben alle Basen zu $\propto$ die Länge $n =: \mathfrak{S} : \mathfrak{E}$, so hat $\mathfrak{S}$ q^n viele Elemente.*

9. 4. 4 Aufgabe. *Man zeige: Es sei $\mathfrak{S}$ ein Schiefkörper und $Z \subset S$ die Menge aller derjenigen Elemente $z \in S$, die mit jedem $s \in S$ vertauschbar sind. Dann ist Z operativ abgeschlossen, bildet also einen Körper, bezeichnet als das Zentrum $\mathfrak{Z}$. von $\mathfrak{S}$.*

9. 4. 5 Aufgabe. *Man zeige: Ist U eine Untergruppe der Gruppe G und $g \in G$, so ist gUg^{-1} eine zu U isomorphe Untergruppe von G.*

Definition : Zwei Untergruppen U, V einer Gruppe G heißen konjugiert, wenn ein $g \in G$ mit $V = gUg^{-1}$ existiert. Zwei Elemente $a,\ b$ aus G heißen konjugiert, wenn ein $g \in G$ mit $b = gag^{-1}$ existiert.

Man prüft sofort nach, dass in beiden Fällen Äquivalenzrelationen definiert werden. Die Menge aller Untergruppen von G zerfällt also in Klassen konjugierter, unter sich isomorpher Untergruppen; die Menge aller Elemente von G lässt sich aufteilen in Klassen konjugierter Elemente.

9. 4. 6 Definition. Es sei g ein Element der Gruppe G und M die Menge aller $m \in G$ mit $mgm^{-1} = g$ oder, gleichwertig, $mg = gm$. Dann heißt M der **Normalisator** von $g \in G$.

9. 4. 7 Proposition. *Man zeige: Es sei G eine Gruppe und M der Normalisator von $g \in G$. Dann ist M eine Untergruppe von G, und die Anzahl der Konjugierten von g ist gleich dem Index von M in G.*

BEWEIS. Wir erhalten geradeaus, dass M abgeschlossen ist bezüglich Multiplikation und Inversenbildung, also eine Untergruppe von $\mathfrak{G}$ „trägt".

Liefern nun $x, y \in G$ dasselbe Konjugierte von g, ist also $xgx^{-1} = ygy^{-1}$, so folgt $y^{-1}xg = gy^{-1}x$, also $y^{-1}x \in M$ oder $x \in yM$, d.h. so liegen x und y in derselben Linksnebenklasse von M.

Und liegen andererseits zwei Elemente hm_1 und hm_2 in derselben Linksnebenklasse hM so liefern sie dasselbe Konjugierte hgh^{-1} von g, wegen

$$(hm_1)g(hm_1)^{-1} = hm_1gm_1^{-1}h^{-1} = hgm_1m_1^{-1}h^{-1} = hgh^{-1}.$$

Damit ist gezeigt: die Anzahl der Konjugierten von g ist gleich dem Index von M in G. □

In den angestrebten Beweis wird der Fundamentalsatz der Algebra ganz wesentlich eingehen:

Es sei m eine natürliche Zahl. Wir betrachten das Polynom $x^m - 1$. Es zerfällt in $\mathfrak{C}[x]$ in Linearfaktoren:

$$x^m - 1 = (x - \zeta_1)(x - \zeta_2)\dots(x - \zeta_m).$$

Dabei sind die komplexen Zahlen ζ_ν $(1 \leq \nu \leq m)$ die sämtlichen m-ten Einheitswurzeln und bilden eine zyklische Gruppe, vgl. 8.2.12, mit $\zeta_\nu = \zeta^\nu$, die o.B.d.A. erzeugt sei von $\zeta := \zeta_1$ und damit exakt auch von allen ζ^ν mit $\nu \perp n$ bzw. $(\nu, n) = 1$. Deren Zahl wird nach Euler mit $\varphi(n)$ bezeichnet. Diese

Erzeugenden bestimmen das m-te Kreisteilungspolynom

$$\Phi_m(x) = \prod_{1\le\nu\le m}^{(\nu,m)=1} (x - \zeta^{\nu}) \tag{9.1}$$

9. 4. 8 Aufgabe. *Man zeige induktiv:*

$$\Phi_m(x) \in \mathfrak{Z}[x]. \tag{9.2}$$

9. 4. 9 Aufgabe. *Man zeige*

$$x^m - 1 = \prod \phi_n(x) \ \ (n \parallel m)\,. \tag{9.3}$$

Hiernach lässt sich beweisen:

9. 4. 10 Der Satz von Wedderburn. *Jeder endliche Schiefkörper ist kommutativ.*

BEWEIS. Wir führen den Beweis nach Ernst Witt.

Es sei $\mathfrak{S}$ ein endlicher Schiefkörper und $\mathfrak{Z}$ das Zentrum von $\mathfrak{S}$.

Es ist zu zeigen $Z = S$. Wir setzen

$$\mathfrak{S} : \mathfrak{Z} =: n$$

Ist nun $|Z| = q > 1$, so gilt $|S| = q^n$.

Für ein festes $s \in S$ betrachten wir den Normalisator $N(s)$ von s. Man bestätigt leicht, dass $N(s) \subset Z$ ein Schiefkörper ist. Nach Satz (2) ist also $|\,N(s)\,| \ = \ q^d$ eine Potenz von $|\,Z\,| \ = \ q$. Da ferner $S \subset N(s)$, also auch $|\,S\,| \ = \ q^n$ eine Potenz von $|\,N(s)\,| \ = \ q^d$ ist, folgt zusätzlich $d \,|\, n$.

Dies nutzen wir in der folgenden gruppentheoretischen Überlegungen aus (Bedingungen (3)-(5)). Wir zerlegen die multiplikative Gruppe S_0 von S in Klassen konjugierter Gruppenelemente (siehe (6)-(10)) und zählen die Elemente der einzelnen Klassen ab. Insgesamt hat S_0 die Ordnung $|\,S_0\,| \ = \ q^n - 1$. Nach Satz (6) ist die Anzahl der Konjugierten eines $s \in S_0$ gleich dem Index des Normalisators $N_0(s) \ = \ \{x \in N(s) : x \neq 0\}$; das ist also eine Zahl der Gestalt

$$\frac{q^n - 1}{q^d - 1} \text{ mit } d \,\big|\, n\,. \tag{9.4}$$

Wir wollen zeigen, dass die multiplikativen Gruppen von S und Z übereinstimmen, also dass $S_0 = Z_0$ erfüllt ist.

Angenommen, das wäre nicht der Fall, dann hätte S über Z einen Grad größer als 1. Außerdem gäbe es ein $s \in S_0$, dessen Normalisator $N_0(s)$ von S_0 verschieden wäre; jedes $s \in S_0$, das nicht in Z_0 liegt, leistet dies. Die Klasse Konjugierter, zu der dieses Element s gehört, hat

$$\frac{q^n - 1}{q^d - 1}$$

viele Elemente, wobei d ein echter Teiler von n ist. Es könnte sein, dass es mehrere solcher Klassen gibt; jedes der $q - 1$ Elemente des Zentrums Z_0 von S_0 aber bildet eine Klasse für sich.
Zählt man also die $q^n - 1$ Elemente von S_0 in dieser Weise ab, so ergibt sich eine Gleichung

$$q^n - 1 \;=\; q - 1 + \sum \frac{q^n - 1}{q^d - 1}, \tag{9.5}$$

in der n und q von Eins verschiedene natürliche Zahlen sind und rechts über einen gewissen echten Teiler d von n summiert wird.

Nun ist aber

$$x^n - 1 = \prod_{m|n} \Phi_m(x)\,.$$

Für einen echten Teiler d von n folgt dementsprechend

$$x^d - 1 = \prod_{m|d} \Phi_m(x)$$

und damit auch

$$\frac{x^n - 1}{x^d - 1} = \Phi_n(x) g(x)$$

in $\Psi[x]$.

Ersetzt man x durch q, so sieht man, dass in (9.5) sowohl $q^n - 1$ als auch die Summe rechts durch $\Phi_n(q)$ teilbar sind; also müsste auch $q - 1$ den Teiler $\Phi_n(q)$ haben.
Wir sind fertig, wenn wir im Widerspruch dazu zeigen:

Für $n > 1$ ist $|\,\Phi_n(q)\,| > q - 1$. Dazu erinnern wir an die Zerlegung

$$\Phi_n(x) = \prod (x - \zeta_\nu)$$

in $\mathbf{C}\ [x]$, worin die ζ_ν gerade die $\varphi(n)$ primitiven n-ten Einheitswurzeln durchlaufen:

Für $n > 1$ ist keine von ihnen gleich Eins, folglich $|\, q - \zeta_\nu \,| > q - 1 \geq 1$ und

$$|\, \Phi_n(q) \,| = \prod |\, q - \zeta_\nu \,| > q - 1.$$

Damit ist der Satz bewiesen. □

9.5 Klassische Algebra und Geometrie

Wir möchten an dieser Stelle – lehramts-orientiert – einige klassische geometrische Probleme aufgreifen. Zu Beginn der Grundgedanke:

Sind endlich viele rationale Punkte gegeben, so erhalten wir im Rahmen einer Zirkel&Lineal-Konstruktion von Schritt zu Schritt einen Punkt hinzu, dessen Koordinaten sich jeweils in der Form $a_x + b_x\sqrt{c}$ bzw. $a_y + b_y\sqrt{c}$) schreiben lassen, wobei die Elemente a_x, b_x, a_y, b_y, c jeweils dem bereits erreichten Körper entstammen..

DENN: Sind g_1 und g_2 zwei Geraden über einem Körper $\mathfrak{K}$, so liegen die Koordinaten ihres Schnittpunktes in K.

Sind weiter g und k eine Gerade und ein Kreis, etwa

$$g \equiv \quad y = mx + b \tag{9.6}$$

$$k \equiv \quad (y-b)^2 + (x-a)^2 = r^2 \tag{9.7}$$

so sehen wir sofort, dass nach der Einsetzungsmethode zunächst die x-Werte der gemeinsamen Schnittpunkte und damit dann auch die korrespondierenden y-Werte vom Typus $a \pm b\sqrt{c}\ \ (a, b, c \in K)$, sofern sich die beiden Kurven schneiden.

Ist aber der Schnittpunkt zweier Kreise zu ermitteln, so lässt sich dies zurückführen auf den Schnitt eines Kreises mit einer Geraden.

HINWEIS: Man beachte in der Abbildung 9.1 die Gleichungen:

$$\begin{array}{rcl} & |M_1S_1|^2 - |M_1F|^2 & = & |M_2S_1|^2 - |M_2F| \\ \rightsquigarrow & |M_1S_1|^2 + |M_2F|^2 & = & |M_2S_1|^2 + |M_1F|^2 \end{array}$$

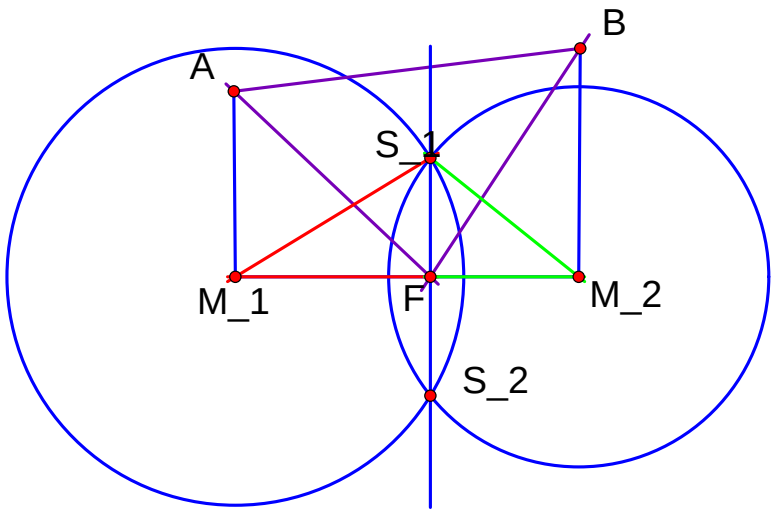


Abbildung 9.1: Kreis – Kreis – und Gerade

Sie liefern ein Konstruktionsverfahren für F. Denn, man trage r_2 in M_1 und r_1 in M_2 jeweils senkrecht nach oben auf. Dann schneidet die Symmetrieachse zur Verbindungsstrecke der beiden Endpunkte – sag' A und B – die Zentrale M_1M_2 in F.

Das bedeutet aber, dass wir den Schnittpunkt zweier Kreise auch als Schnittpunkt eines Kreises mit einer Geraden gewinnen können.

Daher entspricht unserer Konstruktion in jedem Falle am Ende eine Kette

$$\mathfrak{K} \subseteq \mathfrak{K}[\alpha_1] \subseteq \mathfrak{K}[\alpha_2] \subseteq \mathfrak{K}[\alpha_3] \subseteq \mathfrak{K}[\alpha_4] \subseteq \ldots\ldots \subseteq \mathfrak{K}[\alpha_n]$$

im Sonderfall also eine Kette

$$\mathfrak{Q} \subseteq \mathfrak{Q}[\alpha_1] \subseteq \mathfrak{Q}[\alpha_2] \subseteq \mathfrak{Q}[\alpha_3] \subseteq \mathfrak{Q}[\alpha_4] \subseteq \ldots\ldots \subseteq \mathfrak{Q}[\alpha_n]$$

worin jedes α_i $(1 \leq i \leq n)$ Quadratwurzel über dem Körper $\mathfrak{Q}[\alpha_{i-1}]$ – mit $\mathfrak{Q}[\alpha_0] := \mathfrak{Q}$.

Hiernach ein wenig elementare Algebra

9. 5. 1 Lemma. *Jedes Polynom dritten Grades über* $\mathbf{R}$ *hat – wie wir schon oben sahen – mindestens eine reelle Nullstelle.*

BEWEIS. Sei o.B.d.A.

$$f(x) = a_0 + a_1x + a_2x^2 + x^3\,. \tag{9.8}$$

Dann ist $f(x)$ genau dann positiv bzw. negativ an der Stelle a, wenn

$$g(x) = \left(\frac{a_0}{x^2} + \frac{a_1}{x^1} + a_2\right) + x \tag{9.9}$$

an dieser Stelle positiv bzw. negativ ist.

Es strebt aber die Klammer für $x \to \infty$ gegen a_2, weshalb bei hinreichend großem $|a|$ das Polynom je nach $a > 0$ bzw. $a < 0$ einen positiven bzw. einen negativen Wert annimmt. Folglich existiert nach dem Zwischenwertsatz eine Nullstelle α zwischen $|a|$ und $-|a|$. □

Nach der Division mit Rest haben wir hiernach weiter

$$f(x) = q(x)(x - \alpha) + r(x)$$

mit $\operatorname{grad} r(x) < 1$ also $\operatorname{grad} r(x) = 0$ und damit $r(x) = c$ mit $f(\alpha) - q(\alpha) \cdot (x - \alpha) = 0$, woraus $r(x) = c = 0$ und somit

$$f(x) = q(x) \cdot (x - \alpha) \tag{9.10}$$

mit quadratischen Polynom $q(x)$ resultiert.

Zerlegung von $q(x)$ in $(x - \beta_1)(x - \beta_2)$ liefert uns schließlich

$$f(x) = (x - \alpha)(x - \beta_1)(x - \beta_2) \tag{9.11}$$

Die Koeffizienten von f sind rational, die Nullstelle muss aber keineswegs rational sein, man denke hier beispielsweise an $x^2 - 2 := 0$.

Nun kommen wir zu dem zentralen Ergebnis dieses Abschnitts:

9. 5. 2 Ein Satz von Landau. *Sei*

$$f(x) = a_0 + a_1 x + a_2 x^2 + x^3$$

ein (kubisches) Polynom in rationalen Koeffizienten und sei

$$\mathbf{Q}^{(1)} \subseteq \mathbf{Q}^{(2)} \subseteq ... \subseteq \mathbf{Q}^{(n)}$$

eine Folge von quadratischen Erweiterungen im obigen Sinne, also $\mathbf{Q}^{(k+1)} = \mathbf{Q}^{(k)}\left[\sqrt{\alpha_k}\right]$ $\left(\alpha_k \notin \mathbf{Q}^{(k)}\right)$ $(1 \leq k \leq n)$.

Hat dann $f(x)$ eine Nullstelle in $\mathbf{Q}^{(n)}$*, so hat $f(x)$ auch eine Nullstelle in* $\mathbf{Q}$.

BEWEIS. Es sei o.B.d.A. α_1 eine Lösung aus $\mathbf{Q}^{(n)}$, die nicht in $\mathbf{Q}^{(n-1)}$ liegt. Dann gilt

$$\alpha_1 = a + b\,\xi \tag{9.12}$$

mit $a, b \in \mathbf{Q}^{(n-1)}$ und $\xi^2 = c \in \mathbf{Q}^{(n)}$.
Wir bilden nun zu $a + b\,\xi$ die $a + b\,\xi$ in $\mathbf{Q}^{(n)}$ zugeordnete Zahl

$$\alpha_1^* = a - b\,\xi\,. \tag{9.13}$$

Wie vom Rechnen mit komplexen Zahlen her schon bekannt, stellen sich dann die Regeln

$$(x+y)^* = x^* + y^* \quad \text{und} \quad (xy)^* = x^* \cdot y^* \tag{9.14}$$

ein. Es ist also dann – wie oben im Sonderfall $\overline{z}$ –

$$(f(x))^* = f(x^*) \tag{9.15}$$

und daher mit α_1 auch α_1^* Nullstelle von $f(x)$. Nun gilt aber für die Lösungen der Gleichung

$$a_0 + a_1 x + a_2 x^2 + x^3 = 0$$

die Formel

$$-a_2 = \alpha_1 + \alpha_2 + \alpha_3\,, \tag{9.16}$$

also auch die Formel

$$\alpha_3 = -(\alpha_1 + \alpha_2) - a_2 = -a_2 - 2a \qquad (9.12, 9.13) \tag{9.17}$$

Folglich liegt α_3 in $\mathbf{Q}^{(n-1)}$, ist also vom Typ

$$\alpha_3 = u + v\,\eta, \quad \eta^2 = w \quad u, v, w \in \mathbf{Q}^{(n-2)}\,. \tag{9.18}$$

Weiter ist mit α_3 auch α_3^* eine Wurzel von $f(x)$ und zwar verschieden von α_1, α_2, da diese beiden Wurzeln nicht zu $\mathbf{Q}^{(n-1)}$ gehören. Also muss $\alpha_3 = \alpha_3^*$ sein, da $f(x)$ nur drei Wurzeln hat. Das liefert dann $w = \eta = 0$ und damit $\alpha_3 \in \mathbf{Q}^{(n-2)}$, so dass wir unser Verfahren fortsetzen können, bis schließlich $\alpha_3 \in \mathbf{Q}$ bewiesen ist. □

Der soeben bewiesene Satz gibt uns die Möglichkeit, zu zeigen, dass sich kein allgemeines Verfahren für die Dreiteilung des Winkels mit Zirkel und Lineal

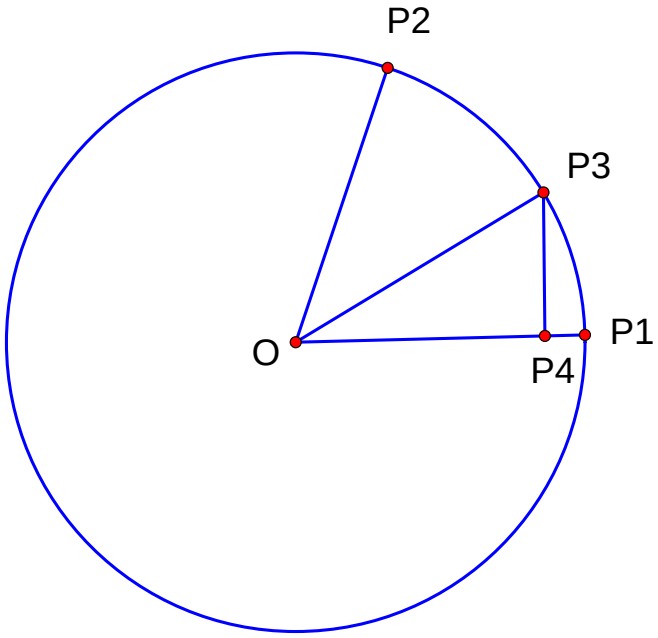


Abbildung 9.2: Zur Trisektion

und – ebenso wenig – ein Verfahren für die Verdoppelung des Würfels mit Zirkel und Lineal entwickeln lässt.

DENN: Wir betrachten den Einheitskreis. Es sei $\angle P_1OP_2$ ein Winkel von $60°$ und $\beta = \angle P_1OP_3$ ein Drittel dieses Winkels, also ein Winkel von $20°$. Ließe sich der Winkel $\angle P_1OP_3$ konstruieren, so auch der Fußpunkt P_4 des Lotes von P_3 auf die x-Achse. Es gilt aber wegen

$$\cos^2\alpha = 1 - \sin^2\alpha \text{ und } \cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$$

die Gleichheit

$$\cos 3\beta = 4\cos^3\beta - 3\cos\beta. \tag{9.19}$$

Setzen wir nun $y := 2\cos\beta, 3\beta = \alpha$ so ergibt sich aus (9.19) die Gleichung

$$y^3 - 3y - 2\cos\alpha = 0\,. \tag{9.20}$$

Wegen $\alpha = 60°$ gilt aber $\cos\alpha = \frac{1}{2}$, was (9.20) in

$$y^3 - 3y - 1 = 0\,. \tag{TRIS}$$

überführt. Nach dem oben bewiesenen Satz gäbe es dann sogar eine rationale Nullstelle, also ein $\frac{a}{b}$ mit teilerfremden ganzen Zahlen a, b, wenn sich ein

Konstruktionsverfahren der gewünschten Art fände, also eine Gleichheit der Form:

$$a^3 - 3ab^2 - b^3 = 0\,. \tag{9.22}$$

Daraus würde aber folgen: jeder Primfaktor von a ist auch ein Primfaktor von b und umgekehrt, entgegen der Annahme, dass a und b teilerfremd sein sollten.

Wie schön !!!

Sei hiernach W der Einheitswürfel. Möchten wir die Streckung x konstruieren, die den Einheitswürfel verdoppelt, also der Bedingung $x^3 = 2$ genügt, so haben wir die Gleichung

$$x^3 - 2 = 0 \tag{9.23}$$

zu lösen. Zu ihr würde im Falle der Lösbarkeit des geometrischen Problems mindestens eine rationale Lösung $\frac{a}{b}$ mit teilerfremden ganzen Zahlen existieren, was der Gleichung

$$a^3 = 2b^3 \tag{9.24}$$

widerspräche. **Nicht minder schön !!!**

Zu den klassischen Problemen der Geometrie zählt auch die Frage, ob sich das regelmäßige 7-eck mit Zirkel und Lineal konstruieren lässt.

Hier gelingt die Antwort erneut dank LANDAU.

9. 5. 3 Proposition. *Das regelmäßige 7-eck lässt sich nicht mittels Zirkel und Lineal konstruieren.*

BEWEIS. Ließe sich das regelmäßige 7-Eck mittels Zirkel und Lineal konstruieren, so ließe sich eine komplexe Zahl konstruieren, deren Potenzen $\zeta^1, ..., \zeta^7$ paarweise verschieden wären und die zudem $\zeta \neq 1$ & $\zeta^7 = 1$ erfüllt. Es gilt aber

$$z^7 - 1 = (z-1) \cdot (z^6 + z^5 + z^4 + z^3 + z^2 + z^1 + 1)\,. \tag{9.25}$$

Daher müsste ζ zu den Nullstellen von

$$p(x) = z^6 + z^5 + z^4 + z^3 + z^2 + z^1 + 1 \tag{9.26}$$

gehören, und es wäre natürlich auch $\zeta + \frac{1}{\zeta}$ konstruierbar (mit Z&L). Wir setzen nun

$$y := z + \frac{1}{z}\,.$$

Dann lässt sich $p(x)$ schreiben als

$$k(y) = y^3 + y^2 - 2y - 1\,, \tag{9.27}$$

man rechne nach, und es wäre $\zeta + \frac{1}{\zeta}$ eine Nullstelle von $k(y)$, die der „Landau-Bedingung" genügt.

Also besäße $k(x)$ auch eine gekürzte rationale Nullstelle $\frac{a}{b}$, mit Widerspruch zur Teilerfremdheit von a und b – man setze $\frac{a}{b}$ ein und erweitere mit b^3. □

9.6 Kubische Gleichungen

Wir betrachten o.B.d.A. das Polynom

$$k(x) = x^3 + bx^2 + cx + d\,. \tag{9.28}$$

Es hat mindestens eine reelle Nullstelle – siehe Übung... zur Analysis – und damit zumindest im Komplexen eine *Zerlegung in Linearfaktoren*

$$k(x) = (x - \alpha) \cdot (x - \beta) \cdot (x - \xi)\,,$$

und erfüllt damit insbesondere für das obige ξ

$$\xi^3 + b\xi^2 + c\xi + d = 0\,. \tag{9.29}$$

Wir bilden nun

$$\eta = \xi + \frac{b}{3}\,.$$

Dann liefert Einsetzen von $\xi = \eta - \frac{b}{3}$ in (9.28), dass η eine Gleichung der Gestalt

$$\eta^3 + p\eta + q = 0 \tag{9.30}$$

mit $p, q \in K$ erfüllt – man beachte, dass sich die quadratischen (η-) Glieder „weg heben".

Ist nun p gleich 0, so sind wir am Ziel. Sonst aber sei ζ eine Nullstelle von $x^2-\eta x-\frac{p}{3}$. Sie ist dann wegen $p \neq 0$ verschieden von 0 und erfüllt demzufolge

$$\eta = \zeta - \frac{p}{3\zeta}\,.$$

Einsetzen der rechten Seite in (9.30) liefert dann für ζ^3 die *quadratische Gleichung*

$$\zeta^3 - \frac{p^3}{27\zeta^3} + q = 0\,.$$

Wir können also zunächst ζ^3 mittels *Wurzelzeichen* über K ausdrücken und damit natürlich auch ζ, was uns dann weiter in die Lage versetzt, auch η und somit schließlich auch ξ durch Wurzelzeichen auszudrücken.

Führt man nun die Berechnung von ζ und damit die aller möglichen Werte von η durch, so gelangt man zu den Formeln von CARDANO **(1501-1576) für die Nullstellen kubischer Gleichungen.**

Kehren wir noch einmal zurück zur *Dreiteilung des Winkels*: Hier waren wir auf die alles entscheidende Gleichung gestoßen:

$$y^3 - 3y - 2\cos\alpha = 0\,. \tag{9.31}$$

Und wir hatten gesehen, dass sich die Lösung dieser Gleichung nicht mit Zirkel und Lineal konstruieren lässt.

Das bedeutet: ausgehend vom Ursprung O und zwei Punkten A und B auf dem Einheitskreis vermögen wir nicht in jedem Falle über Kreise und Geraden jene Punkte zu erreichen, die auf derjenigen Geraden liegen, die den Winkel AOB dreiteilen.

Dies sieht anders aus, wenn wir neben den Geraden und den Kreisen noch die *Normal-Parabel* $y = x^2$ unter unsere Wege mit aufnehmen.

Schon 1637 hat Descartes in seiner GEOMETRIE Probleme der Alten mit seiner analytischen Methode behandelt. Unter diesen Problemen findet sich auch die Dreiteilung des Winkels, für die er eine zeichnerische Lösung unter Heranziehung der Normalparabel gab.

Beginnen wir mit dem Kreis in allgemeiner Lage und der *Normalparabel* , also algebraisch mit dem Gleichungspaar

$$(x-a)^2+(y-b)^2=r^2 \tag{9.32}$$

$$y=x^2 \tag{9.33}$$

Hier liefert Einsetzen von (9.33) in (9.32)

$$x^2-2ax+a^2+x^4-2bx^2+b^2=R^2$$

bzw.

$$x^4-(1-2b)x^2-2ax+a^2+b^2-R^2=0\,, \tag{9.34}$$

also eine Gleichung vom Typ

$$x^4+px^2+qx+r=0 \tag{9.35}$$

mit

$$p=1-2b, \qquad q=-2a, \qquad r=a^2+^2-R^2\,.$$

Das bedeutet: mit (9.35) sind die Werte a, b, R bekannt, und damit dann auch der Kreis (9.32) . Somit kennen wir die x-Werte der Schnittpunkte von Kreis und Parabel, sie sind die Wurzeln der Gleichung (9.35).

Bezogen auf die Dreiteilung des Winkels bedeutet dies: Multiplizieren wir (9.31) mit y, so erhalten wir

$$y^4-3\cdot y^2-2\cos\alpha\cdot y=0 \tag{9.36}$$

und damit eine Gleichung vom Typ (9.35), deren Nullstellen – und hierunter $2\cos\beta$ mit $3\beta=\alpha$ – sich zeichnerisch mittels Normalparabel und Zirkel ermitteln lassen.

In anderen Worten: Zu vorgegebenem $2\cos\alpha$ finden wir $2\cos\beta$ mit $\beta=\alpha/3$ und damit zu vorgegebenem Winkel α den Winkel $\alpha/3$ als Konstruktionsergebnis mittels Zirkel und Normalparabel.

AUFGABE: Man „verdoppele" den Einheitswürfel mittels Zirkel und Normalparabel.

Kapitel 10

Der Satz von Wedderburn*)

Ziel dieses Paragraphen ist der Beweis des Satzes von Wedderburn, der besagt, dass jeder endliche Schiefkörper kommutativ ist.

10. 0. 1 Definition. Unter einem Schiefkörper versteht man einen Ring $\mathfrak{S} = (S, +, \cdot)$, in dem für jedes $a \neq 0$ alle Gleichungsforderungen

$$a \cdot x \doteq b \quad \text{und} \quad y \cdot a \doteq b$$

erfüllbar sind.

Der bekannteste Schiefkörper ist der Schiefkörper der *Quaternionen,* vgl. Elemente der Mathematik. Ziel dieses Abschnitts ist es zu zeigen, dass jeder endliche Schiefkörper kommutativ ist.

Den Weg dorthin skizzieren wir durch Aufgaben, die dem Leser zuzumuten sein sollten, deren Lösungen sich aber natürlich auch in jedem Buch über klassische Algebra finden.

10. 0. 2 Aufgabe. *Man zeige: Es sei $\mathfrak{S}$ ein Oberschiefkörper zu dem Schiefkörper $\mathfrak{K}$. Dann stiftet die Festsetzung*

$$a \propto A :\Longleftrightarrow a = \kappa_1 a_1 + \kappa_2 a_2 + ... + \kappa_n a_n \quad (\kappa_\nu \in K)$$

eine lineare Abhängigkeitsrelation, vgl. Lin Al.

10. 0. 3 Aufgabe. *Man zeige: Ist $\mathfrak{S}$ ein endlicher Schiefkörper vom Grade n – im obigen Sinne – über dem Schiefkörper $\mathfrak{E}$ von der Mächtigkeit q. Dann hat $\mathfrak{S}$ q^n viele Elemente.*

10. 0. 4 Aufgabe. *Man zeige: Es sei $\mathfrak{S}$ ein Schiefkörper. Dann ist die Menge $Z \subset S$ aller derjenigen Elemente $z \in S$, die mit jedem $s \in S$ vertauschbar sind, operativ abgeschlossen.*

10. 0. 5 Aufgabe. *Ist $\mathfrak{U}$ eine Untergruppe der Gruppe $\mathfrak{G}$ und $g \in G$, so bildet gUg^{-1} eine zu $\mathfrak{U}$ isomorphe Untergruppe von $\mathfrak{G}$.*

10. 0. 6 Definition. Zwei Untergruppen $\mathfrak{U}, \mathfrak{V}$ einer Gruppe $\mathfrak{G}$ heißen konjugiert, wenn ein $g \in G$ mit $V = gUg^{-1}$ existiert. Zwei Elemente a, b aus G heißen konjugiert, wenn ein $g \in G$ mit $b = gag^{-1}$ existiert.

Man bestätigt leicht, daß in beiden Fällen Äquivalenzrelationen definiert werden. Die Menge aller Untergruppen von $\mathfrak{G}$ zerfällt also in Klassen konjugierter, paarweise zueinander isomorpher Untergruppen, und die Menge aller Elemente von G zerfällt in Klassen paarweise konjugierter Elemente.

10. 0. 7 Definition. Es sei g ein Element der Gruppe $\mathfrak{G}$ und M die Menge aller $m \in G$ mit $mgm^{-1} = g$ oder, gleichwertig, $mg = gm$. Dann heißt M der *Normalisator* von $g \in G$.

10. 0. 8 Proposition. *Man zeige: Es sei $\mathfrak{G}$ eine Gruppe und M der Normalisator von $g \in G$. Dann ist M operativ abgeschlossen, und die Anzahl der Konjugierten von g ist gleich dem Index von $\mathfrak{M}$ in $\mathfrak{G}$, also gleich $|G| : |M|$.*

Dies bedeutet insbesondere: Ist G endlich, so ist die Anzahl der Konjugierten von $g \in G$ ein Teiler der Ordnung $|\,G\,|$ von $\mathfrak{G}$.

BEWEIS. Wir erhalten geradeaus, dass M abgeschlossen ist bezüglich Multiplikation und Inversenbildung, also eine Untergruppe von $\mathfrak{G}$ „trägt".

Liefern nun $x,\ y \in G$ dasselbe Konjugierte von g, ist also $xgx^{-1} = ygy^{-1}$, so folgt $y^{-1}xg = gy^{-1}x$, also $y^{-1}x \in M$ bzw. $x \in yM$, d.h. so liegen x und y in derselben Linksnebenklasse von M.

Und liegen andererseits zwei Elemente hm_1 und hm_2 in derselben Linksnebenklasse hM so liefern sie dasselbe Konjugierte hgh^{-1} von g, wegen

$$(hm_1)g(hm_1)^{-1} = hm_1gm_1^{-1}h^{-1} = hgm_1m_1^{-1}h^{-1} = hgh^{-1}.$$

Damit ist gezeigt: die Anzahl der Konjugierten von g ist gleich dem Index von $\mathfrak{M}$ in $\mathfrak{G}$. □

In den Beweis des Satzes von WEDDERBURN wird die Theorie der Kreisteilung wesentlich eingehen.

Sei also m eine natürliche Zahl. Wir betrachten das Polynom $x^m - 1$. Es zerfällt in $\mathfrak{C}[x]$ in Linearfaktoren:

$$x^m - 1 = (x - \zeta_1)(x - \zeta_2)\dots(x - \zeta_m).$$

Dabei sind die komplexen Zahlen ζ_ν $(1 \leq \nu \leq m)$ die sämtlichen m-ten Einheitswurzeln und bilden eine zyklische Gruppe, o.B.d.A. erzeugt von $\zeta := \zeta_1$ mit $\zeta_\nu = \zeta^\nu$ und damit exakt auch von allen ζ^ν mit $\nu \perp n$ bzw. $(\nu, n) = 1$. Deren Zahl wird nach Euler mit $\varphi(n)$ bezeichnet.

Unter dem *m-ten Kreisteilungspolynom* versteht man das Polynom

$$\Phi_m(x) = \prod_{1 \leq \nu \leq m}^{(\nu,m)=1} (x - \zeta_\nu)\,, \tag{10.1}$$

10. 0. 9 Aufgabe. *Man zeige*

$$x^m - 1 = \prod_{n|m} \phi_n(x)\,. \tag{10.2}$$

10. 0. 10 Aufgabe. *Man beweise induktiv unter Einsatz der Division mit Rest*

$$\Phi_m(x) \in \mathfrak{Z}[x]. \tag{10.3}$$

Hiernach lässt sich verifizieren

10. 0. 11 Theorem. Der Satz von Wedderburn: *Jeder endliche Schiefkörper ist kommutativ.*

BEWEIS. Wir führen den Beweis nach ERNST WITT.

Es sei $\mathfrak{S}$ ein endlicher Schiefkörper und $\mathfrak{Z}$ das Zentrum von $\mathfrak{S}$.

Es ist zu zeigen $Z = S$. Wir setzen

$$\mathfrak{S} : \mathfrak{Z} =: n$$

und $|\,Z\,| =: q$, dann gilt $q \geq 2$ und $|\,S\,| = q^n$.

Nun betrachten wir für ein festes $s \in S$ den Normalisator $N(s)$ von s. Man bestätigt leicht, daß $N(s) \supseteq Z$ bezüglich $+$ und $\cdot$ die Schiefkörperbedingungen erfüllt. Also ist $|\,N(s)\,| = q^d$ eine Potenz von $|\,Z\,| = q$. Da ferner $S \supseteq N(s)$ erfüllt ist, also auch $|\,S\,| = q^n$ eine Potenz von $|\,N(s)\,| = q^d$ ist, folgt zusätzlich $d \,|\, n$.

Wir zerlegen nun die multiplikative Gruppe $\mathfrak{S}_0$ von $\mathfrak{S}$ in Klassen konjugierter Gruppenelemente und zählen die Elemente der einzelnen Klassen ab. Insgesamt hat $\mathfrak{S}$ die Ordnung $|\,S_0\,| = q^n - 1$. Nach 10.0.8 ist die Anzahl der Konjugierten eines $s \in S_0$ gleich dem Index des Normalisators $N_0(s) = \{x \in N(s) : x \neq 0\}$, also eine Zahl der Gestalt

$$\frac{q^n - 1}{q^d - 1} \quad \text{mit} \quad d \,|\, n\,. \tag{10.4}$$

Wir werden zeigen, daß die multiplikativen Gruppen von $\mathfrak{S}$ und $\mathfrak{Z}$ übereinstimmen, also $S_0 = Z_0$ erfüllt ist.

Angenommen, das wäre nicht der Fall, dann wäre der Grad von $\mathfrak{S}$ über $\mathfrak{Z}$ größer als 1. Außerdem gäbe es ein $s \in S_0$, dessen Normalisator $N_0(s)$ von S_0 verschieden wäre, denn jedes $s \in S_0$, das nicht in Z_0 liegt, würde dies erfüllen. Die Klasse der Konjugierten, zu der dieses Element s gehörte, hätte

$$\frac{q^n - 1}{q^d - 1}$$

viele Elemente, mit echtem Teiler d von n. Es könnte sein, daß es mehrere solcher Klassen gäbe. Jedes der $q - 1$ Elemente des Zentrums Z_0 von S_0 aber bildet eine Klasse für sich.

Somit ergäbe sich durch Abzählen eine Gleichung der Form

$$q^n - 1 = (q - 1) + \sum \frac{q^n - 1}{q^d - 1}, \tag{10.5}$$

in der n und q von 1 verschiedene natürliche Zahlen sind und rechts über einen gewissen echten Teiler d von n summiert wird.

Nun ist aber

$$x^n - 1 = \prod_{m|n} \Phi_m(x)\,.$$

Für jeden echten Teiler d von n folgt dementsprechend

$$x^d - 1 = \prod_{m|d} \Phi_m(x)$$

und damit auch

$$\frac{x^n - 1}{x^d - 1} = \Phi_n(x) g(x) \tag{10.6}$$

in $\mathfrak{Z}[x]$.

Ersetzt man nun in (10.6) x durch q und vergleicht dann (8.6) mit (10.5), so erkennt man, daß in (10.5) sowohl $q^n - 1$ als auch die Summe rechts durch $\Phi_n(q)$ teilbar sind. Also müsste auch $q - 1$ den Teiler $\Phi_n(q)$ haben. Das aber führt zum Widerspruch!

DENN: Für $n > 1$ ist $|\,\Phi_n(q)\,| > q - 1$, man beachte die Zerlegung

$$\Phi_n(x) = \prod (x - \zeta_\nu)$$

in $\mathfrak{C}[x]$, worin die ζ_ν gerade die $\varphi(n)$ primitiven n-ten Einheitswurzeln durchlaufen. Für $n > 1$ ist keine von ihnen gleich 1, was $|\,q - \zeta_\nu\,| > q - 1 \geq 1$ impliziert und damit

$$|\,\Phi_n(q)\,| = \prod |\,q - \zeta_\nu\,| > q - 1.$$

Damit ist der Satz bewiesen. □

Kapitel 11

Hauptidealringe*)

11.1 Hauptidealringe

Die nachfolgenden Resultate basieren auf den Arbeiten [1], [2], [3].

Ist $\mathfrak{R}$ ein kommutativer Ring mit 1, so heißt eine Teilmenge $\mathfrak{i}$ ein Ideal, wenn sie mit je endlich vielen Elementen $a_1, ..., a_n$ auch alle Linearkombinationen $\sum_1^n x_i a_i$ enthält.

11. 1. 1 Aufgabe. *Man zeige: mit jeder Familie* $\mathfrak{a}_i$ *ist auch* $\bigcap \mathfrak{a}_i \, (i \in I)$ *ein Ideal.*

11. 1. 2 Aufgabe. *Man zeige: Mit jeder aufsteigenden Folge*

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq .....\mathfrak{a}_n \subseteq .....$$

von Idealen $\mathfrak{a}_i$ *ist auch deren Vereinigung* $\bigcup \mathfrak{a}_i =: \sum_1^\infty \mathfrak{a}_i \;\; (i \in I)$ *ein Ideal.*

11. 1. 3 Aufgabe. *Man zeige: Jeder Gauß'sche Ring ist ein Hauptidealring.*

11. 1. 4 Aufgabe. *Man zeige: jedes* $\mathfrak{Z}_m$ *ist ein Hauptidealring.*

11. 1. 5 Aufgabe. *Man zeige* $((A)(B)) = (AB)$.

11. 1. 6 Definition. Ein Ring heißt ein Hauptidealring, wenn jedes Ideal 1-erzeugt ist, also vom Typus (a).

11. 1. 7 Aufgabe. *Sei $\mathfrak{R}$ ein Hauptidealring. Man zeige, dass jede Ideal-Kette*

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq ...(a_n) \subseteq ....$$

nach endlich vielen Schritten abbricht.

Im folgenden sei $\mathfrak{R}$ ein kommutativer Hauptidealring mit 1[1)]

Sind dann a und b zwei Elemente aus R und gilt

$$(a, b) = (d) \text{ und } (a) \cap (b) = (v)$$

so ist d ein GGT und v ein KGV zu a und b.

Als Standard-Modell habe der Leser hier etwa einen $\mathfrak{Z}_m$ vor Augen. Als homomorphes Bild eines Hauptidealbereiches ist dies ein geeignetes Modell, allerdings ein endliches.

Um auch einen unendliches Modell zu präsentieren, geben wir noch das direkte Produkt $\mathfrak{Z}^n$ von $\mathfrak{Z}$ hinzu. Natürlich ist auch dies ein Hauptidealring, aber selbstverständlich kein Hauptidealbereich.

Es dürfte sich „lohnen" die einzelnen nachfolgenden Herleitungen in diesen Strukturen nachzuspielen. Dabei beachte man:

11. 1. 8 Lemma. *In $\mathfrak{Z}_m$ ist jedes Element Einsteiler oder Nullteiler und zwar gilt $\overline{a} \mid \overline{1}$ genau dann, wenn $(a, m) = 1$ erfüllt ist.*

BEWEIS. Gilt $(a, m) = (1)$, so ist $ax + my = 1 \ (\exists\, x, y)$, also $ax \equiv 1 \ (m)$.
Und ist $(a, m) = (d) \neq (1)$, so gilt $d \cdot \dfrac{m}{d} = m$ mit $\dfrac{m}{d} \neq m$. □

Wir erinnern an die eingeführten Teilbarkeitsbeziehungen und Lemmata. Zu den bereits definierten Begriffen nehmen wir hier noch hinzu:

11. 1. 9 Definition. Sei $\mathfrak{S}$ ein kommutatives Monoid. Dann erklären wir:

$$\begin{array}{llll} p \in S & \text{heiße} & \textit{halbprim}, \text{ wenn gilt:} & p \sim ab \implies p \mid a \vee p \mid b. \\ p \in S & \text{heiße} & \textit{vollprim}, \text{ wenn gilt:} & p^n \mid ab \implies p^n \mid a \vee p \mid b. \end{array}$$

Halbprim wären in $\mathfrak{Z}^n$ z. B. die Elemente vom Typ $(a_1, \ldots, a_n)$ mit genau einer 1 und lauter Nullen sonst.

[1)] Die Struktur der ZPE-Ringe wird in der Lecture Note Ringe vom Feinsten" abgehandelt.

11. 1. 10 Lemma. *Sei $\mathfrak{S}$ ein kommutatives Monoid. Dann ist $p \in R$ halbprim gdw. $a\|p \;\&\; b\|p \Longrightarrow ab\|p$.*

Denn: Ist p halbprim, so folgt

$$\begin{aligned} a\|p \;\&\; b\|p &\implies p = ax = by = asp = btp \\ &\implies p = asbtp \\ &\implies ab \mid p \;\&\; p \nmid ab \end{aligned}$$

und ist für alle a, b mit $a\|p \;\&\; b\|p$ auch $ab\|p$ erfüllt, so folgt

$$p \sim uv \implies p \mid u \vee p \mid v\,,$$

da p sonst nicht äquivalent zu u oder v wäre, also auch nicht zu uv. □

Ziel dieses Abschnitts ist eine Untersuchung der kommutativen Hauptidealringe mit 1. Hierzu schicken wir einige Hilfssätze voraus:

11. 1. 11 Lemma. *Sei $\mathfrak{R}$ kommutativ mit 1, ansonsten aber beliebig. Dann gilt:*

$$a^2 \cdot x = a \;\&\; au = b \;\&\; bv = a \Longrightarrow a \equiv b\,. \tag{11.1}$$

Denn: $ax - 1 + axu := c \Longrightarrow ac = b \;\&\; c \mid b \mid a \rightsquigarrow c \mid 1$. □

Das letzte Lemma besagt also in anderer Formulierung

$$a^2 \mid a \mid b \implies a \equiv b\,.$$

11. 1. 12 Korollar. $n > m \;\&\; a^n \mid a^m \Longrightarrow a^m \equiv a^n$.

11. 1. 13 Lemma. *Ist $\mathfrak{R}$ sogar ein endlicher kommutativer Ring mit 1, so gilt (stets) $a \sim b \Longrightarrow a \equiv b$.*

Denn: Sei $ax = b \;\&\; by = a$. Dann folgt $a(xy) = a$, also $a(xy)^n x = b$, und es ist $x^r \equiv x^{r+1} (\exists r)$. Also folgt $b = ax = a(xy)^r \varepsilon = a\varepsilon$. □

11. 1. 14 Lemma. *Sei $\mathfrak{R}$ kommutativ mit 1, ansonsten aber beliebig. Dann gilt: Ist a nicht halbprim, so lässt sich a in echte Teiler b, c zerlegen.*

BEWEIS. Nach Voraussetzung existiert ein bc mit $a \sim bc$, aber $b\|a \;\&\; c\|a$. Sei nun $a = bcd$. Ist dann $bd\|a$ oder $cd\|a$, so sind wir am Ziel.

Sonst aber gilt $a \sim cd$ und $a \sim bd$, etwa

also
$$au = cd \quad \text{und} \quad av = bd\,,$$
$$a = bcd = bau = cav \;\rightsquigarrow\; a = cbauv = bc.a.uv \rightsquigarrow a^2 \sim a\,.$$

Somit ist $a \equiv bc$, etwa $a = b.c\varepsilon$ mit $b\big\|a,\ c\varepsilon\big\|a$. □

11. 1. 15 Korollar. *Sei $\mathfrak{R}$ kommutativ mit 1, ansonsten aber beliebig. Dann gilt:*
$$p \text{ halbprim} \iff p = ab \Rightarrow p \,\big|\, a \vee p \,\big|\, b\,.$$

11. 1. 16 Lemma. *Sei $\mathfrak{R}$ kommutativ mit 1, ansonsten aber beliebig. Dann ist jedes irreduzible Halbprimelement ein Nullteiler.*

Denn: $1\big\|a\big\|p \Longrightarrow p = ay \Longrightarrow p = apx \Longrightarrow p(1-ax) = 0$ mit $ax - 1 \neq 0$, da sonst $a \,\big|\, 1$ erfüllt wäre. □

11. 1. 17 Lemma. *Sei $\mathfrak{R}$ kommutativ mit 1, ansonsten aber beliebig. Dann gilt: Ist $a\big\|p$ und p halbprim, so ist a kürzbar.*

Denn: $a\big\|p \Longrightarrow p = pax$. Ist nun $ad = 0$, so folgt $p \sim ap = a(p+d) \rightsquigarrow p \,\big|\, p + d \rightsquigarrow p \,\big|\, d$, etwa $d = py$, und damit $d = py = axpy = axd = 0$. □

Aus dem letzten Lemma folgt fast unmittelbar

11. 1. 18 Proposition. *Sei $\mathfrak{R}$ ein Hauptidealring. Dann zerfällt jedes a aus R in Halbprimelemente.*

Denn: Würde ein a nicht zerfallen, so gäbe es unter den Hauptidealen (x) deren Erzeuger x nicht zerfällt, ein maximales. Dann gibt es aber keine Zerlegung $x = uv$ mit $(x) = (u)(v)$ und $(u) \supset (x) \subset (v)$. Also ist x nach Lemma 11.1.14 halbprim. □

11. 1. 19 Proposition. *Sei $\mathfrak{R}$ ein Hauptidealring. Dann ist jedes halbprime p sogar prim.*

Denn:
$$\begin{aligned} p \,\big|\, ab &\Longrightarrow (p) \supseteq (p,a)(p,b) = (u)(v) \\ &\Longrightarrow (p) = (u) \vee (p) = (v) \\ &\Longrightarrow p \,\big|\, u \vee p \,\big|\, v\,. \end{aligned}$$
□

11. 1. 20 Proposition. *Sei $\mathfrak{R}$ ein Hauptidealring. Dann ist jedes halbprime p sogar vollprim.*

DENN:

$$\begin{array}{rcl} p^n \,|\, ab & \& & p \nmid b \\ & \Rightarrow & \\ (p^n) & \supseteq & (p^n \cdot p^n, p^n \cdot b, a \cdot p^n, ab) \\ & = & (p^n, a)(p^n, b) \\ & \supseteq & (p^n, a)(p, b)^n \\ & = & (p^n, a)(c)^n \;\; (\exists c \| p) \\ & = & (p^n, a) \\ & \rightsquigarrow & \\ p^n & | & a\,. \end{array}$$

□

11. 1. 21 Korollar. *Sei $\mathfrak{R}$ kommutativ mit 1 und zudem endlich. Dann ist jedes halbprime p irreduzibel, denn dies folgt aus der Gruppeneigenschaft der Teiler von p.*

11. 1. 22 Lemma. *Sei $\mathfrak{R}$ kommutativ mit 1, ansonsten aber beliebig. Dann gilt: Sind p, q prim, so folgt $p \,|\, q \vee q \,|\, p \vee (p, q) = (1)$.*

DENN: Sei $p \nmid q \;\&\; q \nmid p$ und $d \,|\, p, q$. Dann folgt $d \| p, q$ und damit

$$\begin{array}{rcl} p = pdx & \Longrightarrow & p\,(1 - dx) = 0 \;\; (\exists x) \\ & \Longrightarrow & q \,|\, 1 - dx \\ & \Longrightarrow & qy + dx = 1 \\ & \Longrightarrow & d \,|\, 1\,. \end{array}$$

□

11. 1. 23 Lemma. *Ist $\mathfrak{R}$ ein Hauptidealring, so gilt*

$$1 \| a \| p \;\&\; p \;\; prim \;\; \Longrightarrow p^2 \,|\, p\,.$$

DENN: Wäre etwa $1 \| a \| p$ mit $p = pax$ und $p^2 \nmid p$, so erhielten wir

$$\begin{array}{rcl} p = pax & \rightsquigarrow & p\,(1 - ax) = 0 \\ & \rightsquigarrow & p \,|\, 1 - ax \\ & \rightsquigarrow & ax = 1 + py \\ & \rightsquigarrow & a \,|\, 1\,. \end{array}$$

mit Widerspruch zu $a \nmid 1$. □

11. 1. 24 Lemma. *Ist $\mathfrak{R}$ ein Hauptidealring, so gilt*

$$a \sim b \;\; \Longrightarrow \;\; a \equiv b\,.$$

BEWEIS. Sind p und q prim mit $p \sim q$, so ist nichts zu zeigen, da im Falle $p^2 \nmid p$ alle echten Teiler von p bzw. q Einsteiler sind.

Seien nun p^e und q^f zwei Primfaktorpotenzen mit $p^e \sim q^f$. Dann gilt etwa $q = p\varepsilon$ mit $\varepsilon \mid 1$ und wir haben im Falle $e = f$ unmittelbar $p^e \equiv p^f$ und im Falle $e < f \vee f < e$ mittelbar $p^e \equiv p^f$, da dann $(p^e)^2 \mid p^c$ erfüllt ist. □

Hiernach können wir 11.1.18 verschärfen zu

11. 1. 25 Proposition. *Sei $\mathfrak{R}$ ein Hauptidealring. Dann zerfällt jedes a aus R in Vollprimelemente und wir dürfen jeweils ausgehen von einer Zerlegung*

$$a = \varepsilon \cdot \prod_1^s p_i^{e_i} \quad mit \quad i \neq j \Longrightarrow p_i \nmid p_j \,.$$

Eine direkte Zerlegung

Zur weiteren Entwicklung geben wir als nächstes

11. 1. 26 Definition. Ein kommutativer Ring mit 1 heiße *speziell* gdw. es ein Primelement gibt, dessen (p^n) alle Ideale aus $\mathfrak{R}$ ausschöpfen –

und zeigen

11. 1. 27 Proposition. *Sei $\mathfrak{R}$ ein Hauptidealring. Dann lässt sich $\mathfrak{R}$ direkt zerlegen in eine endliche Summe von ZPE-Integritätsbereichen und speziellen Ringen.*

BEWEIS. Wir dürfen ausgehen von $0 = \prod_1^n p_i^{f_i}$ mit $p_i^{f_i} \cdot p_i = p_i^{f_i}$ und $1 \leq i \leq n$. Denn es ist

$$\begin{aligned} p_i^{f_i} \cdot p_i \mid p_i^{f_i} \quad &\rightsquigarrow \quad p_i^{f_i} \ (p_i\varepsilon) = p_i^{f_i} \\ &\rightsquigarrow \quad (p_i\varepsilon)^{f_i} \cdot (p_i\varepsilon) = (p_i\varepsilon)^{f_i} \,, \end{aligned}$$

so dass wir gegebenenfalls nur p_i durch $p_i\varepsilon$ zu ersetzen haben.

Wir definieren nun

$$e_j =: \prod p_i^{f_i} \quad (i \neq j) \,.$$

Dann ist $e_1 + \ldots + e_n$ eine *orthogonale Summe*, insbesondere also

$$e_1 + \ldots + e_n = 1\,.$$

Denn es ist $e_1+\ldots+e_n$ idempotent und ist p irgendein Primteiler von $e_1+\ldots+e_n$, so teilt p nach Voraussetzung mindestens zwei teilerfremde Primelemente, also auch 1. Somit ist $\mathfrak{R}$ direkte Summe der Unterringe $\mathfrak{R}e_s$, also

$$\mathfrak{R} = \mathfrak{R}e_1 \oplus \ldots \oplus \mathfrak{R}e_s\,.$$

Zu zeigen bleibt, dass jedes $\mathfrak{R}e_i$ speziell oder integer ist. Hierzu unterscheiden wir die Fälle $p_i = p_i^2$ und $p_i \neq p_i^2$.

(i) Sei $p_i = p_i^2$ und $ae_i \cdot be_i = 0$. Dann folgt $p_i \,\big|\, ab$ und damit $p_i \,\big|\, a \vee p_i \,\big|\, b\,$, also $ae_i = 0$ oder $be_i = 0\,$, also ist $\mathfrak{R}e_i$ nullteilerfrei und damit ein Integritätsbereich.

(ii) Sei $p_i \neq p_i^2$. Dann ist jeder echte Teiler von p_i ein Einsteiler, und es liegen in $\mathfrak{R}e_i$ nur Elemente vom Typ be_i mit $b \sim p_i^t$.

Denn: Mit $p := p_i,\ n = f_i,\ e := e_i$ haben wir im Fall $p \nmid a$ wegen der Irreduzibilität von p zunächst: $(a, p) = (1)$ und folglich

$$(a, p^n) = (1) \rightsquigarrow (a \cdot e, p^n \cdot e) = (ae) \rightsquigarrow (ae) = (e) \rightsquigarrow ae \equiv e$$

und damit weiter im Falle $p^m \,\big|\, de \;\&\; p^{m+1} \nmid de$

$$de \equiv p^m e \cdot x \;\&\; (p^n, x) = (1) \rightsquigarrow ex \equiv e\,.$$

Damit sind wir am Ziel. □

Beispiel: Sei $\mathfrak{R}$ der Restklassenring *modulo* 60. „Eine" Primfaktorzerlegung von $\overline{0}$ ist in diesem Falle gleich $\overline{2}^2 \cdot \overline{3}^1 \cdot \overline{5}^1$.

Wir ersetzen nun die Primfaktorpotenzen im Sinne unseres Satzes.

Es gilt $(\overline{2}^2)^2 \,\big|\, \overline{2}^2$, genauer $(\overline{2}^2)^2 \cdot \overline{4} = \overline{2}^2$, also $\overline{2}^2 \cdot (\overline{16} - \overline{1} + \overline{16} \cdot \overline{2}) = \overline{2}^3$ und damit $\overline{2}^2 \cdot \left((\overline{2} \cdot \overline{47}^{-1}\right) = \overline{2}^2$, also wegen $\overline{47}^{-1} = \overline{23}$ dann $\left(\overline{2} \cdot \overline{23}\right)^2 \cdot \left(\overline{2} \cdot \overline{23}\right) = \left(\overline{2} \cdot \overline{23}\right)^2 = \overline{46}^2$. mit $\overline{46}^2 = \left(\overline{46}^2\right)^2$.

Daher ist $\overline{2}$ zu ersetzen durch $\overline{46}^2$.

Entsprechend sind die Faktoren $\overline{3}$ bzw. $\overline{5}$ zu ersetzen durch die Idempotenten $\overline{21}$ bzw. $\overline{25}$.

Damit gilt in diesem Beispiel

$$\begin{aligned} e_1 &= \overline{21}\cdot\overline{25} = \overline{45}\ , \\ e_2 &= \overline{16}\cdot\overline{25} = \overline{40}\ , \\ e_3 &= \overline{16}\cdot\overline{21} = \overline{36}\ , \end{aligned}$$

Zur transzendenten Erweiterung

Wir fragen nun nach dem Zusammenhang zwischen Hauptidealringen $\mathfrak{R}$, und ihren transzendenten Erweiterungen. Hier gilt:

11. 1. 28 Theorem. *Sei $\mathfrak{R}$ ein Hauptidealring. Dann ist $\mathfrak{R}[x]$ genau dann ein ZPE-Ring, d. h. Ein Ring, in dem jedes Element in Primelemente zerfällt, wenn $\mathfrak{R}$ der Bedingung $a^2 = 0 \Longrightarrow a = 0$ genügt.*

BEWEIS. (a) Gilt die Bedingung des Satzes, so ist $\mathfrak{R}$ direkte Summe von Hauptidealbereichen, und es pflanzt sich die ZPE-Eigenschaft von $\mathfrak{R}$ auf $\mathfrak{R}[x]$ fort nach C. F. Gauss, siehe oben.

(b) Sei hiernach $\mathfrak{R}[x]$ ein ZPE-Ring. Dann besitzt jedes $a \in R$ eine Zerlegung $a = p_1 \dots p_m$ mit primen p_i $(1 \le i \le s)$.

Beachte nun:

$$\begin{aligned} a, b \in R &\implies \Big(a \,\big|_{\,R[x]}\, b \Longrightarrow a \,\big|_{\,R}\, b\Big) \\ \text{und:}\quad a, b \in R &\implies \big(a \ \sim_R \ b \Longrightarrow a \equiv b\big)\,, \end{aligned}$$

wobei die zweite Zeile aus

$$(a_0 + a_1 x + \dots + a_n x^n) \,\Big|\, 1 \implies a_0 \,|\, 1\,.$$

resultiert. Ist dann p prim in $\mathfrak{R}$ und ist

$$p = \prod_1^n p_i(x)$$

die Primfaktorzerlegung von p in $\mathfrak{R}[x]$, so folgt für ein geeignetes j $p \,|\, p_j(x)$ und damit

$$\begin{aligned} p \,|\, ab &\implies p_j(x) \,|\, a \ \vee\ p_j(x) \,|\, b \\ &\implies p_{j_0} \,|\, a \ \vee\ p_{j_0} \,|\, b \\ &\implies p \,|\, a \ \vee\ p \,|\, b\,. \end{aligned}$$

Es ist aber jedes Primelement aus $\mathfrak{R}$ auch prim in $\mathfrak{R}[x]$, denn dies folgt aus den Regeln für das Rechnen mit Polynomen.

(Gäbe es ein erstes a_i in $f(x)$, etwa a_k und ein erstes b_j in $g(x)$, etwa b_ℓ mit $p \nmid a_k$ & $p \nmid b_\ell$, so wäre dies ein Widerspruch zu $p \mid a_k b_\ell$.)

Somit ist die Primfaktorzerlegung von 0 in $\mathfrak{R}$ auch eine Primfaktorzerlegung der 0 in $\mathfrak{R}[x]$.

Wäre nun $a^2 = 0 \neq a$, so gäbe es ein $p, n, e := p_i, n_i, e_i$ mit $p^2 \nmid p$, das dann irreduzibel sein müsste . Dann wäre aber in $\mathfrak{R}e[x]$ jeder Primfaktor von xe ein echter Teiler von pe wegen $(pe)^n = 0$ einerseits und der Kürzbarkeit von xe in $\mathfrak{R}e[x]$ andererseits, man beachte, dass pe ein Nullteiler ist. Und hieraus würde der Widerspruch resultieren $xe \mid e \rightsquigarrow x \,|_R\, e$. □

HINWEIS. Im gegebenen Fall hätten wir auch zeigen können, dass schon xe irreduzibel ist in $\mathfrak{R}e[x]$ – wieso ? –, doch kann x in einem beliebigen $\mathfrak{R}[x]$ sehr wohl zerlegbar sein – warum?

AUSBLICK: Anders als bei Integritätsbereichen können wir unser Verfahren hier nicht fortsetzen, da wir ja ausgegangen sind von einem Hauptidealring. Es gilt aber auch hier:

Nennt man einen Ring einen *Z-Ring,* wenn jedes a äquivalent ist zu einem Produkt von Halbprimelementen und zudem je zwei unverkürzbare Produkte von Halbrimelementen bis auf Äquivalenz die gleichen Faktoren aufweisen, so gilt auch jetzt noch analog zu unseren Herleitungen:

11. 1. 29 Theorem. *Jeder Z-Ring, insbesondere also jeder Ring, dessen Elemente in Primelemente zerfallen, ist direktes Produkt von Z-Bereichen und speziellen Ringen, und es ist genau dann mit $\mathfrak{R}$ auch $\mathfrak{R}[x]$ ein Z-Ring, wenn $\mathfrak{R}$ kein a mit $a^2 = 0$ besitzt.*

Kapitel 12

Übungen

Übungen zur Algebra **WS 95/96** **Blatt 1**

Jörg Binder Abgabetermin: Mo. 30. 10. 1995, 13^{30} Uhr

Aufgabe 1. Es sei $\langle \mathbf{Z}, +, \cdot \rangle$ der Ring der ganzen Zahlen. Definiere für $a, b \in \mathbf{Z}$

$$\begin{aligned} a \oplus b &:= a + b - 1 \\ a \odot b &:= a + b - ab \end{aligned}$$

Zeigen Sie: Dann ist $\langle \mathbf{Z}, \oplus, \odot \rangle$ ein Ring mit Eins. Hat dieser Ring Nullteiler? Welche Elemente sind invertierbar?

Aufgabe 2. Sei $\langle R, +, \cdot \rangle$ ein Ring mit Eins und $x, y \in R$ invertierbar. Zeigen Sie:

(i) Dann ist auch $x \cdot y$ invertierbar und $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.
(ii) Es gilt $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$ genau dann, wenn $x \cdot y = y \cdot x$.

Aufgabe 3. Es sei $\langle R, +, \cdot \rangle$ ein Ring. Wir definieren eine Funktion $\mathbf{Z} \times R \to R$, $(n, x) \mapsto nx$, genannt das *n-fache von* x, wie folgt: Für $n \in \mathbf{N}$ definieren wir rekursiv

$$\begin{aligned} 0x &:= 0 \\ (n+1)x &:= nx + x. \end{aligned}$$

Ist $n \in \mathbf{Z} \setminus \mathbf{N}$, so ist $-n \in \mathbf{N}$ und wir reduzieren auf den ersten Fall: $nx := (-n)(-x)$. Zeigen Sie: Für alle $m, n \in \mathbf{Z}, x, y \in R$ gilt

(i) $1x = x$
(ii) $(m+n)x = (mx) + (nx)$
(iii) $(mn)x = m(nx)$
(iv) $n(x+y) = (nx) + (ny)$
(v) $n(x \cdot y) = (nx) \cdot y = x \cdot (ny)$
(vi) $(nm)(x \cdot y) = (nx) \cdot (my)$

Hat $\langle R, +, \cdot \rangle$ zusätzlich eine Eins 1_R, so gilt

(vii) $nx = (n\, 1_R) \cdot x$

Zusatzaufgabe 4. Zeigen Sie: Das Kommutativgesetz der Addition folgt aus den übrigen Axiomen für Ringe mit Eins.

Puzzle. Es sei $\langle R, +, \cdot \rangle$ ein Ring mit Eins und $a \in R$. Zeigen Sie: Wenn es ein *eindeutig bestimmtes* $a' \in R$ gibt mit $aa' = 1$, so folgt $a'a = 1$.

Übungen zur Algebra **WS 95/96** **Blatt 2**

Jörg Binder Abgabetermin: Mo. 13. 11. 1995, 13^{30} Uhr

Aufgabe 5. Es sei $\langle R, +, \cdot \rangle$ ein Ring und $x, y \in R$.

(i) Dann gilt

$$(x+y)^n = x^n + \sum_{k=1}^{n-1} \binom{n}{k} x^{n-k} y^k + y^n$$

für alle $n \in \mathbf{Z}^+$ genau dann, wenn $x \cdot y = y \cdot x$ (wobei $\binom{n}{k} = \frac{n!}{(n-k)!\,k!}$).

(ii) Wenn $\langle R, +, \cdot \rangle$ eine Eins besitzt und $x \cdot y = y \cdot x$, dann gilt für alle $n \in \mathbf{Z}^+$

$$x^n - y^n = (x-y) \cdot \sum_{k=0}^{n-1} x^k y^{n-1-k}.$$

Aufgabe 6. Es sei $\langle R, +, \cdot \rangle$ ein Ring und $x \in R$. Das Element x heißt *idempotent*, wenn $x^2 = x$. Das Element x heißt *nilpotent*, wenn $x^n = 0$ für ein $n \in \mathbf{Z}^+$. Zeigen Sie:

- (*i*) Ein nilpotentes Element außer Null ist ein Nullteiler.
- (*ii*) Ein idempotentes Element außer Null, das nicht Eins von $\langle R, +, \cdot \rangle$ ist, ist ein Nullteiler.
- (*iii*) Ist $\langle R, +, \cdot \rangle$ ein Ring mit Eins und $x \in R$ nilpotent, so ist $1 - x$ invertierbar.
- (*iv*) Ist $\langle R, +, \cdot \rangle$ kommutativ und $x, y \in R$ nilpotent, so ist $x + y$ nilpotent.
- (*v*) Für einen Ring $\langle R, +, \cdot \rangle$ sind die folgenden Bedingungen äquivalent:
  - (a) $\langle R, +, \cdot \rangle$ besitzt keine nilpotenten Elemente außer Null.
  - (b) Für alle $a \in R$: Wenn $a^2 = 0$, dann $a = 0$.

Aufgabe 7. Sei $\langle R, +, \cdot \rangle$ ein Ring, S eine nichtleere Menge und $f \colon S \to R$ bijektiv. Für $x, y \in S$ definiere

$$x \oplus y := f^{-1}(f(x) + f(y))$$
$$x \odot y := f^{-1}(f(x) \cdot f(y))$$

Zeigen Sie: Dann ist $\langle S, \oplus, \odot \rangle$ ein Ring, der eine Eins besitzt, wenn $\langle R, +, \cdot \rangle$ eine Eins besitzt, und der kommutativ ist, wenn $\langle R, +, \cdot \rangle$ kommutativ ist. Begründen Sie noch einmal, dass $\langle \mathbf{Z}, \oplus, \odot \rangle$ aus Aufgabe 1 ein kommutativer Ring mit Eins ist.

Zusatzaufgabe 8. Es sei $\langle R, +, \cdot \rangle$ ein Ring. $\langle R, +, \cdot \rangle$ heißt *Boolescher Ring*, wenn alle Elemente von R idempotent (s. Aufgabe 6) sind. Zeigen Sie: Ein Boolescher Ring ist kommutativ.

Puzzle. Sei $\langle R, +, \cdot \rangle$ ein Ring mit Eins und $x, y \in R$. Zeigen Sie: Wenn $1 - xy$ invertierbar ist, dann ist $1 - yx$ invertierbar. [*Hinweis:* Versuchen Sie, durch eine heuristische Überlegung mit Hilfe der geometrischen Reihe im Reellen einen Ansatz für $(1 - yx)^{-1}$ zu raten.]

Übungen zur Algebra **WS 95/96** **Blatt 3**

Jörg Binder Abgabetermin: Mo. 20. 11. 1995, 13^{30} Uhr

Aufgabe 9. (i) Es sei $\langle R, +, \cdot \rangle$ ein Ring und $\langle S, +, \cdot \rangle$ ein Unterring von $\langle R, +, \cdot \rangle$ mit Eins 1. Zeigen Sie: Wenn 1 nicht auch Eins von $\langle R, +, \cdot \rangle$ ist (d.h. wenn $\langle R, +, \cdot \rangle$ entweder keine Eins besitzt oder die Eins von $\langle R, +, \cdot \rangle$ verschieden von 1 ist), dann ist 1 Nullteiler von $\langle R, +, \cdot \rangle$. [*Hinweis:* Aufgabe 6(ii)]

(ii) Es sei $\langle R, +, \cdot \rangle$ ein Ring mit Eins, so dass $\langle \mathbf{Z}, +, \cdot \rangle$ Eins-Unterring von $\langle R, +, \cdot \rangle$ ist (d.h. $1_R = 1_{\mathbf{Z}}$). Zeigen Sie: Dann gilt für alle $n \in \mathbf{Z}, x \in R$

$$nx = n \cdot x = x \cdot n$$

(m.a.W. in $\langle R, +, \cdot \rangle$ stimmen n-faches von x und Ringprodukt von n und x überein).

Aufgabe 10. Es sei $\langle R, +, \cdot \rangle$ ein Ring und $\langle S, +, \cdot \rangle$,$\langle T, +, \cdot \rangle$ Unterringe von $\langle R, +, \cdot \rangle$. Zeigen Sie: $S \cup T$ bestimmt einen Unterring von $\langle R, +, \cdot \rangle$ genau dann, wenn $S \subseteq T$ oder $T \subseteq S$.

Aufgabe 11. Es sei $\langle R, +, \cdot \rangle$ ein Ring. Das *Zentrum* von $\langle R, +, \cdot \rangle$ ist definiert durch

$$Z(R) := \{x \in R \mid xy = yx \text{ für alle } y \in R\}.$$

Zeigen Sie: $Z(R)$ bestimmt einen kommutativen Unterring von $\langle R, +, \cdot \rangle$.

Aufgabe 12. Es sei $\langle R, +, \cdot \rangle$ ein Ring, $\langle S, +, \cdot \rangle \subseteq \langle R, +, \cdot \rangle$ und $\emptyset \neq X \subseteq R$. Zeigen Sie: Dann ist $S = [X]$ genau dann, wenn gilt:

(i) $X \subseteq S$
(ii) Wenn $\langle T, +, \cdot \rangle \subseteq \langle R, +, \cdot \rangle$ und $X \subseteq T$, dann $\langle S, +, \cdot \rangle \subseteq \langle T, +, \cdot \rangle$.

Aufgabe 13. Es sei $\langle R, +, \cdot \rangle$ ein Ring und $x \in R$. Dann gilt:

$$[\{x\}] = \{n_1 x + n_2 x^2 + \cdots + n_m x^m \mid m \in \mathbf{Z}^+, n_1, \ldots, n_m \in \mathbf{Z}\}$$

Zusatzaufgabe 14. Es sei $\langle R, +, \cdot \rangle$ eine Ring mit Zentrum $Z(R)$. Zeigen Sie: Wenn $x^2 + x \in Z(R)$ für alle $x \in R$, dann ist $\langle R, +, \cdot \rangle$ kommutativ.

Puzzle. Es sei $\langle R, +, \cdot \rangle$ ein Ring, in dem 0 das einzige nilpotente Element ist. Zeigen Sie: Wenn für alle $a, b \in R$ gilt $(ab)^2 = a^2b^2$, so ist $\langle R, +, \cdot \rangle$ kommutativ.

Übungen zur Algebra **WS 95/96** **Blatt 4**

Jörg Binder Abgabetermin: Mo. 27. 11. 1995, 13^{30} Uhr

Aufgabe 15. Es sei $\langle R, +, \cdot \rangle$ ein Ring und $\langle I, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$. Zeigen Sie:

- (*i*) Wenn $\langle R, +, \cdot \rangle$ kommutativ ist, dann ist auch $\langle R/I, +, \cdot \rangle$ kommutativ.
- (*ii*) Wenn $\langle R, +, \cdot \rangle$ eine Eins hat und $R \neq I$ ist, dann hat $\langle R/I, +, \cdot \rangle$ eine Eins.
- (*iii*) $\langle R/I, +, \cdot \rangle$ kann Nullteiler haben, selbst wenn $\langle R, +, \cdot \rangle$ keine Nullteiler hat.
- (*iv*) $\langle R/I, +, \cdot \rangle$ kann nullteilerfrei sein, selbst wenn $\langle R, +, \cdot \rangle$ Nullteiler hat.

Aufgabe 16. Es sei $\langle R, +, \cdot \rangle$ ein Ring und $\langle I, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$, $\langle J, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$. Definiere:

$$I + J := \{x + y \mid x \in I, y \in J\}$$
$$I \cdot J := \{\sum\nolimits_{i=1}^{n} x_i y_i \mid n \in \mathbf{Z}^+, x_i \in I, y_i \in J\}$$

Zeigen Sie: $I \cap J, I + J$ und $I \cdot J$ bestimmen Ideale von $\langle R, +, \cdot \rangle$ und $I \cdot J \subseteq I \cap J \subseteq I + J$.

Aufgabe 17. Es sei $\langle R, +, \cdot \rangle$ ein kommutativer Ring und $\langle I, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$. Definiere:

$$\mathrm{Rad}(I) := \{x \in R \mid x^n \in I \text{ für ein } n \in \mathbf{Z}^+\}$$

Zeigen Sie:

- (*i*) $\mathrm{Rad}(I)$ bestimmt ein Ideal von $\langle R, +, \cdot \rangle$.
- (*ii*) $I \subseteq \mathrm{Rad}(I)$.
- (*iii*) $\mathrm{Rad}(\mathrm{Rad}(I)) = \mathrm{Rad}(I)$

Es sei N die Menge der nilpotenten Elemente von $\langle R, +, \cdot \rangle$. Zeigen Sie: N bestimmt ein Ideal von $\langle R, +, \cdot \rangle$ und $\langle R/N, +, \cdot \rangle$ hat keine nilpotenten Elemente außer Null.

Aufgabe 18. Es sei $\langle R, +, \cdot \rangle$ eine algebraische Struktur mit zweistelligen Operationen $+$ und $\cdot$. Eine Äquivalenzrelation $\sim$ auf R heißt *Kongruenzrelation* auf $\langle R, +, \cdot \rangle$, wenn für alle $x, y, u, v \in R$ gilt: Wenn $x \sim u$ und $y \sim v$,

dann $x + y \sim u + v$ und $x \cdot y \sim u \cdot v$. Wir bezeichnen die Äquivalenzklasse von $x \in R$ bezüglich $\sim$ mit $x/\!\sim$.

(i) Es sei $\langle R, +, \cdot \rangle$ ein Ring und $\langle I, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$. Zeigen Sie: Dann ist $\equiv (\mathrm{mod}\, I)$ eine Kongruenzrelation auf $\langle R, +, \cdot \rangle$ und $I = 0/\!\equiv (\mathrm{mod}\, I)$.

(ii) Es sei $\langle R, +, \cdot \rangle$ ein Ring und $\sim$ eine Kongruenzrelation auf $\langle R, +, \cdot \rangle$. Definiere
$I := 0/\!\sim$. Zeigen Sie: Dann ist $\langle I, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$ und für alle $x, y \in R$: $x \sim y$ genau dann, wenn $x \equiv y \pmod{I}$.

Zusatzaufgabe 19. Es sei $\langle R, +, \cdot \rangle$ ein Ring, in dem 0 das einzige nilpotente Element ist. Zeigen Sie: Dann gehören alle idempotenten Elemente von $\langle R, +, \cdot \rangle$ zum Zentrum.

Puzzle. Es sei $\langle R, +, \cdot \rangle$ ein Integritätsbereich, in dem jedes echte Ideal endlich ist. Zeigen Sie: Dann ist $\langle R, +, \cdot \rangle$ ein Körper.
[*Hinweis:* Betrachen Sie Ideale der Art $Rx := \{r \cdot x \mid r \in R\}$, wobei $x \in R$.]

Übungen zur Algebra **WS 95/96** **Blatt 5**

Jörg Binder Abgabetermin: Mo. 4. 12. 1995, 13^{15} Uhr

Aufgabe 20. Es sei $\langle R, +, \cdot \rangle$ ein Ring und $\langle I, +, \cdot \rangle, \langle J, +, \cdot \rangle, \langle K, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$. Ferner sei $I + J, I \cdot J$ wie in Aufgabe 16 und $I : J = \{x \in R \mid xy \in I \text{ für alle } y \in J\}$. Zeigen Sie:

(*i*) $I : J$ bestimmt ein Ideal von $\langle R, +, \cdot \rangle$.
(*ii*) $I \cdot J \subseteq K \Leftrightarrow I \subseteq K : J$
(*iii*) $I + (J + K) = (I + J) + K$
(*iv*) $I + J = J + I$
(*v*) $I + I = I$
(*vi*) $I \cdot (J \cdot K) = (I \cdot J) \cdot K$
(*vii*) Wenn $\langle R, +, \cdot \rangle$ kommutativ ist, dann gilt $I \cdot J = J \cdot I$.
(*viii*) Wenn $\langle R, +, \cdot \rangle$ eine Eins hat, dann gilt $I \cdot R = R \cdot I = I$.
(*ix*) $I \cdot (J + K) = (I \cdot J) + (I \cdot K)$
(*x*) $(I + J) \cdot K = (I \cdot K) + (J \cdot K)$

Aufgabe 21. (*Chinesischer Restsatz*) Sei $\langle R, +, \cdot \rangle$ ein Ring und seien die Ringe $\langle A_1, +, \cdot \rangle, \ldots, \langle A_n, +, \cdot \rangle$ Ideale von $\langle R, +, \cdot \rangle$, so dass $R^2 + A_i = R$ für alle i und $A_i + A_j = R$ für alle $i \neq j$.[1)] Ferner seien $b_1, \ldots, b_n \in R$. Zeigen Sie: Dann gibt es $b \in R$, so dass für alle $i = 1, \ldots, n$

$$b \equiv b_i \pmod{A_i}.$$

und b ist eindeutig bestimmt bis auf Kongruenz modulo $A_1 \cap \cdots \cap A_n$. [*Hinweis:* Zeigen Sie zunächst $R = A_k + (\bigcap_{i \neq k} A_i)$.]

Aufgabe 22. Es seien $\mathfrak{R}, \mathfrak{S}$ und $\mathfrak{T}$ Ringe. Zeigen Sie:

(*i*) Wenn $f\colon \mathfrak{R} \to \mathfrak{S}$ und $g\colon \mathfrak{S} \to \mathfrak{T}$, dann $g \circ f\colon \mathfrak{R} \to \mathfrak{T}$.
(*ii*) Wenn $f\colon \mathfrak{R} \rightarrowtail \mathfrak{S}$ und $g\colon \mathfrak{S} \rightarrowtail \mathfrak{T}$, dann $g \circ f\colon \mathfrak{R} \rightarrowtail \mathfrak{T}$.
(*iii*) Wenn $f\colon \mathfrak{R} \twoheadrightarrow \mathfrak{S}$ und $g\colon \mathfrak{S} \twoheadrightarrow \mathfrak{T}$, dann $g \circ f\colon \mathfrak{R} \twoheadrightarrow \mathfrak{T}$.
(*iv*) Wenn $f\colon \mathfrak{R} \twoheadrightarrow\!\!\!\!\rightarrowtail \mathfrak{S}$, dann $f^{-1}\colon \mathfrak{S} \twoheadrightarrow\!\!\!\!\rightarrowtail \mathfrak{R}$, wobei $f^{-1}\colon S \twoheadrightarrow\!\!\!\!\rightarrowtail R$ die Umkehrabbildung von $f\colon R \twoheadrightarrow\!\!\!\!\rightarrowtail S$ ist.

[1)] Besitzt $\langle R, +, \cdot \rangle$ eine Eins, so folgt $R^2 = R$ und damit $R^2 + A = R$ für alle $\langle A, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$.

Aufgabe 23. (i) Es seien $\langle R, +, \cdot \rangle, \langle S, \oplus, \odot \rangle$ die Ringe aus Aufgabe 7. Zeigen Sie: $\langle S, \oplus, \odot \rangle \cong \langle R, +, \cdot \rangle$.

(ii) Es sei $\langle R, +, \cdot \rangle$ ein Boolescher Ring, der zugleich Integritätsbereich ist. Zeigen Sie: Dann ist $\langle R, +, \cdot \rangle \cong \langle \mathbf{Z}_2, +, \cdot \rangle$.

Aufgabe 24. Es sei $\langle R, +, \cdot \rangle$ ein Ring und $f, g \colon \langle R, +, \cdot \rangle \rightarrowtail \langle \mathbf{Z}, +, \cdot \rangle$. Zeigen Sie: Dann gilt $f = g$.

Zusatzaufgabe 25. Es sei $\langle K, +, \cdot \rangle$ ein endlicher Körper und $p \in \mathbf{Z}^+$ eine Primzahl, so dass $px = 0$ für alle $x \in K$. Zeigen Sie: Dann ist $\phi \colon K \to K, x \mapsto x^p$ ein Automorphismus von $\langle K, +, \cdot \rangle$.

Puzzle. Es sei $\langle R, +, \cdot \rangle$ ein Integritätsbereich, der nur endlich viele Ideale besitzt. Zeigen Sie: Dann ist $\langle R, +, \cdot \rangle$ ein Körper.

Übungen zur Algebra **WS 95/96** **Blatt 6**

Jörg Binder Abgabetermin: Mo. 11. 12. 1995, 13^{15} Uhr

Aufgabe 26. Es seien $\mathfrak{R}, \mathfrak{S}$ Ringe und $f\colon \mathfrak{R} \to \mathfrak{S}$ ein Homomorphismus. Zeigen Sie: f ist ein Isomorphismus genau dann, wenn es einen Homomorphismus $g\colon \mathfrak{S} \to \mathfrak{R}$ gibt mit $g \circ f = \mathrm{id}_R$ und $f \circ g = \mathrm{id}_S$ (wobei $\mathrm{id}_A\colon A \to A,\ x \mapsto x$ die Identität auf A bezeichnet).

Aufgabe 27. Es seien $\mathfrak{R} = \langle R, +, \cdot \rangle$ und $\mathfrak{S} = \langle S, +, \cdot \rangle$ Ringe. Definiere auf $R \times S$ eine Addition und eine Multiplikation wie folgt: $(a, x) + (b, y) := (a + b, x+y)$ und $(a, x)\cdot(b, y) := (a\cdot b, x\cdot y)$ für $a, b \in R, x, y \in S$. (Beachten Sie, dass hierbei das Additions- sowie das Multiplikationssymbol in drei verschiedenen Bedeutungen verwendet wird.) Überzeugen Sie sich (ohne Beweis!) davon, dass $\mathfrak{R} \times \mathfrak{S} := \langle R \times S, +, \cdot \rangle$ ein Ring ist.

(*i*) Überprüfen Sie, welche der folgenden Aussagen gelten: Sind $\mathfrak{R}$ und $\mathfrak{S}$ beide a) kommutative Ringe, b) Ringe mit Eins oder c) nullteilerfreie Ringe, so ist auch $\mathfrak{R} \times \mathfrak{S}$ ein kommutativer Ring, Ring mit Eins, bzw. nullteilerfreier Ring.

(*ii*) Definiere

$$\begin{array}{llll} \pi_1\colon R \times S \to R, & (a, x) \mapsto a & \pi_2\colon R \times S \to S, & (a, x) \mapsto x \\ \iota_1\colon R \to R \times S, & a \mapsto (a, 0) & \iota_2\colon S \to R \times S, & x \mapsto (0, x) \end{array}$$

Zeigen Sie: $\pi_1\colon \mathfrak{R}\times\mathfrak{S} \twoheadrightarrow \mathfrak{R}, \pi_2\colon \mathfrak{R}\times\mathfrak{S} \twoheadrightarrow \mathfrak{S}, \iota_1\colon \mathfrak{R} \rightarrowtail \mathfrak{R}\times\mathfrak{S}, \iota_2\colon \mathfrak{S} \rightarrowtail \mathfrak{R} \times \mathfrak{S}$.

(*iii*) Es sei $\mathfrak{T}$ ein Ring und $f\colon \mathfrak{T} \to \mathfrak{R}, \mathfrak{g}\colon \mathfrak{T} \to \mathfrak{S}$. Zeigen Sie: Dann gibt es einen eindeutig bestimmten Homomorphismus $\phi\colon \mathfrak{T} \to \mathfrak{R} \times \mathfrak{S}$, so dass $\pi_1 \circ \phi = f$ und $\pi_2 \circ \phi = g$. (30 P.)

Aufgabe 28. (*Zweiter Isomorphiesatz*) Es sei $\langle R, +, \cdot \rangle$ ein Ring und es gelte $\langle I, +, \cdot \rangle, \langle J, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$. Zeigen Sie:

Dann ist

$$\langle I, +, \cdot \rangle \lhd \langle I + J, +, \cdot \rangle, \langle I \cap J, +, \cdot \rangle \lhd \langle J, +, \cdot \rangle$$

und

$$\langle I + J/I, +, \cdot \rangle \cong \langle J/I \cap J, +, \cdot \rangle$$

Aufgabe 29. Es sei $\langle R, +, \cdot \rangle$ ein Ring mit Eins und $\langle I, +, \cdot \rangle, \langle J, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$ mit $I + J = R$. Zeigen Sie:

$$\langle R/I \cap J, +, \cdot \rangle \cong \langle R/I, +, \cdot \rangle \times \langle R/J, +, \cdot \rangle$$

[*Hinweis:* Aufgabe 21.]

Zusatzaufgabe 30. Es seien $\mathfrak{R}, \mathfrak{S}$ und $\mathfrak{T} = \langle T, +, \cdot \rangle$ Ringe. Zeigen Sie: Dann gilt $\mathfrak{R} \times \mathfrak{S} \cong \mathfrak{T}$ genau dann, wenn es Ideale $\mathfrak{I} = \langle I, +, \cdot \rangle \lhd \mathfrak{T}$ und $\mathfrak{J} = \langle J, +, \cdot \rangle \lhd \mathfrak{T}$ gibt mit

(*i*) $I + J = T$
(*ii*) $I \cap J = \{0\}$
(*iii*) $\mathfrak{R} \cong \mathfrak{I}$ und $\mathfrak{S} \cong \mathfrak{J}$.

Puzzle. Es seien $\mathfrak{R}, \mathfrak{S}$ Ringe. Zeigen Sie, dass $\mathfrak{R} \times \mathfrak{S}$ durch die Bedingung aus Aufgabe 27(iii) bis auf Isomorphie eindeutig bestimmt ist, genauer: Ist $\mathfrak{U} = \langle U, +, \cdot \rangle$ ein Ring und sind $\eta_1 \colon \mathfrak{U} \twoheadrightarrow \mathfrak{R}, \eta_2 \colon \mathfrak{U} \twoheadrightarrow \mathfrak{S}$ Homomorphismen, so dass es zu jedem Ring $\mathfrak{T}$ und allen Homomorphismen $f \colon \mathfrak{T} \to \mathfrak{R}, \mathfrak{g} \colon \mathfrak{T} \to \mathfrak{S}$ es einen eindeutig bestimmten Homomorphismus $\phi \colon \mathfrak{T} \to \mathfrak{U}$ mit $f = \eta_1 \circ \phi, g = \eta_2 \circ \phi$ gibt, so folgt $\mathfrak{U} \cong \mathfrak{R} \times \mathfrak{S}$.

Übungen zur Algebra **WS 95/96** **Blatt 7**

Jörg Binder Abgabetermin: Mo. 18. 12. 1995, 13^{15} Uhr

Aufgabe 31. Es sei $\langle R, +, \cdot \rangle$ ein kommutativer Ring mit Eins und $a, b \in R$. Zeigen Sie: $\langle a \rangle \cdot \langle b \rangle = \langle ab \rangle$.

Aufgabe 32. Seien $\langle R, +, \cdot \rangle$, $\langle S, +, \cdot \rangle$ nicht triviale Ringe und $f \colon \langle R, +, \cdot \rangle \to \to \langle S, +, \cdot \rangle$. Zeigen Sie: Wenn $\langle R, +, \cdot \rangle$ ein kommutativer Ring mit Eins ist, in dem jedes Ideal Hauptideal ist, dann ist auch $\langle S, +, \cdot \rangle$ ein kommutativer Ring mit Eins, in dem jedes Ideal Hauptideal ist.

Aufgabe 33. Es sei $\langle R, +, \cdot \rangle$ ein kommutativer Ring und $\langle I, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$. Das Ideal $\langle I, +, \cdot \rangle$ heisst *Primideal*, wenn $I \neq R$ und für alle $x, y \in R$ gilt:

(12.1) Wenn $xy \in I$, dann $x \in I$ oder $y \in I$.

Zeigen Sie: Ein kommutativer Ring $\langle R, +, \cdot \rangle$ ist Integritätsbereich genau dann, wenn $\langle \{0\}, +, \cdot \rangle$ Primideal ist.

Aufgabe 34. Es sei $\langle R, +, \cdot \rangle$ ein kommutativer Ring mit Eins. Zeigen Sie: Dann ist jedes Maximalideal auch Primideal.

Aufgabe 35. Zeigen Sie, dass $\langle \langle 4 \rangle, +, \cdot \rangle \lhd \langle \mathbf{Z}_e, +, \cdot \rangle$ Maximalideal aber kein Primideal von $\langle \mathbf{Z}_e, +, \cdot \rangle$ ist. (M.a.W. die Aussage von Aufgabe 35 gilt für beliebige kommutative Ringe nicht.)

Aufgabe 36. Zeigen Sie: $\langle \langle n \rangle, +, \cdot \rangle$ ist Primideal von $\langle \mathbf{Z}, +, \cdot \rangle$ genau dann, wenn $n = 0$ oder n eine Primzahl ist.

Aufgabe 37. Es sei $\langle R, +, \cdot \rangle$ ein kommutativer Ring und $\langle I, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$. Dann ist $\langle I, +, \cdot \rangle$ Primideal genau dann, wenn $\langle R/I, +, \cdot \rangle$ ein Integritätsbereich ist.

Zusatzaufgabe 38. Es sei $\langle R, +, \cdot \rangle$ ein Hauptidealring und $\langle \{0\}, +, \cdot \rangle \neq \langle I, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$. Zeigen Sie: Dann ist $\langle I, +, \cdot \rangle$ Primideal genau dann, wenn $\langle I, +, \cdot \rangle$ Maximalideal ist.

Puzzle. Im Fall eines (nicht notwendig kommutativen) Rings $\langle R, +, \cdot \rangle$ nennt man ein Ideal $\langle I, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$ *Primideal*, wenn $I \neq R$ und für alle $\langle A, +, \cdot \rangle, \langle B, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$ gilt:

$$\text{Wenn } A \cdot B \subseteq I, \text{ dann } A \subseteq I \text{ oder } B \subseteq I.$$

Zeigen Sie, dass ein echtes Ideal, das die Bedingung (1) aus Aufgabe 33 erfüllt, Primideal in diesem Sinne ist. Zeigen Sie ferner, dass für kommutative Ringe beide Definitionen von „Primideal“ äquivalent sind.

Übungen zur Algebra **WS 95/96** **Blatt 8**

Jörg Binder Abgabetermin: Mo. 8. 1. 1996, 13^{15} Uhr

Aufgabe 39. Es sei M eine Menge. Eine (zweistellige) Relation $\prec$ auf M heißt *Quasiordnung* (auf M), wenn $\prec$ reflexiv und transitiv ist. Eine *Partialordnung* ist eine antisymmetrische Quasiordnung. Sei $\prec$ eine Quasiordnung auf M. Wir definieren

$$a \sim b :\Leftrightarrow a \prec b \text{ und } b \prec a.$$

Zeigen Sie:

(i) Dann ist $\sim$ eine Äquivalenzrelation auf M.

Sei $a/\!\sim := \{x \in M \mid x \sim a\}$ die Äquivalenzklasse von $a \in M$ und $M/\!\sim := \{a/\!\sim \mid a \in M\}$.

(i) Dann ist die durch die Festsetzung $a/\!\sim \leq b/\!\sim :\Leftrightarrow a \prec b$ gegebene Relation $\leq$ auf $M/\!\sim$ wohldefiniert.

(ii) $\leq$ ist eine Partialordnung auf $M/\!\sim$.

Aufgabe 40. Es sei $\langle R, +, \cdot \rangle$ kommutativer Ring mit Eins. Ein Element $p \in R$ heißt *Primelement*, wenn $p \neq 0$, p nicht invertierbar ist und für alle $a, b \in R$ gilt: Wenn $p|ab$, dann $p|a$ oder $p|b$. Zeigen Sie:

(i) Für alle $u \in R$: u ist genau dann invertierbar, wenn $u|a$ für alle $a \in R$.

(ii) Für alle $u \in R$: u ist genau dann invertierbar, wenn $\langle u \rangle = R$.

(iii) Für alle $0 \neq p \in R$: p ist genau dann Primelement, wenn $\langle p \rangle$ ein Primideal ist.

(iv) Sei nun $\langle R, +, \cdot \rangle$ ein Integritätsbereich mit Eins. Dann gilt für alle $0 \neq c \in R$: c ist genau dann irreduzibel, wenn $\langle c \rangle$ maximal in der Menge der von R verschiedenen Hauptideale ist, d.h. wenn $\langle c \rangle \neq R$ und für alle $a \in R$:
$\langle c \rangle \subseteq \langle a \rangle \Rightarrow \langle a \rangle = \langle c \rangle$ oder $\langle a \rangle = R$.

Aufgabe 41. Zeigen Sie: In $\langle \mathbf{Z}_6, +, \cdot \rangle$ ist 2 Primelement aber nicht irreduzibel. In einem Integritätsbereich mit Eins ist jedes Primelement irreduzibel. In einem Hauptidealring ist ein Element genau dann Primelement, wenn es irreduzibel ist.

Aufgabe 42. Es sei $\langle R, +, \cdot \rangle$ eine kommutativer Ring mit Eins und $a, b \in R \setminus \{0\}$. Zeigen Sie: a und b besitzen genau dann einen größten gemeinsamen Teiler, der Linearkombination von a und b ist, wenn es ein $c \in R$ gibt mit $\langle \{a, b\} \rangle = \langle c \rangle$.

Aufgabe 43. Es sei $\langle R, +, \cdot \rangle$ eine kommutativer Ring mit Eins und $a, b, k \in R \setminus \{0\}$. Das Element k heißt *kleinstes gemeinsames Vielfaches* von a und b, wenn $a|k, b|k$ und für alle $u \in R \setminus \{0\}$ mit $a|u, b|u$ folgt, dass $k|u$. Zeigen Sie:

(*i*) k ist kleinstes gemeinsames Vielfaches von a und b genau dann, wenn $\langle a \rangle \cap \langle b \rangle = \langle k \rangle$. Daher besitzen je zwei Elemente eines Hauptidealrings ein kleinstes gemeinsames Vielfaches.

(*ii*) Sind k_1 und k_2 kleinste gemeinsame Vielfache von a und b, so folgt $k_1 \sim k_2$.

(*iii*) Ist in einem Hauptidealring g größter gemeinsamer Teiler und k kleinstes gemeinsames Vielfaches von a und b, so folgt $a \cdot b \sim g \cdot k$.

Zusatzaufgabe 44. Es sei $\langle R, +, \cdot \rangle$ ein Integritätsbereich mit Eins. Zeigen Sie: Dann sind äquivalent:

(*i*) $\langle R, +, \cdot \rangle$ ist ein Gauß'scher Ring.

(*ii*) $\langle R, +, \cdot \rangle$ ist ein Ring, in dem jedes Element, das weder Null noch invertierbar ist, Produkt von irreduziblen Elementen ist und alle irreduziblen Elemente von R sind Primelemente.

(*iii*) $\langle R, +, \cdot \rangle$ ist ein Ring, in dem jedes Element, das weder Null noch invertierbar ist, Produkt von Primelementen ist.

Puzzle. Es sei $\langle R, +, \cdot \rangle$ kommutativer Ring mit Eins. Zeigen Sie: $\langle R, +, \cdot \rangle$ ist Hauptidealring genau dann, wenn $\langle R, +, \cdot \rangle$ Gauß'scher Ring ist und je zwei Elemente $a, b \in R$ einen größten gemeinsamen Teiler besitzen, der Linearkombination von a und b ist.

Übungen zur Algebra **WS 95/96** **Blatt 9**

Jörg Binder Abgabetermin: Mo. 15. 1. 1996, 13^{15} Uhr

Aufgabe 45. Betrachte $\langle \mathbf{Z}, +, \cdot \rangle \subseteq \langle \mathbf{Z}[\sqrt{10}], +, \cdot \rangle \subseteq \langle \mathbf{R}, +, \cdot \rangle$. Zeigen Sie: Jedes Element aus $\mathbf{Z}[\sqrt{10}]$ lässt sich eindeutig darstellen als $m + n\sqrt{10}$ mit $m, n \in \mathbf{Z}$. Definiere $N(m + n\sqrt{10}) := (m + n\sqrt{10})(m - n\sqrt{10}) = m^2 - 10n^2$. Zeigen Sie: Dann gilt für alle $a, b \in \mathbf{Z}[\sqrt{10}]$:

- (*i*) $N(ab) = N(a)N(b)$.
- (*ii*) $N(a) = 0 \Leftrightarrow a = 0$.
- (*iii*) a ist invertierbar in $\langle \mathbf{Z}[\sqrt{10}], +, \cdot \rangle$ genau dann, wenn $N(a) = \pm 1$.
- (*iv*) $2, 3, 4 + \sqrt{10}$ und $4 - \sqrt{10}$ sind irreduzibel in $\langle \mathbf{Z}[\sqrt{10}], +, \cdot \rangle$.
- (*v*) $2, 3, 4+\sqrt{10}$ und $4-\sqrt{10}$ sind nicht prim in $\langle \mathbf{Z}[\sqrt{10}], +, \cdot \rangle$. [*Hinweis:* $2 \cdot 3 = 6 = (4 + \sqrt{10}) \cdot (4 - \sqrt{10})$]

Aufgabe 46. Zeigen Sie, dass sich in dem Ring aus Aufgabe 45 jedes Element, das weder Null noch invertierbar ist, als Produkt irreduzibler Elemente darstellen lässt; diese Darstellung jedoch nicht eindeutig (bis auf Assoziierte und Ordnung der Faktoren) zu sein braucht (m.a.W. $\langle \mathbf{Z}[\sqrt{10}], +, \cdot \rangle$ ist kein Gauß'scher Ring).

Aufgabe 47. Sei $\langle R, +, \cdot \rangle$ ein kommutativer Ring und $\langle I, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$. Wir sagen, $\langle I, +, \cdot \rangle$ ist *endlich erzeugt* (oder $\langle I, +, \cdot \rangle$ hat eine *endliche Basis*), wenn es eine endliche Menge $\emptyset \neq X \subseteq I$ gibt, so dass $I = \langle X \rangle$. Zeigen Sie, dass die folgenden Aussagen äquivalent sind:

- (*i*) $\langle R, +, \cdot \rangle$ ist ein Noetherscher Ring.
- (*ii*) Jedes Ideal von $\langle R, +, \cdot \rangle$ ist endlich erzeugt.
- (*iii*) Jede nichtleere gerichtete Menge von Idealen in $\langle R, +, \cdot \rangle$ enthält ein größtes Ideal.
- (*iv*) Jede nichtleere Menge von Idealen in $\langle R, +, \cdot \rangle$ enthält ein maximales Ideal, d.h. ein Ideal, das in keinem anderen Ideal dieser Menge echt enthalten ist. (Ein solches Ideal braucht natürlich kein Maximalideal von $\langle R, +, \cdot \rangle$ zu sein.)

Aufgabe 48. (*Euklidischer Algorithmus*) Es sei $\langle R, +, \cdot \rangle$ ein Euklidischer Ring mit Euklidischer Norm d und $0 \neq x, y \in R$. Wenn $y \nmid x$, dann gibt es

$n \in \mathbf{Z}^+$ und $q_0, \ldots, q_n \in R, r_1, \ldots, r_n \in R \setminus \{0\}$, so dass

$$\begin{aligned} x &= q_0 \cdot y + r_1, \text{ wobei } d(r_1) < d(y) \\ y &= q_1 \cdot r_1 + r_2, \text{ wobei } d(r_2) < d(r_1) \\ r_1 &= q_2 \cdot r_2 + r_3, \text{ wobei } d(r_3) < d(r_2) \\ &\vdots \\ r_{n-2} &= q_{n-1} \cdot r_{n-1} + r_n, \text{ wobei } d(r_n) < d(r_{n-1}) \\ r_{n-1} &= q_n \cdot r_n \end{aligned}$$

Zeigen Sie: Dann ist r_n größter gemeinsamer Teiler von x und y.

Zusatzaufgabe 49. Mit Hilfe des Euklidischen Algorithmus bestimme man in $\langle \mathbf{Z}[i], +, \cdot \rangle$:

(i) einen größten gemeinsamen Teiler von $3 + 4i$ und $4 - 3i$,
(ii) einen größten gemeinsamen Teiler von $11 + 7i$ und $18 - i$.

Puzzle. Es sei $\langle R, +, \cdot \rangle$ ein kommutativer Ring mit Eins, $\langle I, +, \cdot \rangle \lhd \langle R, +, \cdot \rangle$ ein Ideal und $\langle P_1, +, \cdot \rangle, \ldots, \langle P_n, +, \cdot \rangle$ Primideale von $\langle R, +, \cdot \rangle$, so dass $I \subseteq P_1 \cup \cdots \cup P_n$. Zeigen Sie: Dann gibt es ein $1 \leq i \leq n$, so dass $I \subseteq P_i$.

Übungen zur Algebra **WS 95/96** **Blatt 10**

Jörg Binder Abgabetermin: Mo. 22. 1. 1996, 13^{15} Uhr

Aufgabe 50. Sei $\langle F, +, \cdot \rangle$ ein Körper, $x, u \in F$ und $y, v \in F \setminus \{0\}$. Zeigen Sie:

$$\frac{x}{y} = \frac{u}{v} \quad \text{genau dann, wenn } x \cdot v = y \cdot u$$
$$\frac{x}{y} + \frac{u}{v} = \frac{x \cdot v + y \cdot u}{y \cdot v}$$
$$\frac{x}{y} - \frac{u}{v} = \frac{x \cdot v - y \cdot u}{y \cdot v}$$
$$\frac{x}{y} \cdot \frac{u}{v} = \frac{x \cdot u}{y \cdot v}$$
$$\frac{\left(\frac{x}{y}\right)}{\left(\frac{u}{v}\right)} = \frac{x \cdot v}{y \cdot u}, \text{ wobei } u \neq 0$$

Aufgabe 51. Ein Körper heißt *Primkörper*, wenn er keine echten Unterkörper enthält. Zeigen Sie:

(*i*) $\langle \mathbf{Q}, +, \cdot \rangle$ ist ein Primkörper.
(*ii*) Für jede Primzahl $p \in \mathbf{Z}$ ist $\langle \mathbf{Z}_p, +, \cdot \rangle$ ein Primkörper.

Aufgabe 52. Zeigen Sie: Jeder Körper enthält genau einen Primkörper als Unterkörper.

Aufgabe 53. Es sei $\langle R, +, \cdot \rangle$ ein kommutativer Ring. Eine nichtleere Teilmenge $S \subseteq R$ heißt *multiplikativ*, wenn $a, b \in S \Rightarrow ab \in S$. Sei also nun S eine multiplikative Teilmenge von R. Zeigen Sie: (i) Die Relation $\sim$ auf $R \times S$ definiert durch

$$(r, s) \sim (r', s') \Leftrightarrow \text{ es gibt ein } s_1 \in S : s_1(rs' - r's) = 0$$

ist eine Äquivalenzrelation.

(ii) Wenn $\langle R, +, \cdot \rangle$ nullteilerfrei ist und $0 \notin S$, dann

$$(r, s) \sim (r', s') \quad \Leftrightarrow \quad rs' - r's = 0$$

Wir bezeichnen die Äquivalenzklasse von $(r, s) \in R \times S$ mit r/s und die Menge aller Äquivalenzklassen von $R \times S$ mit $S^{-1}R$. Zeigen Sie:

(iii) $r/s = r'/s' \Leftrightarrow$ es gibt ein $s_1 \in S : s_1(rs' - r's) = 0$

(iv) Für alle $r \in R,\ s, t \in S : tr/ts = r/s$.

(v) Wenn $0 \in S$, dann besteht $S^{-1}R$ aus einer einzigen Äquivalenzklasse.

Wir definieren

$$r/s + r'/s' := (rs' + r's)/ss' \quad \text{und} \quad (r/s) \cdot (r'/s') := rr'/ss'.$$

(vi) Dann sind $+$ und $\cdot$ wohldefiniert und $\langle S^{-1}R, +, \cdot \rangle$ ist ein kommutativer Ring.

(vii) Wenn $\langle R, +, \cdot \rangle$ Integritätsbereich ist und $0 \notin S$, dann ist $\langle S^{-1}R, +, \cdot \rangle$ ein Integritätsbereich mit Eins.

(viii) Ist $\langle R, +, \cdot \rangle$ Integritätsbereich und $S = R \setminus \{0\}$, dann ist $\langle S^{-1}R, +, \cdot \rangle$ ein Körper.

Zusatzaufgabe 54. Es sei S eine multiplikative Teilmenge eines nicht trivialen kommutativen Rings und $S^{-1}R$ wie in Aufgabe 53. Zeigen Sie:

(i) Die Abbildung $\varphi_S \colon R \to S^{-1}R,\ r \mapsto rs/s$ (für irgendein $s \in S$) ist ein wohl definierter (d.h. $s, s' \in S \Rightarrow rs/s = rs'/s'$) Ringhomomorphismus, so dass $\varphi_S(s)$ für alle $s \in S$ invertierbar ist.

(ii) Wenn $\langle R, +, \cdot \rangle$ Integritätsbereich ist und $0 \notin S$, dann ist φ_S eine Einbettung.

(iii) Wenn zusätzlich $\langle R, +, \cdot \rangle$ eine Eins hat und S aus invertierbaren Elementen besteht, dann ist φ_S ein Isomorphismus.

Puzzle. Sei $\langle F, +, \cdot \rangle$ ein Primkörper. Zeigen Sie:

Dann ist $\langle F, +, \cdot \rangle \cong \langle \mathbf{Q}, +, \cdot \rangle$ oder es existiert eine Primzahl $p \in \mathbf{Z}$, so dass $\langle F, +, \cdot \rangle \cong \langle \mathbf{Z}_p, +, \cdot \rangle$. [*Hinweis:* Betrachte $f \colon \langle \mathbf{Z}, +, \cdot \rangle \to \langle F, +, \cdot \rangle, n \mapsto n1$.]

Übungen zur Algebra **WS 95/96** **Blatt 10**

Jörg Binder Abgabetermin: Mo. 22. 1. 1996, 13^{15} Uhr

Aufgabe 50. Sei $\langle F, +, \cdot \rangle$ ein Körper, $x, u \in F$ und $y, v \in F \setminus \{0\}$. Zeigen Sie:

$$\frac{x}{y} = \frac{u}{v} \quad \text{genau dann, wenn } x \cdot v = y \cdot u$$

$$\frac{x}{y} + \frac{u}{v} = \frac{x \cdot v + y \cdot u}{y \cdot v}$$

$$\frac{x}{y} - \frac{u}{v} = \frac{x \cdot v - y \cdot u}{y \cdot v}$$

$$\frac{x}{y} \cdot \frac{u}{v} = \frac{x \cdot u}{y \cdot v}$$

$$\frac{\left(\frac{x}{y}\right)}{\left(\frac{u}{v}\right)} = \frac{x \cdot v}{y \cdot u}, \text{ wobei } u \neq 0$$

Aufgabe 51. Ein Körper heißt *Primkörper*, wenn er keine echten Unterkörper enthält. Zeigen Sie:

(*i*) $\langle \mathbf{Q}, +, \cdot \rangle$ ist ein Primkörper.
(*ii*) Für jede Primzahl $p \in \mathbf{Z}$ ist $\langle \mathbf{Z}_p, +, \cdot \rangle$ ein Primkörper.

Aufgabe 52. Zeigen Sie: Jeder Körper enthält genau einen Primkörper als Unterkörper.

Aufgabe 53. Es sei $\langle R, +, \cdot \rangle$ ein kommutativer Ring. Eine nichtleere Teilmenge $S \subseteq R$ heißt *multiplikativ*, wenn $a, b \in S \Rightarrow ab \in S$. Sei also nun S eine multiplikative Teilmenge von R. Zeigen Sie: (i) Die Relation $\sim$ auf $R \times S$ definiert durch

$$(r, s) \sim (r', s') \Leftrightarrow \text{ es gibt ein } s_1 \in S : s_1(rs' - r's) = 0$$

ist eine Äquivalenzrelation.

(ii) Wenn $\langle R, +, \cdot \rangle$ nullteilerfrei ist und $0 \notin S$, dann

$$(r, s) \sim (r', s') \quad \Leftrightarrow \quad rs' - r's = 0$$

Wir bezeichnen die Äquivalenzklasse von $(r, s) \in R \times S$ mit r/s und die Menge aller Äquivalenzklassen von $R \times S$ mit $S^{-1}R$. Zeigen Sie:

(iii) $r/s = r'/s' \Leftrightarrow$ es gibt ein $s_1 \in S : s_1(rs' - r's) = 0$

(iv) Für alle $r \in R,\ s, t \in S : tr/ts = r/s$.

(v) Wenn $0 \in S$, dann besteht $S^{-1}R$ aus einer einzigen Äquivalenzklasse.

Wir definieren

$$r/s + r'/s' := (rs' + r's)/ss' \quad \text{und} \quad (r/s) \cdot (r'/s') := rr'/ss'.$$

(vi) Dann sind $+$ und $\cdot$ wohldefiniert und $\langle S^{-1}R, +, \cdot \rangle$ ist ein kommutativer Ring.

(vii) Wenn $\langle R, +, \cdot \rangle$ Integritätsbereich ist und $0 \notin S$, dann ist $\langle S^{-1}R, +, \cdot \rangle$ ein Integritätsbereich mit Eins.

(viii) Wenn $\langle R, +, \cdot \rangle$ Integritätsbereich ist und $S = R\backslash\{0\}$, dann ist $\langle S^{-1}R, +, \cdot \rangle$ ein Körper.

Zusatzaufgabe 54. Es sei S eine multiplikative Teilmenge eines nichttrivialen kommutativen Rings und $S^{-1}R$ wie in Aufgabe 53. Zeigen Sie:

(i) Die Abbildung $\varphi_S \colon R \to S^{-1}R,\ r \mapsto rs/s$ (für irgendein $s \in S$) ist ein wohl definierter (d.h. $s, s' \in S \Rightarrow rs/s = rs'/s'$) Ringhomomorphismus, so dass $\varphi_S(s)$ für alle $s \in S$ invertierbar ist.

(ii) Wenn $\langle R, +, \cdot \rangle$ Integritätsbereich ist und $0 \notin S$, dann ist φ_S eine Einbettung.

(iii) Wenn zusätzlich $\langle R, +, \cdot \rangle$ eine Eins hat und S aus invertierbaren Elementen besteht, dann ist φ_S ein Isomorphismus.

Puzzle. Sei $\langle F, +, \cdot \rangle$ ein Primkörper. Zeigen Sie:

Dann ist $\langle F, +, \cdot \rangle \cong \langle \mathbf{Q}, +, \cdot \rangle$ oder es gibt eine Primzahl $p \in \mathbf{Z}$, so dass $\langle F, +, \cdot \rangle \cong \langle \mathbf{Z}_p, +, \cdot \rangle$. [*Hinweis:* Betrachte $f \colon \langle \mathbf{Z}, +, \cdot \rangle \to \langle F, +, \cdot \rangle, n \mapsto n1$.]

Übungen zur Algebra **WS 95/96** **Blatt 11**

Jörg Binder Abgabetermin: Mo. 29. 1. 1996, 13^{30} Uhr

Aufgabe 55. (*Existenz des Polynomrings*) Sei $\langle R, +, \cdot \rangle$ ein kommutativer Ring mit Eins und P die Menge aller unendlicher Folgen $(a_0, a_1, a_2, \dots)$ von Elementen aus R, so dass $a_i = 0$ für alle bis auf endlich viele Indices i. Definiere

$$(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$$
$$(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots),$$

wobei

$$c_n = \sum_{i=0}^{n} a_i b_{n-i}$$

Zeigen Sie: (i) Dann ist $\langle P, +, \cdot \rangle$ ein kommutativer Ring mit Eins.

(ii) Definiere $\psi\colon R \to P, r \mapsto (r, 0, 0, \dots)$. Dann ist $\psi\colon \langle R, +, \cdot \rangle \rightarrowtail \langle P, +, \cdot \rangle$ eine Eins-Einbettung.

(iii) Sei $x := (0, 1, 0, 0, \dots)$. Dann ist für $n \in \mathbf{N}$: $x^n = (0, 0, \dots, 0, 1, 0, \dots)$, wobei die 1 an der $(n+1)$-ten Stelle steht.

(iv) Wir identifizieren nun $\langle R, +, \cdot \rangle$ mit $\langle \psi(R), +, \cdot \rangle \cong \langle R, +, \cdot \rangle$, d.h. wir schreiben statt $(r, 0, 0, \dots)$ einfach r. Dann ist $rx^n = (0, 0, \dots, 0, r, 0, \dots)$, wobei r an der $(n+1)$-ten Stelle steht.

(v) Sei $(a_0, a_1, a_2, \dots) \in P$, wobei $a_i = 0$ für $i > n$. Dann ist $(a_0, a_1, a_2, \dots) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$.

(vi) $P = R[x]$.

(vii) $\langle P, +, \cdot \rangle$ ist Polynomring in einer Unbestimmten x über $\langle R, +, \cdot \rangle$.

Aufgabe 56. (*Verallgemeinerter Divisionsalgorithmus*) Sei $\langle R, +, \cdot \rangle$ ein kommutativer Ring mit Eins und $\langle R[x], +, \cdot \rangle$ Polynomring in einer Unbestimmten x über $\langle R, +, \cdot \rangle$. Seien ferner $f = a_0 + a_1 x + \cdots + a_n x^n$ und $g = b_0 + b_1 x + \cdots + b_m x^m$ Polynome aus $R[x]$, wobei $m \leq n + 1$. Zeigen Sie: Dann gibt es $q, r \in R[x]$, so dass

$${b_m}^{n-m+1} f = q \cdot g + r$$

mit $r = 0$ oder $\operatorname{grad} r < m$.

Aufgabe 57. (*Die funktionale Auffassung von Polynomen.*) Sei $\langle R, +, \cdot \rangle$ ein kommutativer Ring mit Eins und $\langle R[x], +, \cdot \rangle$ Polynomring in einer Unbestimmten x über $\langle R, +, \cdot \rangle$. Für $f = a_0 + a_1 x + \cdots + a_n x^n$ definiere $\tilde{f}\colon R \to R$, $a \mapsto \tilde{f}(a) := a_0 + a_1 a + \cdots + a_n a^n$. $\tilde{f}$ heißt *die von f erzeugte Polynomfunktion.* Setze

$$\tilde{R} = \{\tilde{f} \mid f \in R[x]\}$$
$$(\tilde{f} + \tilde{g})(a) := \tilde{f}(a) + \tilde{g}(a)$$
$$(\tilde{f} \cdot \tilde{g})(a) := \tilde{f}(a) \cdot \tilde{g}(a)$$

für $a \in R$. Ohne Beweis: Dann ist $\langle \tilde{R}, +, \cdot \rangle$ ein kommutativer Ring mit Eins. Definiere $\varphi\colon R[x] \to \tilde{R}, f \mapsto \tilde{f}$. Zeigen Sie:

(i) $\varphi\colon \langle R[x], +, \cdot \rangle \twoheadrightarrow \langle \tilde{R}, +, \cdot \rangle$.

(ii) Für alle $x \in \langle \mathbf{Z}_p, +, \cdot \rangle$, p eine Primzahl, gilt $x^p = x$. [*Hinweis:* Aufgabe 25.] Folgern Sie, dass für $\langle R, +, \cdot \rangle = \langle \mathbf{Z}_p, +, \cdot \rangle$ der Epimorphismus φ aus (i) kein Isomorphismus ist. Was folgt hieraus für die funktionale Auffassung von Polynomen?

Aufgabe 58. Sei $\langle \mathbf{Q}[x], +, \cdot \rangle$ Polynomring in einer Unbestimmten x über dem Körper $\langle \mathbf{Q}, +, \cdot \rangle$ der rationalen Zahlen und $f = x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1, g = x^4 + x^2 + 1 \in \mathbf{Q}[x]$. Bestimmen Sie einen größten gemeinsamen Teiler von f und g.

Aufgabe 59. Zeigen Sie: Der Polynomring in einer Unbestimmten x über $\langle \mathbf{Z}, +, \cdot \rangle$ ist kein Hauptidealring. [*Hinweis:* Betrachten Sie das von x und 2 erzeugte Ideal.]

Zusatzaufgabe 60. Wir knüpfen an Aufgabe 57 an.

(i) Sei $\langle R, +, \cdot \rangle$ ein unendlicher Integritätsbereich (mit Eins). Dann ist φ in ein Isomorphismus.

(ii) $\langle \tilde{R}, +, \cdot \rangle$ ist Integritätsbereich genau dann, wenn $\langle R, +, \cdot \rangle$ ein unendlicher Integritätsbereich ist.

Puzzle. Sei $\langle \mathbf{Q}[x], +, \cdot \rangle$ Polynomring in einer Unbestimmten x über dem Körper $\langle \mathbf{Q}, +, \cdot \rangle$ der rationalen Zahlen. Bestimmen Sie ein Polynom $p \in \mathbf{Q}[x]$, so dass p durch $x^2 + 1$ und $p + 1$ durch $x^3 + x^2 + 1$ teilbar ist.

Übungen zur Algebra **WS 95/96** **Blatt 12**

Jörg Binder Abgabetermin: Mo. 5. 2. 1996, 13^{15} Uhr

Aufgabe 61. (*Rational-Root-Test*) Es sei $\langle \mathbf{Z}[x], +, \cdot \rangle$ Polynomring in einer Unbestimmten x über $\langle \mathbf{Z}, +, \cdot \rangle$ und $f = a_0 + a_1 x + \cdots + a_n x^n \in \mathbf{Z}[x]$. Zeigen Sie:

(i) Wenn $p/q \in \mathbf{Q}$ Wurzel von f ist, wobei $p, q \in \mathbf{Z}$ teilerfremd sind, dann $p | a_0$ und $q | a_n$.

(ii) Wenn a_0, a_n und $f(1)$ ungerade sind, dann hat f keine rationale Wurzel.

Aufgabe 62. Es sei $\mathfrak{F} = \langle F, +, \cdot \rangle$ ein Körper, $\langle F[x], +, \cdot \rangle$ Polynomring in einer Unbestimmten x über $\mathfrak{F}$ und $f \in F[x]$ irreduzibel. Zeigen Sie: Wenn $\langle G, +, \cdot \rangle$ eine f-Wurzelerweiterung von $\mathfrak{F}$ ist, dann gilt

$$\langle G, +, \cdot \rangle \cong \langle F[x]/\langle f \rangle, +, \cdot \rangle$$

Aufgabe 63. (*Existenz der Wurzelerweiterung*) Es sei $\mathfrak{F} = \langle F, +, \cdot \rangle$ ein Körper, $\langle F[x], +, \cdot \rangle$ Polynomring in einer Unbestimmten x über $\mathfrak{F}$ und $f \in F[x]$ irreduzibel. Zeigen Sie:

(i) $\langle F[x]/\langle f \rangle, +, \cdot \rangle$ ist ein Körper.

Definiere

$$\varphi \colon F \to F[x]/\langle f \rangle,\ c \mapsto \langle f \rangle + c.$$

(ii) Dann ist $\varphi \colon \langle F, +, \cdot \rangle \rightarrowtail \langle F[x]/\langle f \rangle, +, \cdot \rangle$. Nach Identifizierung bekommen wir also:

$$\langle F, +, \cdot \rangle \subseteq \langle F[x]/\langle f \rangle, +, \cdot \rangle.$$

Setze $a := \langle f \rangle + x$.

(iii) Für jedes $g \in F[x]$ gilt: $g(a) = \langle f \rangle + g$.

(iv) $F[x]/\langle f \rangle = F(a)$.

(v) $f(a) = \langle f \rangle + 0$, d.h. a ist Wurzel von f in $\langle F[x]/\langle f \rangle, +, \cdot \rangle$.

(vi) Was ändert sich in (i)-(v), wenn wir nicht mehr voraussetzen, dass f irreduzibel ist?

Aufgabe 64. Es sei $\langle \mathbf{Z}_3[x], +, \cdot \rangle$ Polynomring in einer Unbestimmten x über $\langle \mathbf{Z}_3, +, \cdot \rangle$.

(i) Zeigen Sie: $f = x^2 + x + 2$ ist irreduzibel in $\langle \mathbf{Z}_3[x], +, \cdot \rangle$.

(ii) Es sei $\langle \mathbf{Z}_3(a), +, \cdot \rangle$ der von einer Wurzel a von f über $\langle \mathbf{Z}_3, +, \cdot \rangle$ erzeugte Erweiterungskörper. Stellen Sie die Additions- und Multiplikationstabellen für $\langle \mathbf{Z}_3(a), +, \cdot \rangle$ auf.

Aufgabe 65. Es seien $\mathfrak{F} = \langle F, +, \cdot \rangle \subseteq \langle G, +, \cdot \rangle$ Körper, $\langle F[x], +, \cdot \rangle$ Polynomring in einer Unbestimmten x über $\mathfrak{F}$ und $f \in F[x]$ mit $n := \operatorname{grad} f > 0$. Ferner sei $a \in G$ mit $f(a) = 0$ und $G = F(a)$. Zeigen Sie: Wenn es zu jedem $u \in G$ eindeutig bestimmte $a_0, a_1, \ldots, a_{n-1} \in F$ gibt, so dass

$$u = a_0 + a_1 a + \cdots + a_{n-1} a^{n-1},$$

dann ist f irreduzibel. (Vgl. auch Theorem 3.14!)

Zusatzaufgabe 66. (*Hilbert-Basis-Satz*) Sei $\mathfrak{R} = \langle R, +, \cdot \rangle$ ein Noetherscher Ring mit Eins und $\langle R[x], +, \cdot \rangle$ Polynomring in einer Unbestimmten x über $\mathfrak{R}$. Zeigen Sie: Dann ist auch $\langle R[x], +, \cdot \rangle$ Noethersch.

[*Anleitung:* Benutzen Sie Aufgabe 47 (i)⇔(ii). Sei $\langle I, +, \cdot \rangle \lhd \langle R[x], +, \cdot \rangle$. Annahme: $\langle I, +, \cdot \rangle$ ist nicht endlich erzeugt. Konstruiere eine Folge $f_0, f_1, f_2, \ldots$ von Elementen aus I wie folgt: Wähle $0 \neq f_0 \in I$ mit minimalen Grad. Sind $f_0, \ldots, f_n$ bereits definiert, so sei f_{n+1} ein Polynom minimalem Grad aus $I \setminus \langle \{f_0, \ldots, f_n\} \rangle$. Zeigen Sie $\operatorname{grad} f_i \leq \operatorname{grad} f_j$ für $i < j$. Sei a_n der Leitkoeffizient von f_n. Betrachten Sie die Kette $\langle a_0 \rangle \subseteq \langle \{a_0, a_1\} \rangle \subseteq \ldots \subseteq \langle \{a_0, \ldots, a_n\} \rangle \subseteq \ldots$. Benutzen Sie nun, dass $\langle R, +, \cdot \rangle$ Noethersch ist und konstruieren Sie zum Widerspruch für ein n ein Polynom aus $I \setminus \langle \{f_0, \ldots, f_n\} \rangle$ mit kleinerem Grad als f_{n+1}. Siehe auch: H. Sarges. Ein Beweis des Hilbertschen Basissatzes. *J. Reine Angew. Math.* **283/84**, 436–437, (1976).]

Puzzle. Eine reelle Zahl heißt *algebraisch* über $\langle \mathbf{Q}, +, \cdot \rangle$, wenn sie Wurzel eines Polynoms mit rationalen Koeffizienten ist. Zeigen Sie, dass $\sin(1^\circ)$ algebraisch über $\langle \mathbf{Q}, +, \cdot \rangle$ ist.

Übungen zur Algebra **WS 95/96** **Blatt 13**

Jörg Binder Abgabetermin: Mo. 12. 2. 1996, 13^{15} Uhr

Aufgabe 67. Seien $\mathfrak{F} = \langle F, +, \cdot \rangle$ und $\mathfrak{G} = \langle G, +, \cdot \rangle$ Körper mit $\mathfrak{F} \subseteq \mathfrak{G}$, $\langle F[x], +, \cdot \rangle$ Polynomring in einer Unbestimmten x über $\mathfrak{F}$, und sei $f \in F[x]$ mit $n := \operatorname{grad} f \geq 1$. Zeigen Sie: $\mathfrak{G}$ ist genau dann Zerfällungskörper von f über $\mathfrak{F}$, wenn es Elemente $a, a_1, \ldots, a_n \in G$ gibt, so dass

$$f = a(x - a_1)(x - a_2) \cdots (x - a_n)$$

als Element von $\langle G[x], +, \cdot \rangle$ und $G = F(a_1, \ldots, a_n)$ [der von $F \cup \{a_1, \ldots, a_n\}$ erzeugte Unterkörper von $\mathfrak{G}$].

Aufgabe 68. Es sei $\langle \mathbf{Z}_2[x], +, \cdot \rangle$ Polynomring in einer Unbestimmten x über $\langle \mathbf{Z}_2, +, \cdot \rangle$. Zeigen Sie:

(i) $f = x^3 + x^2 + 1$ ist irreduzibel in $\langle \mathbf{Z}_2[x], +, \cdot \rangle$.

(ii) Es sei $\langle \mathbf{Z}_2(b), +, \cdot \rangle$ der von einer Wurzel b von f über $\langle \mathbf{Z}_2, +, \cdot \rangle$ erzeugte Erweiterungskörper. Dann ist $\langle \mathbf{Z}_2(b), +, \cdot \rangle$ Zerfällungskörper von f über $\langle \mathbf{Z}_2, +, \cdot \rangle$.

(iii) Ist $\langle \mathbf{Z}_2(b), +, \cdot \rangle$ zu dem Erweiterungskörper $\langle \mathbf{Z}_2(a), +, \cdot \rangle$ aus Beispiel 3.18 isomorph?

Aufgabe 69. Es sei $\langle \mathbf{Q}[x], +, \cdot \rangle$ Polynomring in einer Unbestimmten x über $\langle \mathbf{Q}, +, \cdot \rangle$, und sei

$$\omega := \frac{-1 + \sqrt{-3}}{2} \in \mathbf{C}$$

Zeigen Sie:

(i) $1, \omega, \omega^2 \in \mathbf{C}$ sind die drei komplexen Wurzeln von $x^3 - 1 \in \mathbf{Q}[x]$.

(ii) $x^3 - 1 = (x-1) \cdot (x^2 + x + 1)$ ist eine Zerlegung in ein Produkt irreduzibler Faktoren in $\langle \mathbf{Q}[x], +, \cdot \rangle$.

(iii) $\omega + 1$ ist Wurzel von $x^2 - \omega \in \mathbf{Q}(\omega)[x]$.

(iv) Setze $\sqrt{\omega} := \omega + 1$. Dann sind $\sqrt{\omega}$, $\omega \cdot \sqrt{\omega}$, $\omega^2 \cdot \sqrt{\omega} \in \mathbf{C}$ die drei komplexen Wurzeln von $x^3 + 1 \in \mathbf{Q}[x]$.

(v) $x^3 + 1 = (x+1) \cdot (x^2 - x + 1)$ ist eine Zerlegung in ein Produkt irreduzibler Faktoren in $\langle \mathbf{Q}[x], +, \cdot \rangle$.

(vi) $\mathbf{Q}(\omega) = \mathbf{Q}(\sqrt{\omega})$.

(vii) $\langle \mathbf{Q}(\omega), +, \cdot \rangle$ ist Zerfällungskörper der folgenden drei Polynome:

$$x^2 + x + 1\,,\; x^2 - x + 1\,,\; x^4 + x^2 + 1\,.$$

Ein Erweiterungskörper kann also sogar Zerfällungskörper verschiedener *irreduzibler* Polynome sein!

Aufgabe 70. Es seien $\langle \mathbf{Q}[x], +, \cdot \rangle$ und $\langle \mathbf{Q}(\sqrt{2})[x], +, \cdot \rangle$ Polynomringe in einer Unbestimmten x über $\langle \mathbf{Q}, +, \cdot \rangle$ bzw. $\langle \mathbf{Q}(\sqrt{2}), +, \cdot \rangle$. Dann ist der Zerfällungskörper von $x^2 + 1$ über $\langle \mathbf{Q}, +, \cdot \rangle$ nicht isomorph zu dem Zerfällungskörper von $x^2 + 1$ über $\langle \mathbf{Q}(\sqrt{2}), +, \cdot \rangle$.

Zusatzaufgabe 71. (*Eisenstein'sches Irreduzibilitätskriterium*) Es sei $\mathfrak{Z}$ der Polynomring in einer Unbestimmten x über $\langle \mathbf{Z}, +, \cdot \rangle$, und es sei $f \in \mathbf{Z}[x]$,

$$f = a_0 + a_1 x + \cdots + a_n x^n,$$

wobei $a_0, a_1, \ldots, a_n$ teilerfremd sind. Ist $p \in \mathbf{N}$ dann eine Primzahl und gilt $p \,|\, a_0, p \,|\, a_1, \ldots, p \,|\, a_{n-1}$, aber $p \nmid a_n$ und $p^2 \nmid a_0$, dann ist f irreduzibel in $\langle \mathbf{Z}[x], +, \cdot \rangle$.

Puzzle. Zeigen Sie, dass die folgenden Polynome irreduzibel in $\langle \mathbf{Z}[x], +, \cdot \rangle$ sind:

(i) $x^3 - 2$
(ii) $x^2 + 5x + 1$
(iii) $x^3 + 39x^2 - 4x + 8$
(iv) $3x^3 - 5x^2 + 128x + 17$
(v) $x^6 + x^3 + 1$
(vi) $x^5 - 2x^4 + 6x + 10$

Literaturverzeichnis

[1] Bosbach, B.: *Charakterisierungen von Halbgruppen mit eindeutigen Halbprimfaktorzerlegungen unter Berücksichtigung der Verbände und Ringe.* Math. Ann. **141**, (1960), 193 - 209.

[2] Bosbach, B.: *Eine Zerlegungs- und Idealtheorie für kommutative Halbgruppen.* Math. Z. **82**, (1963), 37 - 58.

[3] Bosbach, B.: *Transzendente Ringerweiterungen.* Math. Ann. **178**, (1968), 299 - 301.

[4] Bosbach, B.: *ELEMENTARIA MATHEMATICAE.* KOBRA, Universität Kassel, 2014.

[5] Burris, St. and H. P. Sankappanavar: *A Course in Universal Algebra.* Springer, New York Heidelberg Berlin, 1981.

[6] Dörge K.: *Algebra.* Scriptum, Universität Köln, 1956.

[7] Hasse H.: *Höhere Algebra,* 2 Bände, 6. bzw. 5. Auflage, de Gruyter, Sammling Göschen, Berlin 1969 bzw. 1967.

[8] Hornfeck B.: *Algebra,* 2., verbesserte Auflage, Walter de Gruyter, Berlin · New York, 1973.

[9] Krull, W.: *Elementare Algebra vom höheren Standpunkt.* de Gruyter (Sammlung Göschen) Bd. 930, Verlag Walter de Gruyter, Berlin, 1939.

[10] Reidt/Wolff/Kerst: Elemente der Mathematik, Oberstufe, Dritter Band, Hauptausgabe. G. Grote'sche Verlagsbuchhandlung / Berlin 1938.

[11] van der Waerden, B. L.: Algebra I/II., etwa 5. Auflage. Springer, Berlin-Heidelberg-New York, 1967.

Index

Ringe vom Feinsten

Bruno Bosbach
1996

Emil Artin
1898 -1962

Inhaltsverzeichnis

Vorbemerkungen

Die hier vorgelegte „Trilogie" basiert in der Reihenfolge der Kapitel auf Ergebnissen des Autors (ZPE-Ringe), von EMMY NOETHER bzw. WOLFGANG KRULL (Idealtheorie) entlang der Linien in VAN DER WAERDEN [17] und LARSEN/MC CARTHY [15], und von EMIL ARTIN (Artin'sche Ringe) entlang der Linien in DIVINSKY in [6].

Die einzelnen Kapitel sind unabhängig voneinander geschrieben und eignen sich als Seminarthemen, je nach Wahl, für HRL-Kandidaten, Gymnasial-Kandidaten, aber auch für Diplom-Aspiranten ehemaliger „Prägung".

In Kapitel 1 befassen wir uns mit $ZPE\text{-}Ringen$ das sind Ringe, in denen sich jedes Element in $Primfaktoren$ ($p \mid ab \Longrightarrow p \mid a \,\mathsf{V}\, p \mid b$) zerlegen lässt.

Bekannt ist natürlich jedem Mathematiker der Satz von Euklid, dass sich jede natürliche Zahl in $Primzahlen$ zerlegen lässt [1)]. Diese Eigenschaft besitzt die Menge der geraden ganzen Zahlen, auch bei Erweiterung um 1 nicht, denn in ihr sind z.B. $6, 10, 2, 30$ $unzerlegbar$ aber es gilt dennoch $60 = 6 \cdot 10 = 2 \cdot 30$. Andererseits wurde schon in [2] gezeigt, dass in jedem $Polynombereich$ über einem Körper $\mathfrak{K}$ die Polynome „eindeutig" in $irreduzible$ Polynome zerfallen und auch, dass der Ring $\mathfrak{Z}[i]$ der $ganzen\ Gauß'schen\ Zahlen$ ein ZPE-Ring ist, der Ring $\mathfrak{Z}[\sqrt{-5}]$ hingegen nicht, und ebenso wurde gezeigt, dass alle $Restklassenringe$ ZPE-Ringe sind. Die allgemeine Klärung der Frage, welche Bedingungen charakteristisch dafür sind, dass ein kommutativer Ring mit 1 ein ZPE-Ring ist, wird im Focus von Kapitel 1 stehen. Sie wurde vom Autor in einigen „Jugendarbeiten" geklärt und in [3] noch einmal aufgearbeitet.

Kapitel 2 geht nach einer historischen Einführung der Frage nach, unter welchen Bedingungen ein kommutativer Integritätsbereich ein $Dedekindbereich$ ist, d.h. ein Integritätsbereich, dessen $Dedekind\text{-}Ideale$ in $Primideale$ zerfallen. Dabei beschränken wir uns hier auf Bereiche statt allgemeiner Ringe, die ausführlich

[1)] Tatsächlich beweist Euklid diesen Satz nicht, sondern lediglich das Euklidische Lemma

in der Lecture Note [3] behandelt werden. Das ist die klassische Situation, die zunächst im Konkreten von RICHARD DEDEKIND und im Abstrakten dann später von EMMY NOETHER UND WOLFGANG KRULL studiert wurde und eine Flut von Nachfolgearbeiten auslöste, was hier in Anlehnung an LARSEN/MC CARTHY [15] nur aufscheinen kann.

Schließlich bringen wir in Kapitel 3 die großartige Charakterisierung der Matrizenringe über *Divisionsringen* (alternativ auch bezeichnet als *Schiefkörper*) von EMIL ARTIN, eine Symphonie der kombinatorischen elementaren nicht notwendig kommutativen Ringtheorie, ein Ergebnis, das ebenfalls zu einer Flut von Nachfolgearbeiten geführt hat.

Kapitel 1

Kommutative ZPE-Ringe

Ein kommutativer Ring heiße ein *ZPE-Ring,* wenn jedes Element diese Ringes in Primelemente zerfällt. Ziel dieses Abschnitts ist eine Antwort auf die Frage:

Was zeichnet ZPE-Ringe aus ?

Dieser Frage werden wir mit allgemein-algebraischen und idealtheoretischen Mitteln nachgehen. Wir werden die Struktur dieser Ringe zurückführen auf wohl bekannte Strukturen und sehen, dass im allgemeinen Fall exakt die t-*Hauptidealringe* dieser Bedingung genügen und im endlichen Fall diese Ringe übereinstimmen mit den d-Hauptidealringen, d.h. den Hauptidealringen im dedekindschen Sinne.

1.1 ZPE-Ringe

Alle Teilbarkeitstheorie beginnt in $\mathbf{N}$ bzw. in dem kommutativen Ring mit 1 der ganzen Zahlen, also in $(\mathbf{Z}, +, \cdot)$. Vergisst man nun alles bis auf die Eigenschaften des kommutativen Ringes, so wird die klassische Teilbarkeitslehre empfindlich gestört, aber dennoch finden sich gute Beschreibungen dieser Strukturen.

Sei im folgenden $\mathfrak{R}$ ein kommutativer Ring mit 1.

Wir nennen a einen *Teiler* von b (b ein *Vielfaches* von a) und schreiben $a \mid b$, wenn es ein x gibt mit $ax = b$.

Sind a, b aus R und gilt $c \mid a, b$ sowie $d \mid c$ für alle d, die ebenfalls a und auch b *teilen,* so nennen wir d *einen größten gemeinsamen Teiler,* kurz einen GGT

zu a und b. Besitzen a und b nur Einsteiler als gemeinsame Teiler, so heißen a und b *fremd* bzw. *teilerfremd.*

Gilt $a \mid b$ aber $b \nmid a$, also nicht $b \mid a$, so nennen wir a einen *echten Teiler* von b bzw. b ein *echtes Vielfaches* von a und schreiben $a \parallel b$. Gilt $a \mid b \ \& \ b \mid a$, so nennen wir a *äquivalent* zu b und schreiben $a \sim b$. Offenbar ist $\mid$ *transitiv* und wegen $1 \in R$ auch *reflexiv.*

$a \in R$ heißt ein *Einsteiler,* wenn $a \mid 1$ erfüllt ist. $a \in R$ heißt ein *Nullteiler,* wenn $0 = ay$ mit $y \neq 0$ erfüllt ist.

Ist a kein Nullteiler, so ist a wegen $ax = ay \Longrightarrow a(x-y) = 0 \Longrightarrow x - y = 0 \Longrightarrow x = y$ *kürzbar,* und ist a kürzbar, so ist a kein Nullteiler, wegen $ay = a0 \Longrightarrow y = 0$.

Schließlich nennen wir a und b *assoziiert,* i. Z. $a \equiv b$, falls $a = b\varepsilon$ gilt - mit $\varepsilon \mid 1$.

Es findet sich dem Anschein nach kein Lehrbuch, in dem gezeigt wird, dass die Relationen $\equiv$ und $\sim$ nicht stets identisch sind. Darauf weist IRVIN KAPLANSKY in [11] hin, wo er den Ring der stetigen reellen Funktionen als ein Beispiel herausstellt, in dem tatsächlich $\equiv \neq \sim$ erfüllt ist. Um dies einzusehen betrachte man zwei über ganz $\mathbf{R}$ stetige Funktionen f und g mit $f(-1) = -1$, $g(-1) = 1$, $f(x) = -g(x)$ für $x \leq 0$, $f(x) = g(x) = 0$ für $0 \leq x \leq 1$ und $f(x) = g(x) = x - 1$ für $1 \leq x$. Sie sind offenbar äquivalent, nicht aber assoziiert, da nach dm Zwischenwertsatz jede Funktion h mit $f \cdot h = g$ zwischen 0 und 1 zumindest einmal den Wert 0 annehmen muss, also kein Teiler der Eins (-funktion) sein kann.

1. 1. 1 LEMMA. *$\sim$ und $\equiv$ sind multiplikative Kongruenzrelationen.*

DENN: Dies folgt *geradeaus.* □

1. 1. 2 LEMMA. *Die Einsteiler von $\mathfrak{R}$ bilden eine Gruppe.*

DENN: Dies verifiziert der Leser ebenfalls *geradeaus.* □

1. 1. 3 DEFINITION. Sei $\mathfrak{S}$ ein *kommutatives Monoid.* Dann heiße

$p \in S$ *halbprim*, wenn gilt: $p \sim ab \implies p \mid a \vee p \mid b.$

$p \in S$ *prim*, wenn gilt: $p \mid ab \implies p \mid a \vee p \mid b.$

$p \in S$ *vollprim*, wenn gilt: $p^n \mid ab \implies p^n \mid a \vee p \mid b.$

$p \in S$ *irreduzibel*, wenn gilt: $a \parallel p \implies a \mid 1$

Ist p halbprim und $a \parallel p$ erfüllt, so folgt mit geeignetem $ax = p$ $(\exists x \in R)$ und folglich wegen $p + a$ auch $p = apy = pay$ $(\exists y \in R)$. Dies behalte der Leser vor Augen.

1. 1. 4 LEMMA. *$p \in R$ ist halbprim gdw. gilt*

$$a \parallel p \;\&\; b \parallel p \implies ab \parallel p\,,$$

also gdw. die Menge der echten Teiler ein Multiplikations-Monoid bildet.

DENN: Wir haben

$$\begin{aligned} a \parallel p \;\&\; b \parallel p &\implies p = asp = btp \;\; (\exists s, t \in R) \\ &\implies p = asbtp \\ &\implies p = ab.stp \;\&\; p + ab \end{aligned}$$

und gilt $a \parallel p \;\&\; b \parallel p \implies ab \parallel p$, so folgt

$$p \sim uv \implies p \,|\, u \,\mathsf{V}\, p \,|\, v\,,$$

da p sonst nicht äquivalent zu uv wäre. □

Im weiteren bezeichnen wir die Klasse von a bezüglich $\sim$ mit $\overline{a}$ und das homomorphe Bild von $(R, \cdot)$ unter $a \mapsto \overline{a}$ mit $\overline{\mathfrak{R}}$.

Man beachte: $(\overline{R}, \cdot)$ ist isomorph zum Bereich der Hauptideale $\langle a \rangle$ bezüglich $\cdot$. Offenbar gilt:

$$a \,|\, b \iff \overline{a} \,|\, \overline{b} \quad \text{und} \quad a \parallel b \iff \overline{a} \parallel \overline{b}\,.$$

Somit liefert $|$ auf $\overline{R}$ eine Partialordnung, weshalb wir auch

$$\overline{a} \leq \overline{b} \text{ statt } \overline{a} \,|\, \overline{b} \quad \text{und} \quad \overline{a} < \overline{b} \text{ statt } \overline{a} \parallel \overline{b}$$

schreiben.

Ist $\overline{c}$ ein und damit dann „der" GGT zu $\overline{a}$ und $\overline{b}$ in $\overline{\mathfrak{R}}$, so bezeichnen wir $\overline{c}$ auch mit $\overline{a} \wedge \overline{b}$. Offenbar gilt $\overline{a} \wedge \overline{b} = \overline{c}$ gdw. c ein GGT zu a und b in $\mathfrak{R}$ ist.

Klar ist ferner, dass die Eigenschaften reduzibel, halbprim, prim und vollprim von $\mathfrak{R}$ nach $\overline{\mathfrak{R}}$ und zurück mitgehen, s.o.

Ziel dieses Paragraphen ist eine Untersuchung der kommutativen Ringe mit 1, in denen jedes a in Primelemente zerfällt.

1. 1. 5 DEFINITION. $\mathfrak{R}$ heiße ein *ZPE-Ring,* wenn jedes $a \in R$ in Primelemente zerfällt.

Wir schicken einige Hilfssätze voraus. Zunächst gilt:

$$a^2 \,|\, a \;\&\; a \sim b \implies a \equiv b\,. \tag{1.1}$$

DENN: $a^2x = a \;\&\; au = b \Longrightarrow a(ax-1+axu) = b \Longrightarrow (\,) \,|\, b \,|\, a \Longrightarrow (\,) \,|\, 1.$ □

und hieraus folgt fast geradeaus

$$n > m \;\&\; a^n \,|\, a^m \implies a^m \equiv a^n\,. \tag{1.2}$$

DENN: Es gilt: $m > n \;\&\; a^m \,|\, a^n \Longrightarrow (a^n)^2 \,|\, a^n \sim a^m$ □

1. 1. 6 LEMMA. *Ist $\mathfrak{R}$ endlich, so gilt $a \sim b \Longrightarrow a \equiv b$.*

DENN: Sei $ax = b \quad \& \quad by = a$. Dann folgt $a(xy)^n x = b$, und es gilt $x^{r+1} = x^r \cdot \varepsilon \;\; (\exists r \in R)$, also auch $b = ax = a(xy)^r\varepsilon = a\varepsilon$. □

1. 1. 7 LEMMA. *Ist a nicht halbprim, so ist a zerlegbar in echte Teiler b, c.*

BEWEIS. Nach Voraussetzung existiert ein bc mit $a \sim bc \;\&\; b \parallel a \;\&\; c \parallel a$. Sei nun $a = bcd$. Ist dann $bd \parallel a$ oder $cd \parallel a$, so sind wir am Ziel.

Sonst aber gilt $a \sim cd$ und $a \sim bd$, etwa

$$\begin{array}{rcl} au = cd & \text{und} & av = bd\,, \\ & \text{also} & \\ a = bcd & = & bau = cav \\ & \rightsquigarrow & \\ a & = & cbauv \\ & = & bc \cdot a \cdot uv \\ & \sim & a^2\,. \end{array}$$

Somit haben wir $a \equiv bc$, etwa $a = b \cdot c\varepsilon$ mit $b \parallel a,\; c\varepsilon \parallel a$. □

$$p \text{ halbprim} \iff p = ab \Rightarrow p \,|\, a \,\mathsf{V}\, p \,|\, b\,. \tag{1.3}$$

DENN: Nach dem letzten Lemma ist ein a nicht halbprim gdw. a nicht die Bedingung $a = bc \Rightarrow a \,|\, b \,\mathsf{V}\, a \,|\, c$ erfüllt. □

1. 1. 8 LEMMA. *Jedes reduzible Halbprimelement ist ein Nullteiler.*

DENN: Es gilt $a \parallel p \Longrightarrow p = ay \Longrightarrow p = pax \Longrightarrow p(1-ax) = 0$ mit $ax - 1 \neq 0$, da sonst $a \,|\, 1$ erfüllt wäre. □

1. 1. 9 LEMMA. *Ist $a \parallel p$ und p halbprim, so ist a kürzbar.*

DENN: $a \parallel p \Longrightarrow p = pax$, was mit $ad = 0$ zu $p \sim ap = a(p+d) \rightsquigarrow p \,|\, p+d \rightsquigarrow p \,|\, d$, etwa $d = py$ führt. Hieraus resultiert dann $d = py = axpy = axd = 0$. □

1. 1. 10 KOROLLAR. *In einem endlichen $\mathfrak{R}$ ist jedes halbprime p irreduzibel, denn dies folgt aus der Gruppeneigenschaft der Teiler von p.*

1. 1. 11 LEMMA. *Sind p, q prim, so gilt $p \,|\, q \,\mathsf{V}\, q \,|\, p \,\mathsf{V}\, d \,|\, p, q \Longrightarrow d \,|\, 1$.*

DENN: Sei $p \dotplus q \;\&\; q \dotplus p$ und $d \,|\, p, q$. Dann folgt $d \parallel p, q$ und damit

$$\begin{aligned} p = pdx &\Longrightarrow p(1-dx) = 0 \;\; (\exists x \in R) \\ &\Longrightarrow q \,|\, 1 - dx \\ &\Longrightarrow qy + dx = 1 \\ &\Longrightarrow d \,|\, 1\,. \end{aligned}$$ □

Halbprim ist ein p also gdw. die echten Teiler von p eine kürzbare Halbgruppe bilden, irreduzibel ist ein p nach Definition gdw. die echten Teiler von p sogar eine Gruppe bilden.

Schließlich zeigen wir noch

$$1 \parallel a \parallel p \;\&\; p \; \textit{vollprim} \Longrightarrow p^2 \,|\, p\,. \tag{1.4}$$

DENN: Ist p vollprim, so folgt:

$$\begin{aligned} p^2 \dotplus p \;\&\; a \parallel p &\Longrightarrow p = pax \;\; (\exists x) \\ &\Longrightarrow p \,|\, p(1-ax) = 0 \\ &\Longrightarrow p \,|\, 1 - ax \\ &\Longrightarrow py + ax = 1 \;\; (\exists y \in R) \\ &\Longrightarrow a \,|\, 1\,. \end{aligned}$$ □

1. 1. 12 DEFINITION. Sei $\mathfrak{M}$ ein abelsches Monoid. Dann nennen wir t^* ein *Komplement* zu t (in a), wenn gilt $\overline{tt}^* = \overline{a}$ und $\overline{tt}^* = \overline{t}\overline{x} \Longrightarrow \overline{t}^* \,|\, \overline{x}$ $(\Longleftrightarrow t^* \,|\, x\,.$

1. 1. 13 LEMMA. *Ist t^* Komplement zu t, so folgt*

$$tt^* \,|\, tx \implies t^* \,|\, x\,.$$

DENN:
$$\begin{aligned} tt^* \,|\, tx &\implies tt^*y = tx \\ &\implies t(t^*y - x + t^*) = tt^* \\ &\implies t^* \,|\, x\,, \end{aligned}$$

fertig! □

1. 1. 14 DEFINITION. Ein Ring $\mathfrak{R}$ heiße *schwach kanonisch,* wenn jedes $\overline{a}$ in Halbprimfaktoren $\overline{p}_i$ zerfällt und zudem je zwei *unverkürzbare* Halbprimfaktorprodukte (kein Faktor lässt sich streichen) die gleichen Faktoren – wenn auch nicht jeweils in der gleichen Potenz – aufweisen.

1. 1. 15 LEMMA. *Sei $\mathfrak{R}$ schwachkanonisch. Dann ist jedes halbprime p sogar prim.*

BEWEIS. Zunächst sei $\overline{p} \preceq \overline{a}$ als Abkürzung für „$\overline{p}$ kommt in einer" – und damit dann in jeder – unverkürzbaren Halbprimfaktorzerlegung von $\overline{a}$ vor.

Zu zeigen ist: $p \,|\, ab \implies p \,|\, a \,\mathsf{V}\, p \,|\, b$ bzw. $\overline{p} \,|\, \overline{ab} \implies \overline{p} \,|\, \overline{a} \,\mathsf{V}\, \overline{p} \,|\, \overline{b}\,.$

(i) Gilt $\overline{p} \preceq \overline{ab}$, so sind wir am Ziel.

(ii) Gilt aber $\overline{p} \not\preceq \overline{ab}$, so folgt $\overline{p} \cdot \overline{ab} = \overline{ab}$, also $\overline{a} \cdot \overline{p} \leq \overline{a} \cdot \overline{b}$ und o. B. d. A. etwa $\overline{p} \not\leq \overline{a}$.

Das bedeutet aber $\overline{a} < \overline{ap}$ und somit $\overline{p} \preceq \overline{x}$ für alle $\overline{x}$ mit $\overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{p}$. Daher ist $\overline{p}$ Komplement zu $\overline{a}$ und folglich ein Teiler von $\overline{b}$. □

Dies liefert uns als ein erstes Hauptergebnis:

1. 1. 16 KOROLLAR. *Ein Ring $\mathfrak{R}$ ist ein ZPE-Ring gdw. er schwach kanonisch ist.*

1. 1. 17 LEMMA. *Sei $\mathfrak{R}$ ein Ring, in dem jedes $\overline{a}$ in Primelemente zerfällt. Dann ist jedes prime p sogar vollprim.*

BEWEIS. Zunächst ist im Falle $p^{m+1} \nmid p^m$ das Element $\overline{p}$ Komplement zu $\overline{p}^m$, wegen:

$$\begin{aligned} p^m p \,|\, p^m x &\implies p^m(pa - x + p) = p^m p \\ &\implies (\ ) \,\|\, p \vee p \,|\, (\ ) \\ &\implies p \,|\, (pa - x + p) \\ &\implies p \,|\, x\,. \end{aligned}$$

Sei hiernach

$$\overline{p}^n \leq \overline{a}\overline{b} \quad \& \quad \overline{p}^n \not\leq \overline{a}\,.$$

Dann ist etwa $\overline{p}^m \overline{x} = \overline{a}$ mit $\overline{p} \not\leq \overline{x}$ und $0 \leq m < n$. Das liefert uns weiter

$$\begin{aligned} \overline{p}^m \cdot \overline{p} &\leq \overline{p}^m \cdot \overline{x} \cdot \overline{b} \\ &\rightsquigarrow \\ \overline{p} &\leq \overline{x} \cdot \overline{b} \\ &\rightsquigarrow \\ \overline{p} &\leq \overline{b} \qquad (\text{wegen } \overline{p} \not\leq \overline{x})\,. \end{aligned}$$

Damit sind wir am Ziel. □

Zusammenfassend erhalten wir damit

1. 1. 18 PROPOSITION. *Sei $\mathfrak{R}$ ein Ring. Dann sind die Aussagen äquivalent:*

- (i) *$\mathfrak{R}$ ist schwach kanonisch.*
- (ii) *Jedes $a \in R$ zerfällt in Primelemente.*
- (iii) *Jedes $a \in R$ zerfällt in Vollprimelemente.*

Wir untersuchen im weiteren ZPE-Ringe auf ihre arithmetischen Besonderheiten.

1. 1. 19 LEMMA. *In ZPE-Ringen gilt:*

$$\overline{a} \leq \overline{b} \iff \overline{p}^e \leq \overline{a} \Rightarrow \overline{p}^e \leq \overline{b}\,.$$

BEWEIS. Sei $\overline{a} = \prod_1^s \overline{p}^{n_\sigma}$ eine unverkürzbare Primfaktorzerlegung und gelte die Implikation $\sigma' \neq \sigma'' \Longrightarrow \overline{p}_{\sigma'} \not\leq \overline{p}_{\sigma''}$. Dann folgt mit geeigneten x_σ $(1 \leq \sigma \leq s)$

aus der rechten Seite $\overline{b} = \overline{p}_1^{n_1} \cdot \overline{x}_1$

$= \overline{p}_1^{n_1} \cdot \overline{p}_2^{n_2} \cdot \overline{x}_2 \qquad (1.1.17),$

also auch $\overline{b} = \overline{a} \cdot \overline{x}_\sigma\,.$ □

1. 1. 20 LEMMA. *ZPE-Ringe erfüllen* $a \sim b \Longrightarrow a \equiv b$.

BEWEIS. Sind p und q prim mit $p \sim q$, so ist nichts zu zeigen, da im Falle $p^2 + p$ alle echten Teiler von p bzw. q Einsteiler sind.

Seien nun p^e und q^f zwei Primfaktorpotenzen mit $p^e \sim q^f$. Dann gilt etwa $q = p\varepsilon$ mit $\varepsilon \,|\, 1$ und wir haben im Falle $e = f$ unmittelbar $p^e \equiv p^f$ und o. B. d. A. im Falle $e < f$ mittelbar $p^e \equiv p^f$, da dann $(p^e)^2 \,|\, p^e$ erfüllt ist.

Hiernach betrachten wir den allgemeinen Fall.

Offenbar sind wir nach unseren Vorbemerkungen am Ziel, wenn wir zeigen können, dass jedes $a \in R$ eine Primfaktorzerlegung in $\mathfrak{R}$ besitzt. Dies ist aber gewährleistet nach 1.1.7 □

1.2 Eine direkte Zerlegung

Ziel dieses Abschnitts ist eine direkte Zerlegung für ZPE-Ringe. Grundlage wird dabei deren Teilbarkeitsarithmetik sein. Wesentlich beisteuern wird zu dieser Zerlegung die Existenz eines *kleinsten gemeinsamen Vielfachen* zu jedem a, b, i. Z. KGV (a, b), also eines gemeinsamen Vielfachen zu jedem Paar a, b, das alle übrigen gemeinsamen Vielfachen teilt, sowie die Existenz eines GGT zu jedem Paar a, b.

Wir wissen schon, dass je zwei Primelemente einen GGT besitzen und zeigen als nächstes, dass ganz allgemein zu je zwei Elementen aus R ein KGV und auch ein GGT existiert.

1. 2. 1 PROPOSITION. *In ZPE-Ringen besitzt jedes Paar* a, b *ein KGV und einen GGT.*

BEWEIS. Seien a, b aus R. Wir zerlegen $\overline{a}, \overline{b}$ in $\overline{R}$ und fassen gleiche Primfaktoren zu Potenzen zusammen. Sind dann

$$\overline{a} = \prod \overline{p}_\sigma^{m_\sigma} \quad \text{und} \quad \overline{b} = \prod \overline{q}_\tau^{n_\tau}$$

die eindeutig bestimmten unverkürzbaren Zerlegungen zu $\overline{a}$ bzw. $\overline{b}$, so ist das Produkt der maximalen Elemente aus

$$\{\overline{p}_1^{m_1}, \ldots, \overline{p}_s^{m_s}, \overline{q}_1^{n_1}, \ldots, \overline{q}_t^{n_t}\}$$

"das" KGV zu $\overline{a}, \overline{b}$ in $\overline{R}$ und jedes Urbild hierzu „ein" KGV zu a, b in $\mathfrak{R}$.

Hiernach lässt sich der GGT zu $\overline{a}, \overline{b}$ in $\overline{\mathfrak{R}}$ wie folgt konstruieren:

Nach 1.1.11 existiert zu je zwei Primelementen der GGT $(\overline{p}, \overline{q}) =: \overline{p} \wedge \overline{q}$.

Damit gilt aber im Falle $\overline{p} \not\leq \overline{q} \ \ \& \ \ \overline{q} \not\leq \overline{p}$

$$\overline{p}^m \wedge \overline{q}^n = \overline{p} \wedge \overline{q} \quad (\text{wegen} \quad \overline{a} < \overline{p} \Longrightarrow \overline{ap} = \overline{p})$$

und hieraus folgt

$$\text{KGV} \ \ (\overline{p}_\sigma^{m_\sigma} \wedge q_\tau^{n_\tau}) \ \tbinom{1 \leq \sigma \leq s}{1 \leq \tau \leq t} \ = \ \text{GGT} \ \ (\overline{a}, \overline{b}) =: \overline{a} \wedge \overline{b},$$

was bedeutet, dass jedes Urbild zu $\overline{a} \wedge \overline{b}$ ein GGT zu a und b in $\mathfrak{R}$ ist. □

1. 2. 2 DEFINITION. Sei $\mathfrak{R}$ ein Ring. Dann nennen wir $\mathfrak{R}$ einen *speziellen primären Ring,* wenn es ein Primelement $p \in R$ gibt, derart dass die Hauptideale $\langle p^k \rangle$ alle Ideale des Ringes ausschöpfen.

Hiernach zeigen wir

1. 2. 3 PROPOSITION. *Sei $\mathfrak{R}$ ein Ring. Dann ist $\mathfrak{R}$ genau dann ein ZPE-Ring, wenn $\mathfrak{R}$ sich direkt zerlegen lässt in eine endliche Summe von ZPE-Integritätsbereichen und speziellen Ringen.*

BEWEIS. Sei $\overline{0} = \prod \overline{p}_\sigma^{n_\sigma}$ die kanonische Zerlegung von $\overline{0}$. Dann können wir ausgehen von

$$0 \ = \ \prod p_\sigma^{n_\sigma} \quad (1 \leq \sigma \leq s)$$

mit $p_\sigma^{n_\sigma} \cdot p_\sigma = p_\sigma^{n_\sigma}$ $(1 \leq \sigma \leq s)$. Denn es gilt

$$\begin{aligned} p_\sigma^{n_\sigma} \cdot p_\sigma \,|\, p_\sigma^{n_\sigma} \ &\rightsquigarrow \ p_\sigma^{n_\sigma}(p_\sigma \varepsilon) = p_\sigma^{n_\sigma} \\ &\rightsquigarrow \ (p_\sigma \varepsilon)^{n_\sigma} \cdot (p_\sigma \varepsilon) = (p_\sigma \varepsilon)^{n_\sigma}, \end{aligned}$$

so dass wir gegebenenfalls nur p_σ durch $p_\sigma \varepsilon$ zu ersetzen haben.

Wir definieren:

$$e'_\sigma \ := \ \prod p_\sigma^{n_\sigma} \qquad (\sigma \neq \sigma').$$

Dann ist $e_1 + \ldots + e_n$ eine *orthogonale Summe,* also eine Summe, die den Gleichungen $e_i^2 = e_i\ ,\quad e_i \cdot e_j = 0\ \ (i \not\equiv j)$ genügt und der Bedingung $1 = e_1 + \ldots + e_n$.

Denn es ist $e_1 + \ldots + e_s$ idempotent und ist p ein Primteiler von $e_1 + \ldots + e_s$, so teilt p ein p_σ , also alle $e_{\sigma'}$ und damit auch e_σ , was bedeutet, dass p mindestens zwei verschiedene und daher teilerfremde p_σ teilt und folglich ein Einsteiler ist. Somit ist $\mathfrak{R}$ direkte Summe der Ideale Re_s, also

$$R \ = \ Re_1 \oplus \ldots \oplus Re_s\,.$$

Zu zeigen bleibt, dass jedes Re_σ speziell oder integer ist. Hierzu unterscheiden wir die Fälle $p_\sigma = p_\sigma^2$ und $p_\sigma \neq p_\sigma^2$.

(i) Sei $p_\sigma = p_\sigma^2$ und $ae_\sigma \cdot be_\sigma = 0$. Dann folgt $p_\sigma \,|\, ab$, also $p_\sigma \,|\, a \,\mathsf{V}\, p_\sigma \,|\, b$ und damit $ae_\sigma = 0 \,\mathsf{V}\, be_\sigma = 0$.

(ii) Sei $p_\sigma \neq p_\sigma^2$. Dann ist jeder echte Teiler von p_σ ein Einsteiler, und es liegen in Re_σ nur Elemente vom Typ be_σ mit $b \sim p_\sigma^t$.

DENN: Mit $p := p_\sigma,\ n := n_\sigma,\ e := e_\sigma$ haben wir im Falle $p \nmid a$ wegen der Irreduzibilität von p zunächst:

$$\begin{array}{rcl} \overline{a} \leq \overline{0} & = & \overline{p}^n \cdot \overline{e} \\ & \rightsquigarrow & \\ \overline{a} & = & \overline{a} \wedge q\overline{p} \cdot \overline{e} \\ & \leq & (\overline{a} \wedge \overline{p})^n (\overline{a} \wedge \overline{e}) \\ & = & \overline{a} \wedge \overline{e} \\ & \rightsquigarrow & \\ \overline{a} \cdot \overline{e} & \leq & \overline{e} \cdot \overline{e} = \overline{e} \\ & \rightsquigarrow & ae \equiv e \end{array}$$

und damit weiter im Falle $p \,|\, a$ also auch $p^m \,|\, ae \,\&\, p^{m+1} \nmid ae$ für ein geeignetes positives m aus $\mathbf{Z}$

$$\begin{array}{rcl} ae & = & p^m e \cdot x \text{ mit } p \nmid x \\ & \rightsquigarrow & x \equiv 1\,. \end{array}$$

□

Wir fragen nun nach dem Zusammenhang zwischen ZPE-Ringen $\mathfrak{R}$ und ihren *transzendenten Erweiterungen.* Hier gilt:

1. 2. 4 THEOREM. *Sei $\mathfrak{R}$ ein Ring. Dann ist $\mathfrak{R}[x]$ genau dann ein ZPE-Ring, wenn $\mathfrak{R}$ ein ZPE-Ring ist und die Implikation $a^2 = 0 \neq a \Longrightarrow a = 0$ erfüllt (das Radikal $\langle 0 \rangle$ besitzt).*

BEWEIS. (a) Gilt die Bedingung des Satzes, so ist $\mathfrak{R}$ direkte Summe von ZPE-Bereichen, und es pflanzt sich die ZPE-Eigenschaft fort von $\mathfrak{R}$ auf $\mathfrak{R}[x]$ nach C. F. Gauß.

(b) Sei hiernach $\mathfrak{R}[x]$ ein ZPE-Ring. Dann ist die aufsteigende Kettenbedingung für Hauptideale erfüllt, und es besitzt jedes $a \in R$ eine Zerlegung $a = p_i \cdot \ldots \cdot p_\sigma$ mit halbprimen $p_\sigma \ (1 \leq \sigma \leq s)$ aus $\mathfrak{R}[\mathfrak{x}]$. Beachte nun, dass Elemente a, b aus R den Implikationen genügen:

$$\begin{aligned} & a \mid_{R[x]} b \implies a \mid_R b \\ \text{und} \quad & a \sim_{R[x]} b \implies a \equiv_R b, \end{aligned}$$

wobei die zweite Zeile aus

$$(a_0 + a_1 x + \cdots + a_n x^n) \Big| 1 \implies a_0 \mid 1$$

resultiert.

Das bedeutet dann für halbprime p aus $\mathfrak{R}$ mit ZPE-Zerlegung

$$p = \prod p_i(x) \rightsquigarrow p \sim p_{j_0} \quad (\exists j \in I),$$

also auch

$$\begin{aligned} p \mid ab &\implies p_j(x) \mid a \vee p_j(x) \mid b \\ &\implies p_{j_0} \mid a \vee p_{j_0} \mid b \\ &\implies p \mid a \vee p \mid b. \end{aligned}$$

Es ist aber weiterhin jedes Primelement aus $\mathfrak{R}$ auch prim in $\mathfrak{R}[x]$, denn dies folgt aus den Regeln für das Rechnen mit Polynomen.

Denn: Gäbe es einen ersten Koeffizienten a_k in $f(x)$ und ein erstes b_ℓ in $g(x)$ mit $p \nmid a_k,\ p \nmid b_\ell$, so käme es zu $p \mid a_k \cdot b_\ell$ mit Widerspruch zu $p \mid a_i b_j \ (1 \leq i, j \leq n)$.

Somit ist die ZPE-Zerlegung aus 0 in $\mathfrak{R}$ die gleiche wie diejenige in $\mathfrak{R}[x]$.

Wäre nun $a^2 = 0 \neq a$, so gäbe es ein $p,\ n,\ e := p_\sigma,\ n_\sigma,\ e_\sigma$ mit $p^2 \nmid p$, also mit irreduziblem p.

Dann wäre aber wegen der Kürzbarkeit von ex in $\mathfrak{R}e[x]$ jeder Primfaktor von ex in $\mathfrak{R}e[x]$ kürzbar, und zudem ein Teiler von pe, also ein echter Teiler von pe wegen $(pe)^n = 0$.

Und das hieße: $xe \mid e \rightsquigarrow x \mid_R e$, ein Widerspruch! □

1.3 Idealtheoretische Charakterisierungen

1. 3. 1 LEMMA. *Sei $\mathfrak{R}$ ein ZPE-Ring. Dann haben wir*

$$\text{(D)} \qquad \overline{a} \cdot (\overline{b} \wedge \overline{c}) \;=\; \overline{a} \cdot \overline{b} \wedge \overline{a} \cdot \overline{c}\,.$$

DENN: Offenbar gilt

$$\overline{a} \cdot (\overline{b} \wedge \overline{c}) \;\leq\; \overline{a} \cdot \overline{b} \wedge \overline{a} \cdot \overline{c}\,.$$

Somit bleibt zu zeigen

$$\overline{a} \cdot \overline{b} \wedge \overline{a} \cdot \overline{c} \;\leq\; \overline{a} \cdot (\overline{b} \wedge \overline{c})\,.$$

Sei also p prim und gelte $\overline{p}^n \,|\, \overline{ab}, \overline{ac}$ sowie $\overline{p}^m \,|\, \overline{a} \;\;\&\;\; \overline{p}^{m+1} \nmid \overline{a}$. Dann muss $\overline{p}^{n-m} \,|\, \overline{b}, \overline{c}$ erfüllt sein und damit $\overline{p}^n \,|\, \overline{a} \cdot (\overline{b} \wedge \overline{c})$, also $\overline{a} \cdot \overline{b} \wedge \overline{a} \cdot \overline{c} \leq \overline{a}(\overline{b} \wedge \overline{c})$. □

1. 3. 2 LEMMA. *Sei $\mathfrak{R}$ ein ZPE-Ring. Dann erfüllt $\mathfrak{R}$ die aufsteigende Kettenbedingung für Hauptideale.*

BEWEIS. Dies ist klar für die einzelnen Komponenten der direkten Zerlegung nach den Idempotenten e_σ und folgt hieraus sofort für $\mathfrak{R}$, doch lässt sich natürlich auch, wie folgt, direkt schließen:

Wir betrachten $\overline{\mathfrak{R}}$. Gilt hier $\overline{a} \leq \overline{b}$, so sind die Primteiler von $\overline{a}$ entweder Faktoren der unverkürzbaren Primfaktorzerlegung von $\overline{b}$ oder aber echte Teiler solcher Faktoren und somit kürzbar, vgl. 1.1.9

Somit führt jede Kette $\overline{a}_1 > \overline{a}_2 > \overline{a}_3 > \ldots > \overline{a}_n \;\ldots$ schließlich zu einem $\overline{a}_e$, das nur noch irreduzible Faktoren besitzt, weshalb die betrachtete Kette nach weiteren endlich vielen Schritten abbricht.

Dem entspricht aber die aufsteigende Kettenbedingung für Hauptideale in R. □

Hiernach erklären wir

1. 3. 3 DEFINITION. Ein Ring $\mathfrak{R}$ heiße ein *GGT-Ring,* wenn in ihm zu je zwei Elementen a, b ein GGT existiert und zudem das Gesetz (D) erfüllt ist.

Damit ist jeder ZPE-Ring ein GGT-Ring.

1. 3. 4 LEMMA. *Sei $\mathfrak{R}$ ein GGT-Ring. Dann gilt*

$$\begin{array}{rcl} \overline{a} \,|\, \overline{b} \cdot \overline{c} & \& & \overline{a} \wedge \overline{b} = \overline{1} \\ & \Rightarrow & \\ \overline{a} & \leq & \overline{c}\,. \end{array}$$

DENN: Die Prämisse liefert

$$\begin{array}{rcl} \overline{a} & = & \overline{a} \wedge \overline{b} \cdot \overline{c} \\ & \leq & (\overline{a} \wedge \overline{b}) \cdot (\overline{a} \wedge \overline{c}) \\ & = & \overline{a} \wedge \overline{c}\,. \end{array}$$ □

1. 3. 5 LEMMA. *Sei $\mathfrak{R}$ ein GGT-Ring. Dann ist jedes Halbprimelement aus $\mathfrak{R}$ sogar vollprim.*

BEWEIS. Sei $\overline{p}$ halbprim und $\overline{p} \,|\, \overline{a} \cdot \overline{b}$. Dann folgt

$$\begin{array}{rcl} \overline{p} & = & \overline{p} \wedge \overline{a} \cdot \overline{b} \\ & \leq & (\overline{p} \wedge \overline{a}) \cdot (\overline{p} \wedge \overline{b})\,. \end{array}$$

Das liefert dann weiter $\overline{p} = \overline{p} \wedge \overline{a}$ oder $\overline{p} = \overline{p} \wedge \overline{b}$, da sonst $\overline{p} \leq (\overline{p} \wedge \overline{a}) \cdot (\overline{p} \wedge \overline{b}) < \overline{p}$ erfüllt wäre. Somit gilt $\overline{p} \leq \overline{a} \,\mathsf{V}\, \overline{p} \leq \overline{b}$.

Betrachten wir hiernach ein $\overline{p}^n$ mit

$$\overline{p}^n \leq \overline{a}\overline{b} \quad \& \quad \overline{p} \not\leq \overline{a}\,.$$

Dann folgt zunächst $\overline{p} \leq \overline{b}$ und damit dann weiter:

$$\begin{array}{rcl} \overline{p}^n & = & \overline{p}^n \wedge \overline{a} \cdot \overline{b} \\ & \leq & (\overline{p}^n \wedge \overline{a}^n) \cdot (\overline{p}^n \wedge \overline{b}) \\ & \leq & (\overline{p} \wedge \overline{a})^n \cdot (\overline{p}^n \wedge \overline{b}) \\ & = & \overline{p}^n \wedge \overline{b}\,. \end{array}$$ □

Ist $\mathfrak{R}$ ein *Hauptidealring,* so ist natürlich im Falle $\langle b, c\rangle = \langle g\rangle$ das Element g ein GGT zu a und b, und es gilt weiter

$$\langle a\rangle \cdot \langle b, c\rangle \;=\; \langle ab, ac\rangle\,,$$

also für die Klassen $\overline{x}$ das Gesetz (D).

Es ist in $\mathfrak{R}$ aber auch die aufsteigende Kettenbedingung für Hauptideale erfüllt, wegen

$$\begin{array}{rcl} \langle a_1\rangle \subset \langle a_2\rangle \subset \langle a_3\rangle \subset \ldots & \& & \langle\{a_i\}\rangle = \langle c\rangle \\ & \Longrightarrow & \\ c \,|\, a_i \;\; (i \in \mathbf{N}) & \& & c \in \langle a_1, \ldots, a_\ell\rangle = \langle a_\ell\rangle \\ & \rightsquigarrow & \\ \langle a_\ell\rangle & = & \langle a_{\ell+1}\rangle \cdots . \end{array}$$

Folglich ist jeder Hauptidealring ein ZPE-Ring. Wir dürfen aber natürlich nicht erwarten, dass auch umgekehrt jeder ZPE-Ring ein Hauptidealring sei. Dass dies nicht so ist, folgt u. a. aus dem Satz vonGauß, der besagt, dass sich bei Integritätsbereichen die ZPE-Eigenschaft von $\mathfrak{R}$ auf $\mathfrak{R}[x]$ überträgt.

Es lässt sich aber natürlich in $\mathbf{Z}[x, y]$ die 1 nicht linear kombinieren mittels x und y.

Daher haben wir uns um eine abgeschwächte Bedingung zu bemühen. Hierbei wird uns ein *additionsfreier* Idealbegriff zum Erfolg führen.

Neben den (üblichen) nachDedekind auch als *d-Ideale* bezeichneten Idealen spielt in der Teilbarkeitstheorie eine weitere Klasse von Idealen ein gewichtige Rolle. Wir erklären:

1. 3. 6 DEFINITION. Sei $\mathfrak{S}$ ein kommutatives Monoid. Dann heiße eine Teilmenge $\mathfrak{a}$ aus S ein v-Ideal, wenn gilt

$$(\, s \,|\, \mathfrak{a} \cdot t \Rightarrow s \,|\, c \cdot t \,) \implies c \in \mathfrak{a}\,.$$

Offenbar gehört in einem kommutativen Ring die Null zu jedem v-Ideal, deshalb ist der Durchschnitt einer Familie von v-Idealen niemals leer. Weiter erkennt man sofort, dass damit der Durchschnitt einer Familie von v-Idealen stets wieder ein v-Ideal ist. Folglich existiert zu jedem $A \subseteq R$ ein engstes A umfassendes v-Ideal $\langle A\rangle_v$. Schließlich bestätigt man

$$\langle A\rangle_v = \langle B\rangle_v \;\&\; \langle C\rangle_v = \langle D\rangle_v \implies (AC)_v = (BD)_v\,,$$

da aus der Prämisse die Äquivalenz

$$\begin{array}{rcl} s \,|\, (AB)t & \Longleftrightarrow & s \,|\, (AB')t \\ & \Longleftrightarrow & s \,|\, (A'B')t \end{array}$$

resultiert, durch die gewährleistet ist, dass sich mit v-Idealen i. w. rechnen lässt wie mit d-Idealen.

Eine Besonderheit der v-Ideale liegt natürlich darin, dass sie $additionsfrei$ definiert sind.

Ausgehend von den v-Idealen gelangt man zu den t-Idealen:

1. 3. 7 DEFINITION. Eine Teilmenge $\mathfrak{a}$ aus S heißt eine t-Ideal, wenn mit jeder endlichen Teilmenge $E \subseteq \mathfrak{a}$ auch $\langle E\rangle_v$ noch ganz in $\mathfrak{a}$ liegt.

Auch für t-Ideale gilt, dass mit jeder Familie auch ihr Durchschnitt ein t-Ideal ist, weshalb auch hier jede Teilmenge A ein eindeutig bestimmtes Erzeugnis $\langle A\rangle_t$ liefert, das sich als die mengentheoretische Vereinigung V aller $\langle a_1, \ldots, a_n\rangle_v$ $(a_i \in A)$ erweist. Denn, sind endlich viele Elemente $b_1, \ldots, b_k$ aus A gegeben, so liegt jedes von ihnen in einem $\langle A_e\rangle_t$ $(A_e \subseteq A)$ mit endlichem A_e, weshalb sie alle gemeinsam in der Vereinigungsmenge dieser von endlichen A_e erzeugten v-Ideale liegen. Also ist V ein A umfassendes t-Ideal und natürlich das engste.

Dies liefert analog zu der multiplikations-sichernden Implikation für v-Ideale

$$\langle A\rangle_t = \langle B\rangle_t \;\&\; \langle C\rangle_t = \langle D\rangle_t \implies \langle AC\rangle_t = \langle BD\rangle_t\,,$$

was dem Leser an dieser Stelle als Problem überlassen bleibe, da wir t-Ideale in diesem Abschnitt nicht multiplizieren werden.

Offenbar erfüllen v- und t-Ideale die Gleichung $\langle a\rangle_v = \langle a\rangle_t = \langle a\rangle = aS\,.$

Somit ist jeder v-$Hauptidealring$ und auch jeder t-$Hauptidealring$ ein GGT-Ring. Denn wie für d-Ideale gilt

$$(\mathrm{D}_v) \qquad \langle a\rangle_v \cdot \langle b, c\rangle_v \;=\; \langle ab, ac\rangle_v\,,$$

und damit auch hier für die Klassen $\overline{x}$ das Gesetz (D).

Nun sind wir in der Lage, ZPE-Ringe einschlägig zu charakterisieren.

1. 3. 8 Das Charakterisierungstheorem. *Ein Ring R ist genau dann ein ZPE-Ring, wenn R ein t-Hauptidealring ist.*

BEWEIS. (a) Sei $\mathfrak{R}$ ein ZPE-Ring. Dann gibt es in $\mathfrak{R}$ wegen der Kettenbedingung für Hauptideale in jedem $\langle A\rangle_t$ ein a, das in $\langle A\rangle_t$ keinen echten Teiler

besitzt, also für jedes weitere c aus R $\langle a,c\rangle_t = \langle d\rangle_t = \langle a\rangle_t \rightsquigarrow a \,|\, c$ erfüllt, wegen der Implikation $\langle d\rangle_t = \langle a,c\rangle_t \Longrightarrow \langle d \in A\rangle_t \ \& \ d \,|\, a \Longrightarrow d \sim a$.

(b) Sei nun R ein t-Hauptidealring. Dann resultiert die aufsteigende Kettenbedingung für Hauptideale wie oben, und es ist $\mathfrak{R}$ ein GGT-Ring, wie wir unter D sahen. Folglich ist $\mathfrak{R}$ in diesem Fall ein ZPE-Ring. □

Ist $\mathfrak{R}$ sogar endlich, so dürfen wir auf etwas mehr hoffen. Und – in der Tat – hier gilt sogar:

1. 3. 9 PROPOSITION. *Ein endlicher kommutativer Ring mit* 1 *ist genau dann ein ZPE-Ring, wenn er ein d-Hauptidealring ist.*

BEWEIS. (a) Ist $\mathfrak{R}$ ein beliebiger Hauptidealring, so ist $\mathfrak{R}$ auch ein ZPE-Ring, wie wir oben sahen.

(b) Sei hiernach $\mathfrak{R}$ ein ZPE-Ring. Wir zeigen $\overline{a} \wedge \overline{b} = \overline{c} \Longrightarrow \langle a,b\rangle = \langle c\rangle$. Sei hierzu

$$\overline{a} \wedge \overline{b} = \overline{c} \ \text{ mit } \ \overline{a} = \overline{c}\cdot\overline{a'},\ \overline{b} = \overline{c}\cdot\overline{b'}\,.$$

Dann dürfen wir a', b' als teilerfremd annehmen.

Denn: Nach 1.1.10 können wir in $\overline{\mathfrak{R}}$ ausgehen von unverkürzbaren Zerlegungen der Elemente $\overline{a'}, \overline{b'}$ in irreduzible Faktoren – man konsultiere 1.1.10 – und da jedes gemeinsame $\overline{p}$ zu $\overline{cp} \,|\, \overline{c} \rightsquigarrow \overline{cp} = \overline{c}$ führt, gemeinsame Faktoren sukzessive streichen, bis teilerfremde Reste zurück bleiben.

Gilt nun $a' \,|\, t1$ oder $b' \,|\, 1$, so existiert *a fortiori* eine Darstellung

$$a'x + b'y \ = \ 1\,.$$

Sonst aber gibt es ein n mit

$$(a')^{n+1} \,\Big|\, (a')^n \rightsquigarrow (a')^n(a'u) = (a')^n \rightsquigarrow (a')^n(1-a'u) = 0\,.$$

Da a' , b' teilerfremd sind, führt dies zu $b' \,|\, (1-a'u)$,also etwa zu $b'v = 1-a'u$ und damit zu

$$\begin{aligned} b'v + a'u \ &= \ 1 \\ \rightsquigarrow \qquad ca'u + cb'v \ &= \ au + bv = c, \end{aligned}$$

was $\langle a,b\rangle = \langle c\rangle$ bedeutet. Das liefert dann induktiv

$$\langle a_1,\ldots,a_n\rangle \ = \ \langle d\rangle \ \ (\exists d \in R)\,. \qquad \square$$

Kapitel 2

Dedekindbereiche

-

2.1 Zur Historie

Lange Zeit galt die Meinung, die *Idealtheorie* verdanke ihre Entstehung dem Bemühen von Ernst Eduard Kummer (1810-1893), eine Lücke zu schließen, die „seinem Beweis" der Fermatschen Vermutung auf der Grundlage von *Teilbarkeits-Annahmen* für $\mathbf{Z}[\zeta]$ mit *primitiver p-ter Einheitswurzel* ζ angehaftet habe.

Doch scheint diese Meinung, die wohl aufgekommen ist durch eine Festrede von Kurt Hensel (1861-1941), [9], heute nicht mehr haltbar.

Studiert man nämlich die mathematik-historischen Beiträge aus jüngerer Zeit, etwa die Artikel [7], [8], so ist wohl mit Sicherheit nur zu sagen, dass Kummer gewisse Probleme über höhere Reste unter Annahme eindeutiger Primfaktorzerlegungen in $\mathbf{Z}[\zeta]$ behandelte und dass er Beiträge zum Fermatschen Problem leistete, für die er einen Preis der Pariser Akademie der Wissenschaften zuerkannt bekam, obwohl, wie er selbst Liouville und Cauchy später mitteilte, seine Ausführungen noch Lücken enthielten, die zu schließen er sich „bemühe".

Ob es dann diese Bemühungen oder aber Bemühungen im Zusammenhang mit Problemen der Theorie höherer Reste waren, die letztlich die Schöpfung der *idealen komplexen Zahlen* initiierten, scheint bis heute nicht geklärt, wohingegen man weiß, dass Kummer „seine idealen Zahlen" erfolgreich einsetzte zur Bearbeitung zahlentheoretischer Probleme über höhere Reste.

Dennoch, soll es lediglich um einen Aufweis gehen, wie sich Zerlegungstheorie bei der Bearbeitung zahlentheoretischer Fragen ins Spiel bringen lässt, so eignet sich das FERMATsche Problem vorzüglich zur Demonstration.

Die entscheidende Grundidee liegt darin, Summen zu faktorisieren und hiernach die Gesetze der Teilbarkeit heranzuziehen. Dies sei kurz erläutert in Anlehnung an BOREWICZ/ŠAFAREVIČ [1].

Bekanntlich glaubte PIERRE FERMAT (Jurist, 1601-1665), einen Beweis für den „Satz" zu haben, dass

$$x^n + y^n = z^n \tag{2.1}$$

in $\mathbf{Z}$ für kein $n \geq 3$ eine nicht triviale Lösung besitze.

Gilt nun $n = m\ell$, so lässt sich (2.1) umformen zu

$$(x^m)^\ell + (y^m)^\ell = (z^m)^\ell\,, \tag{2.2}$$

was bedeutet, dass die FERMATsche Vermutung schon dann verifiziert ist, wenn man sie für 4 und alle ungeraden Primzahlen verifiziert hat.

Nun fand aber schon FERMAT selbst einen elementaren Beweis für $n = 4$, weshalb sich das Problem reduziert auf prime ungerade p.

Weiter sieht man leicht, dass es eine Lösung mit paarweise *teilerfremden* Zahlen x, y, z gibt, wenn überhaupt eine Lösung aus $\mathbf{Z}\backslash\{0\}$ existiert, da jedes t, das zwei der Zahlen x, y, z teilt, auch die dritte teilt (beachte: $t^p \mid a^p \Longrightarrow t \mid a$).

Daher bleiben zwei Fälle zu studieren, nämlich

$$(1)\quad x^p + y^p = z^p \text{ mit: } p \text{ teilt genau ein } u \in \{x, y, z\}$$

und

$$(2)\quad x^p + y^p = z^p \text{ mit: } p \text{ teilt keines der } u \in \{x, y, z\}\,.$$

Wir gehen hier nur kurz auf den ersten Fall ein, da es an dieser Stelle lediglich um eine historische Anbindung geht.

Wir beachten vorab: Ist ζ eine nicht reelle *p-te Einheitswurzel*, so durchlaufen die Potenzen $\zeta^0, \zeta^1, \ldots, \zeta^{p-1}$ alle Wurzeln von $x^p - 1$. Somit ist dann

$$z^p = \prod_0^{p-1}(x + \zeta^k y) \tag{2.3}$$

erfüllt, da die Koeffizienten des Polynoms auf der rechten Seite dem Betrage nach die gleichen sind wie die Koeffizienten von $x^p - 1$.

Es lässt sich aber unter den gemachten Voraussetzungen zeigen, dass je zwei der Faktoren $x + \zeta^k y$ in $\mathbf{Z}[\zeta]$ teilerfremd sind. Das führt dann bei Annahme der *eindeutigen Primfaktorzerlegung* zu

$$x + \zeta^k y \;=\; \varepsilon_k \alpha_k^p \tag{2.4}$$

mit $\varepsilon_k \mid 1$ und $\alpha_k \in \mathbf{Z}[\zeta]$, insbesondere also zu

$$x + \zeta y \;=\; \varepsilon_1 \alpha^p \;\; (\text{mit} \;\; \alpha = \alpha_1),$$

d. h., aus Gründen der Symmetrie auch zu

$$x - \zeta z \;=\; \varepsilon_2 \beta^p$$

und damit nach [1] *verhältnismäßig leicht* zu einem Widerspruch.

Dass die eindeutige Faktorzerlegung in $\mathbf{Z}[\zeta]$ keineswegs für jedes ζ im obigen Sinne gilt, hat als erster KUMMER selbst in [14] nachgewiesen – und zwar für $p = 23$. [1)]

Was also tun? KUMMER erkannte, dass in vielen Fällen schon weniger als die eindeutige Faktorzerlegung im unterliegenden Bereich der betrachteten Zahlen genügt, um vermutete Sachverhalte zu beweisen. Insbesondere erkannte er, dass schon eine Ausdehnung der Multiplikation vom Ausgangsbereich auf einen geeigneten *multiplikativen* Erweiterungsbereich sich als geeignetes Instrument erweist. Dies führte ihn dazu, mit *Kongruenzklassen* als *idealen komplexen Zahlen* zu operieren, und er erreichte auf diese Weise, dass nunmehr die Elemente des Ausgangsbereichs in der betrachteten multiplikativen Erweiterung eindeutig zerfielen. Nicht hingegen gewährleistete seine Methode auch die eindeutige Zerlegbarkeit der hinzu genommenen Objekte.

Dennoch, die KUMMERsche Konstruktion machte Probleme der Zahlentheorie einer Lösung zugänglich, die sich zuvor einer erfolgreichen Bearbeitung entzogen hatten. Wesentlich war es hierbei, in $\mathbf{Q}[\zeta]$, ζ *p-te Einheitswurzel*, gewisse Zahlen als *ganze Zahlen* auszuzeichnen.

Es war dann RICHARD DEDEKIND (1831-1916), der bahnbrechend zur Klärung der Teilbarkeitsverhältnisse in beliebigen algebraischen Zahlbereichen beitrug, indem er die KUMMERsche Grundidee aufgriff, und der als Vollender der nach ihm benannten Theorie, der klassischen (DEDEKINDschen) Idealtheorie,

[1)] Einen Nachweis für allgemeine ϑ werden wir im nächsten Abschnitt bringen

bezeichnet werden darf [X. Supplement zur 2. Auflage, bzw. XI. Supplement zur 3. und 4. Auflage von DIRICHLETs Vorlesungen über Zahlentheorie] [5].

Ist ζ eine p-te Einheitswurzel, so ist $\mathbf{Q}(\zeta)$ ein Zerfällunhskörper, und es liegen demzufolge mit jedem α auch alle Konjugierten zu α in $\mathbf{Q}(\zeta)$, vgl. [2].

Das bedeutet vgl. [2]: Starten wir von einem Zerfällungskörper $\mathbf{Q}(\alpha_1, ..., \alpha_n) = \mathbf{Q}[\alpha_1, ..., \alpha_n]$, über $\mathbf{Q}$, so können wir diesen nach dem Satz vom primitiven Element auffassen als ein $\mathbf{Q}[\vartheta]$. Dann ist insbesondere $\mathbf{Q}(\vartheta) = \mathbf{Q}[\vartheta]$ Zerfällungskörper über $\mathbf{Q}$ bezüglich des zu ϑ gehörenden irreduziblen Polynoms f_ϑ, und es liegen mit jedem α auch alle Konjugierten zu α in $\mathbf{Q}[\vartheta]$.

DEDEKIND fragte nun, wie sich ganz allgemein unter Einbeziehung *idealer Objekte* eine *Teilbarkeitstheorie* in Zahlbereichen $\mathbf{Q}[\vartheta]$ der soeben beschriebenen Bauart, begründen ließe.

Orientiert an der von seinem Lehrer CARL FRIEDRICH GAUSS (1777-1855) entworfenen Theorie der ganzen *komplexen Zahlen,* die ihrerseits dem *Satz von der eindeutigen Primfaktorzerlegung* genügen, untersuchte er die Frage, welche Elemente aus $\mathbf{Q}(\vartheta)$ im allgemeinsten Fall die Rolle von *ganzen Zahlen* übernehmen könnten, derart dass die ganzen rationalen Zahlen ganze Zahlen „blieben" und keine weiteren rationalen Zahlen zu ganzen Zahlen „würden".

Dass eine solche Forderung sinnvoll ist, folgt schon daraus, dass sich die Teilbarkeitsverhältnisse in $\mathbf{Z}$ über eine Erweiterung natürlich nur dann studieren lassen, wenn kein a des Ausgangsbereichs ein b des Ausgangsbereichs in der Erweiterung teilt, ohne dass dies nicht schon im Ausgangsbereich der Fall wäre.

Ferner ist eine Auszeichnung ganzer Zahlen wohl nur dann von Wert, wenn mit einer ganzen (algebraischen) Zahl auch alle ihre *konjugierten Zahlen* ganz sind, da anderenfalls (zumindest) eine nicht ganze Zahl allen rationalen Bedingungen genügen würde, denen eine andere – ihrerseits – ganze Zahl genügt.

Somit stellt sich als Minimalforderung, dass die Koeffizienten des *normierten irreduziblen* Polynoms f_α mit $f_\alpha(\alpha) = 0$ ganze rationale Zahlen seien, da die Koeffizienten *elementarsymmetrische* Werte der Konjugierten α_i $(1 \leq i \leq n)$ von α sind und $a_i = \dfrac{u_i}{v_i}$ zu $v_i \Big|_Z u_i$ führt.

Ganz müssten also zumindest alle algebraischen Zahlen „werden", die einer Beziehung der Art

$$\alpha^n = a_{n-1}\alpha^{n-1} + ... + a_1\alpha^1 + a_0 \tag{2.5}$$

genügen, man beachte $g(\alpha) = 0 \Longrightarrow f_\alpha \,|\, g$ (in $\mathbf{Z}\,[x]$), und natürlich sollte man mit ganzen algebraischen Zahlen rechnen können, ohne aus dem Bereich dieser Zahlen „herausgetragen" zu werden.

DEDEKIND konnte nun zeigen – und zwar *via* Determinanten und Moduln, dass mit α und β auch $\alpha + \beta$ und $\alpha \cdot \beta$ der Bedingung (2.5) genügen, also in unserer heutigen Sprache, dass die ganzen Zahlen im Sinne von (2.5) einen Zahlenring bilden, ja er zeigte darüber hinaus, dass α schon dann i. S. von (2.5) ganz ist, wenn α Nullstelle eines normierten Polynoms mit *ganz-algebraischen* Koeffizienten ist, was sich summarisch und modern in dem Satz ausdrückt:

Die ganzen algebraischen Zahlen bilden einen Ring $\mathfrak{G}$
und dieser ist ganz-abgeschlossen.

Ferner sieht man leicht:

Ist α *algebraisch, so gibt es ein* m*, für das* $\dfrac{\alpha}{m}$ *sogar ganz-algebraisch ist.*

Denn jede algebraische Zahl ist Nullstelle eines ganzzahligen Polynoms, also eines

$$a_0 + a_1 x + ... + a_n x^n$$

mit $a_n =: m \in \mathbf{Z}$. Daher liefert Multiplikation mit m^{n-1} ein

$$g(x) = a_0 m^{n-1} + a_1 m^{n-2}(mx) + ... + (mx)^n\,,$$

d. h. mit $g(\dfrac{\alpha}{m}) = 0$. Folglich gilt für jedes *normale algebraische* ϑ:

Der Ring aller ganz-algebraischen Zahlen aus $\mathbf{Q}\,[\vartheta]$ *ist ganz-abgeschlossen in seinem Quotientenkörper.*

DEDEKIND verzichtete auf die Forderung, dass die Erweiterung ein Zahlbereich sei und schaute nach einer Erweiterung von $(\mathbf{N}, \cdot, \,|\,)$, derart dass $a \,|\, b$ für Elemente aus $\mathbf{N}$ in dieser Erweiterung genau dann erfüllt sei, wenn $a \,|\, b$ in $\mathbf{N}$ erfüllt ist. Eine solche Erweiterung sollte vor allem eine optimale Teilbarkeitsarithmetik besitzen und dies hängt – wie man aus der klassischen Teilbarkeitslehre weiß – vor allem daran, dass zu je zwei Elementen a, b eine Linearkombination

$$ua + vb = c \text{ mit } c \,|\, a \;\;\&\;\; c \,|\, b \quad (\exists\, u, v)$$

existiert. Es war dann wohl auch diese Bedingung, die Dedekind in ganz besonderer Weise angeregt hat. Von ausgeprägtem Gespür für relevante Begrifflichkeit, entdeckte er einen Weg von historischer Bedeutung, der nicht nur

zu einer befriedigenden Lösung im Falle $\mathbf{Q}[\zeta]$, ζ *primitive p-te Einheitswurzel*, führte, sondern ganz allgemein das Problem der Teilbarkeitsverhältnisse in *Normal-Körpern* $\mathbf{Q}[\vartheta]$ unter Bezugnahme auf $\mathbf{Z}$ erschloss.

Er schuf den Begriff des *Ideals* anstelle der idealen Zahlen, indem er Zahlenmengen $\mathfrak{a}$ betrachtete, die abgeschlossen sind bezüglich $+$ und $-$ und zudem mit jedem Element x auch die Vielfachenmenge $\langle x\rangle$ dieses Elementes enthalten.

So gewann er eine Erweiterung $(\mathfrak{A}, \cdot, \supseteq)$ von $(\mathbf{N}, \cdot, |\,)$ mit

$$\begin{aligned} \langle a\rangle \cdot \langle b\rangle &= \langle ab\rangle \\ \text{und} \qquad \langle a\rangle \supseteq \langle b\rangle &\iff a \,|\, b\,, \end{aligned}$$

in der die eindeutige „Faktorzerlegung" gewährleistet ist und deren Begriffsapparat u. a. wesentlich beigetragen hat zu einer Ausdehnung der KUMMERschen Resultate zum FERMATschen Problem, vgl. BOREWICZ/ ŠAFAREVIČ.

DEDEKIND berichtete gleich dreimal über seine Theorie und zwar jeweils in den oben zitierten Supplementen, und jedesmal änderte er seinen Aufbau. Dabei stellte er in der 4. Auflage den *Gruppensatz* heraus, d. h. den Sachverhalt, dass die Gruppeneigenschaft der Halbgruppe der Moduln, die sich durch Multiplikation mit einem Element c in ein Ideal *verwandeln lassen*, zu der Implikation

$$\text{(M)} \qquad \mathfrak{a} \supseteq \mathfrak{b} \implies \mathfrak{a} \,|\, \mathfrak{b}\ .$$

Schon auf den ersten Blick erkennt der Leser, dass der DEDEKINDsche Entwurf bis hin zum Hauptsatz der Idealtheorie vorrangig algebraischer Natur ist. Da überrascht es nicht, dass DEDEKIND und WEBER 1882 in einer grundlegenden Arbeit über Funktionenkörper, [4], in der transzendenten Erweiterung $\mathbf{Q}(x)$ zu ähnlichen Resultaten gelangen wie DEDEKIND zuvor in der algebraischen Erweiterung $\mathbf{Q}(\vartheta)$ und dabei bis zum Satz von RIEMANN-ROCH vorstoßen.

2.2 Zur klassischen Idealthorie

Wir betrachten den Ring der ganzen Zahlen $a + b\sqrt{-3}$. Hier gilt

$$4 = 2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})\,,$$

und wir werden an diesem Beispiel zeigen, dass der Satz von der eindeutigen Primfaktorzerlegung schon in dieser klassischen Situation nicht gilt.

Zum Zwecke des Beweises definiert man als $Norm\ N(a+b\sqrt{-3}\ )$ den Wert a^2+3b^2. Dann gilt $N(\alpha)\cdot N(\beta)=N(\alpha\cdot\beta)$, und es hat die Zahl 4 in diesem Ring die Zerlegungen

$$4=2\cdot 2=(1+\sqrt{-3})\cdot(1-\sqrt{-3})$$

Dabei haben alle Faktoren die Norm 4. Die eigentlichen Teiler $a+b\sqrt{-3}$ dieser Faktoren hätten somit die Norm 2, da ihre Norm die Norm der Faktoren echt teilen müsste. Dies ist aber ausgeschlossen, da

$$a^2+3b^2=2$$

zu $b=0$ und damit zu $a^2=2$ führen würde, mit Widerspruch!

So stellt sich die Frage, ob es möglicherweise eine ideale eindeutige Faktorzerlegung gibt, mit der sich klassische Probleme angehen lassen – so wie es oben beschrieben wurde.

Unter welchen Bedingungen dies möglich ist, werden wir im folgenden entwickeln. Dabei präsentieren wir die klassische Idealtheorie entlang der Linien von Emmy Noether [16], in Anlehnung an Krull [12], van der Waerden [17], Larsen/McCarthy [15], und geben eine

2.3 Axiomatische Begründung

Im folgenden bezeichnen wir Strukturen stets mit großen gotischen Buchstaben, ihre Trägermengen und deren Untermengen stets mit großen lateinischen Buchstaben.

Ideale wurden in den Notizen zur Algebra abgehandelt, sie wurden dort als Untermengen von Ringen definiert. Dennoch bezeichnen wir sie der Klassik folgend mit kleinen gotischen Buchstaben. Insbesondere bedeute $\mathfrak{p}$ stets ein Primideal und $\mathfrak{o}$ stets die Menge aller Elemente aus R. Ist ein Ideal von der Menge A erzeugt, so schreiben wir (A). Wir erinnern an $(A)(B)=(AB)$. Zu ihrer Arithmetik sei – erneut – auf die Notizen zur Algebra, [2], verwiesen.

2. 3. 1 DEFINITION. Ein Integritätsbereich, kurz ein IB, heißt ein Dedekind-Bereich, kurz ein DB, wenn sich jedes Ideal darstellen lässt als Produkt von Primidealen.

Ein wesentliches Ergebnis neben den klassischen Resultaten wird sein:

2. 3. 2 THEOREM. *Genau dann ist ein IB ein DB, wenn er die Bedingung erfüllt:* $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \,|\, \mathfrak{b}$ *in Worten*

To contain is to divide

Sei im folgenden $\mathfrak{R}$ stets ein Integritätsbereich.

2.4 Ganze Elemente

In der klassischen Mathematik führten Probleme in *algebraischen Zahlkörpern* zu Teilbarkeitsfragen in $\mathbf{Z}$ bzw. $\mathbf{Z}[\zeta]$. Dabei stellte sich in natürlicher Weise die Frage, ob sich bei gegebenem

$$\mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{Q}(\alpha_1, ..., \alpha_n) = \mathbf{Q}(\alpha)$$

einen Zwischenring $\mathfrak{S}$ finden lässt, der die Teilbarkeitsbeziehungen in $\mathbf{Z}$ respektiert, also

$$a, b \in \mathbf{Z} \;\; \& \;\; a\Big|_S b \Longrightarrow a\Big|_{\mathbf{Z}} b \tag{2.7}$$

erfüllt, und darüber hinaus eine starke Teilbarkeitsarithmetik, kurz eine gute Arithmetik, besitzt. Optimal wäre in dieser Hinsicht natürlich eine Erweiterung von $\mathbf{Z}$, in der je zwei Elemente ein Hauptideal erzeugen, doch dürfen wir darauf natürlich nicht hoffen.

2. 4. 1 Wiederholung. α *heißt algebraisch über dem Körper* $\mathfrak{K}$*, wenn* α *Nullstelle eines irreduziblen Polynoms*

$$f(x) = a_0 + a_1 x + ... + x^n$$

mit $a_i \in K$ *ist. Insbesondere heißt* $\alpha \in \mathbf{C}$ *eine algebraische Zahl, wenn* α *algebraisch über* $\mathfrak{Q}$ *ist.*

Sind α und β beide algebraisch über $\mathfrak{K}$, so sind auch $\alpha \pm \beta$ und $\alpha \cdot \beta$ sowie im Falle $\beta \neq 0$ auch $\dfrac{\alpha}{\beta}$ algebraisch über $\mathfrak{K}$. Ist weiter f das zu α gehörende irreduzible Polynom und gilt neben $f(\alpha) = 0$ auch $f(\beta) = 0$, so nennt man α und β konjugiert, und es gilt $\mathbf{Q}(\alpha) \cong \mathbf{Q}(\beta)$ *via* $\mathbf{Q} \overset{id}{\longmapsto} \mathbf{Q}$ und $\alpha \to \beta$. Schließlich:

Ist $\mathfrak{A} = \mathbf{Q}(\alpha_1, ..., \alpha_n)$ mit algebraischem α_i $(1 \leq i \leq n)$, so findet sich ein ϑ mit $\mathbf{Q}(\alpha_1, ..., \alpha_n) = \mathbf{Q}(\vartheta)$ – s.o.

Schließlich sei daran erinnert, dass sich im klassischen Fall die Betrachtung jener Zahlen bewährt, die sich als Wurzel eines ganzzahligen normierten Polynoms erweisen, also der Bedingung

$$\alpha^n = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} \tag{2.8}$$

mit ganzen Zahlen genügten. Dies ist auch der Ansatz der abstrakten Idealtheorie, wie wir nun sehen werden.

2. 4. 2 DEFINITION. Sei $\mathfrak{R} \subseteq \mathfrak{S}$. Dann nennen wir $\alpha \in S$ ganz über $\mathfrak{R}$, wenn α Nullstelle eines normierten Polynoms über $\mathfrak{R}$ ist, also (2.8) mit Koeffizienten aus R genügt.

α ist also ganz über $\mathfrak{R}$, wenn α^n Linearkombination der Potenzen $1, \alpha^1, ..., \alpha^{n-1}$ ist. Dies führt uns zu dem Begriff des *Moduls*.

2. 4. 3 DEFINITION. Sei $\mathfrak{R} \subseteq \mathfrak{S}$ – wie oben. Dann nennen wir $M \subseteq S$ einen $\mathfrak{R}$-*Modul*, wenn gilt:

$$M - M \subseteq M \qquad \& \qquad RM \subseteq M \tag{MOD}$$

Man verifiziert leicht, dass sich mit Moduln operieren lässt wie mit Idealen. Weiter erkennt man, dass zu jedem $A \subseteq S$ *der von* A *erzeugte Modul*

$$[\, A \,]_R := \{\sum r_i a_i \;\Big|\; r_i \in R, a_i \in A\}$$

existiert. Demzufolge sind Moduln nichts anderes als „Vektorräume" über Skalar-Ringen (anstelle von Skalar-Körpern). .

2. 4. 4 DEFINITION. Ein Modul M heißt endlich erzeugt, wenn für mindestens ein n-tupel $M = [a_1, ..., a_n]$ erfüllt ist.

Wir sagen M erfülle den *Basissatz*, wenn nicht nur M selbst, sondern auch jeder *Untermodul* von M endlich erzeugt ist.

Hinweis. Ist M sogar ein Vektorraum, d.h. $\mathfrak{R}$ ein Körper, so ist nach den Einsichten der LinAl mit M zwangsläufig auch jeder Untermodul – hier Unterraum – endlich erzeugt, beachte $U \subseteq M \Longrightarrow \dim U \leq \dim M$. Im allgemeinen ist dies aber keineswegs selbstverständlich.

2. 4. 5 PROPOSITION. *Sei* $\mathfrak{R} \subseteq \mathfrak{S}$ *wie oben. Dann sind paarweise äquivalent:*

(i) α *ist ganz über* $\mathfrak{S}$
(ii) $\mathfrak{R}[\alpha]$ *ist ein* $[b_1, ..., b_n]_R$
(iii) *Es gilt* $\alpha \in R' \subseteq S$ *für mindestens einen endlich erzeugten Modul* R', *der sogar einenUnterring zu* $\mathfrak{S}$ *bildet.*

BEWEIS. Gilt (i), so lässt sich etwa α^n als Linearkombination der $\alpha^0, ..., \alpha^{n-1}$ darstellen. Dies pflanzt sich dann fort auf alle α^{n+k}, woraus dann $\mathfrak{R}[\alpha] = [\alpha^0, ..., \alpha^{n-1}]_R$ resultiert.

Somit gilt $(i) \Longrightarrow (ii)$, und es ist $(ii) \Longrightarrow (iii)$ evident.

Wir zeigen nun $(iii) \Longrightarrow (i)$.

Sei hierzu $\alpha \in [b_1, ..., b_n]_R$ und $[b_1, ..., b_n]_R$ zudem Unterring zu $\mathfrak{S}$. Dann folgt:

$$
\begin{array}{ccccccccc}
\alpha \cdot b_1 & = & a_{11}\, b_1 & + & a_{12}\, b_2 & + & \cdots & + & a_{1,n}\, b_n \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
\alpha \cdot b_n & = & a_{n,1}\, b_1 & + & a_{n,2}\, b_2 & + & \cdots & + & a_{n,n}\, b_n\,,
\end{array}
\tag{2.10}
$$

also im Falle eines Integritätsbereiches und $b_i \neq 0$

$$f(t) := \det(A - E\alpha) = 0.$$

mit normiertem $f(t)$.

Es gilt die Behauptung aber auch für beliebige kommutative Ringe. Hier hilft uns die Implikation weiter:

$$\sum_{j=1}^{n} a_{ij} b_{ij} = 0 \;\; (1 \leq i \leq n) \Longrightarrow (\det[a_{ij}]) b_j = 0\,. \tag{2.11}$$

DENN: Ist d_{ij} der *Kofaktor* zu a_{ij} in der Matrix $[a_{ij}]$, so folgt:

$$\sum_{j=1}^{n} (d_{ij} a_{ih}) \;=\; \begin{cases} \det[a_{ij}], & \text{falls } j = h \\ 0, & \text{falls } j \neq h. \end{cases}$$

Also gilt

$$
\begin{aligned}
d b_j &= \sum_{h=1}^{k} \left(\sum_{i=1}^{k} d_{ij} \cdot a_{ih} \right) b_h \\
&= \sum_{i=1}^{k} d_{ij} \left(\sum_{h=1}^{k} a_{ih} b_h \right) \\
&= 0\,.
\end{aligned}
$$

Das liefert – für unser Problem – $dc = 0$ für alle Elemente aus $[b_1, ..., b_n]_R$, also unter Anwendung von (2.11) auf diesen Sonderfall

$$c \cdot \det(A - Et) = 0 \tag{2.12}$$

für alle $c \in [b_1, ..., b_n]_R$ und damit auch $d = d \cdot 1 = 0$, wegen $1 \in [b_1, ..., b_n]_R$.[2]
FAZIT: Es gilt $(iii) \Longrightarrow (i)$ – auch im allgemeinen Fall. □

2. 4. 6 KOROLLAR. *Gilt $\mathfrak{R} \subseteq \mathfrak{S}$ wie oben, so bildet die Menge aller ganzen Elemente über $\mathfrak{R}$, i.Z. $G_R(S)$, einen Zwischenring.*

DENN: Sind α und β ganz über $\mathfrak{R}$, so ist β auch ganz über $\mathfrak{R}[\alpha]$, und wir haben

$$\mathfrak{R}[\alpha] = [\alpha^0, ..., \alpha^{n-1}]_R \quad \& \quad \mathfrak{R}[\beta] = [\beta^0, ..., \beta^{m-1}]_R$$

$$\Longrightarrow$$

$$\begin{aligned} \mathfrak{R}[\alpha, \beta] &= (\mathfrak{R}[\alpha])[\beta] \\ &= [\beta^0, ..., \beta^{m-1}]_{R[\alpha]} \\ &= [\alpha^0\beta^0, \alpha^0\beta^1, ..., \alpha^{n-1}\beta^{m-1}]_R \end{aligned}$$

und somit

$$\alpha + \beta, \alpha - \beta, \alpha \cdot \beta \in [\alpha^0\beta^0, \alpha^0\beta^1, ..., \alpha^{n-1}\beta^{m-1}] = \mathfrak{R}[\alpha, \beta]\,. \qquad \square$$

Der soeben konstruierte *Zwischenring* $\mathfrak{G}_R(S)$ heißt der ganze Abschluss von $\mathfrak{R}$ in $\mathfrak{S}$. Dies rührt her von dem Sachverhalt:

2. 4. 7 PROPOSITION. *Gilt $\mathfrak{R} \subseteq \mathfrak{T} \subseteq \mathfrak{S}$ und ist α ganz über $\mathfrak{T}$ und jedes $t \in T$ ganz über $\mathfrak{R}$, so ist α auch ganz über $\mathfrak{R}$.*

BEWEIS. Wie unter Korollar 2.4.6 folgt im Falle

$$\alpha^0 + b_1\alpha^1 + ... + \alpha^n = 0 \quad (b_i \in T)$$

die Gleichheit

$$\mathfrak{R}[b_1, ..., b_{n-1}, \alpha] = [c_1, ..., c_k]_R$$

mit geeignetem c_i. □

Schließlich sei für *nullteilerfreies* $\mathfrak{R}$ noch angemerkt:

[2] Unterring bedeutet stets Unterring mit der gleichen 1.

2. 4. 8 PROPOSITION. *Ist $\mathfrak{R}$ ein Integritätsbereich mit eindeutiger Faktorzerlegung* [3] *– auch bezeichnet als* GAUSS*-Ring – so ist $\mathfrak{R}$ ganz-abgeschlossen in seinem Quotientenkörper, d.h., so ist kein $\frac{a}{b}$ mit $(a,b) = 1$ ganz über $\mathfrak{R}$.*

DENN:

$$(ab^{-1})^n = c_0 + c_1(ab^{-1}) + ... + c_{n-1}(ab^{-1})^{n-1} \Longrightarrow a^n b^{-1} \in R-$$

mit Widerspruch! □

Wir haben also bislang gezeigt: Wenn es eine gute Teilbarkeitserweiterung für einen Ring $\mathfrak{R}$, im Sonderfall etwa einen Ring vom Typus $\mathfrak{Z}(\alpha)$ gibt, dann die Erweiterung $\mathfrak{G}_R(\mathfrak{Q})$ von $\mathfrak{R}$ zum Ring der ganzen Elemente aus dem Quotientenkörper von $\mathfrak{R}$ über $\mathfrak{R}$.

Es ist unser nächstes Ziel, dieses $\mathfrak{G}_R(\mathfrak{Q}) =: \mathfrak{G}$ in der klassischen Situation zu studieren, in der $R = \mathbf{Z}$, $Q = \mathbf{Q}$ und $\mathfrak{S} = \mathfrak{Q}[\alpha_1, ..., \alpha_n)] = \mathfrak{Q}(\alpha) = \mathfrak{Q}[\alpha]$ ist.

Wie wir schon sahen, vgl. 2.4.8, gilt dann $\mathbf{Q} \cap \mathbf{G} = \mathbf{Z}$, weshalb die Teilbarkeitsbeziehungen in $\mathbf{Z}$ nicht verletzt werden.

Dabei orientieren wir uns an dem abstrakten Aufbau der DEDEKINDschen Idealtheorie von EMMY NOETHER (1883-1935).

Insbesondere werden wir zunächst zeigen:

A. Ist $\mathfrak{Q}$ der Quotientenkörper zu $\mathfrak{R}$ und α_0 separabel über $\mathfrak{Q}$ und $\mathfrak{G}$ der Ring der über $\mathfrak{R}$ ganzen Elemente aus $\mathfrak{Q}(\alpha_0)$, gilt also

$$R \subseteq Q \subseteq Q(\alpha_o) \;\; \& \;\; R \subseteq G \subseteq Q(\alpha_o)$$

und ist zudem $Q \cap G = R$, so folgt:

- (i) Ist in $\mathfrak{R}$ jedes Ideal endlich erzeugt, so auch in $\mathfrak{G}$.
- (ii) Ist in $\mathfrak{R}$ jedes von O veschiedene *Primideal maximal*, so auch in $\mathfrak{G}$.
- (iii) $\mathfrak{G}$ ist ganz-abgeschlossen in seinem Quotientenkörper.

und hiernach beweisen:

B.

- (iv) Erfüllt ein Integritätsbereich die Bedingungen $(i), ..., (iii)$, so ist er ein Dedekind-Bereich.

[3] Unter anderem also etwa $\mathfrak{Z}$, $\mathfrak{K}(x)$ oder auch $\mathfrak{C}(i)$

(v) Ist $\mathfrak{R}$ ein Dedekind-Bereich, so erfüllt er die Bedingungen $(i), ..., (iii)$.

ZU A: Grundgegebenheit sei also im folgenden

$$\mathfrak{R} \subseteq \mathfrak{Q} \subseteq \mathfrak{Q}(\alpha_o) =: \mathfrak{S} \ \& \ \mathfrak{R} \subseteq \mathfrak{G} = (G_R, +, \cdot) \subseteq \mathfrak{Q}(\alpha_o) = \mathfrak{S}$$

mit $Q \cap G = R$ und separablem α über dem Quotientenkörper $\mathfrak{Q}$ von $\mathfrak{R}$.

2. 4. 9 LEMMA. *Ist α aus S, so ist α Quotient eines $g \in G$ und eines $r \in R$, also $\alpha = \frac{g}{r}$.*

DENN:

$$q_0 + q_1\alpha + ... + \alpha^n = 0$$

führt zu einem

$$r_0 + r_1\alpha + ... + r_n\alpha^n = 0\,,$$

und dies liefert nach Multiplikation mit r_n^{n-1} die Gleichheit

$$(r_0 r^{n-1}) + (r_1 r^{n-1})\alpha + ... + (r_n\alpha)^n = 0 \ \ (r_i \in R)\,.$$

Folglich ist $r_n\alpha =: g$ ganz in Bezug auf $\mathfrak{R}$, d.h. es gilt $\alpha = \frac{g}{r_n}$ mit $g \in G$ und $r_n \in R$. □

Insbesondere ist also nach 2.4.9 $\mathfrak{Q}(\alpha)$ Quotientenkörper zu $\mathfrak{G}$.

2. 4. 10 PROPOSITION. *Ist α ganz über $\mathfrak{R}$, so ist das zu α gehörende – per definitionem normierte – irreduzible Polynom f_α über $\mathfrak{Q}$ bereits aus $\mathfrak{R}[x]$.*

DENN: Es sind mit jedem α auch seine Konjugierten α_i und damit alle Koeffizienten von f_α ganz und aus Q, also aus $Q \cap G = R$. □

Hiernach kommen wir zu den zentralen Sätzen aus **A**.

2. 4. 11 Der Basissatz. *Ist* M *ein (allgemeiner) Modul*[4]*, d.h. ein „Vektorraum mit Skalaren aus einem nicht notwendig nullteilerfreien Ring", so gilt:*

[4]Wir symbolisieren Moduln mit serifenfreien Buchstaben

Erfüllt $\mathfrak{R}$ den Basissatz für alle Unterideale, und ist zudem M *endlich erzeugt, so erfüllt M den Bassissatz für (alle) Untermoduln.*

BEWEIS. Sei M $= [a_1, ..., a_n]_R$ ein endlich erzeugter $\mathfrak{R}$-Modul und gelte in $\mathfrak{R}$ der Basissatz.

Wir betrachten einen beliebigen Untermodul N von M. Dann ist nach Voraussetzung jedes a $\in N$ darstellbar als Linearkombination

$$\mathsf{a} = r_1a_1 + r_2a_2 + ... + r_na_n \ .$$

Ist hierin r_ℓ der letzte wirklich auftretende Koeffizient, so nennen wir ℓ die Länge von a.[5] Wir betrachten nun zu jedem $\ell \leq n$ die Menge $\mathcal{A}_\ell$ aller Ausdrücke von einer Länge $\leq \ell$. Diese Menge ist *operativ abgeschlossen*, bildet also einen Untermodul von N, und es bilden die ℓ-ten Koeffizienten ein endlich erzeugtes Ideal in $\mathfrak{R}$, etwa

$$(b_{\ell_1}, ..., b_{\ell_{s_\ell}})$$

Hierin ist jedes k_{ℓ_i} $(1 \leq i \leq s_\ell)$ ℓ-ter Koeffizient eines gewissen Ausdrucks

$$\mathsf{b}_{\ell_i} = r_1a_1 + ... + b_{\ell_i}a_{\ell_i} \, .$$

BEHAUPTUNG: Die so gewonnenen b_{ℓ_i} bilden eine Basis zu N.

IDEE: Den Linearkombinationen der b_{ℓ_i} entsprechen in kanonischer Weise Linearkombinationen der ℓ-ten Koeffizienten. Deshalb kann man jeden Ausdruck a der Länge ℓ durch Subtraktion einer Linearkombination $\sum_{i=1}^{\ell_{s_e}}$ in einen Ausdruck einer Länge $e \leq \ell - 1$ überführen, was sukzessive zu

$$\mathsf{a} - \sum - \sum ... = 0$$

führt. □

Wir kehren zurück zur Ausgangssituation und zeigen, dass unter den gemachten Voraussetzungen $\mathfrak{G}$ einen endlich erzeugten $\mathfrak{R}$-Modul bildet und damit insbesondere den Basissatz für Ideale erfüllt.

2. 4. 12 THEOREM. *Unter den Voraussetzungen von* **A** *überträgt sich der Basissatz von $\mathfrak{R}$ auf $\mathfrak{G}$.*

[5] Man beachte, dass es um Ausdrücke geht. Natürlich kann ein Element aus M verschiedene Darstellungen haben, doch tut dies hier nichts zur Sache.

BEWEIS. $\mathfrak{S} = \mathfrak{Q}(\alpha_o)$ kann dargestellt werden als $\mathfrak{Q}(s)$ mit $s =: s_o$. Ist nun $\mathfrak{S}$ vom Grade n über $\mathfrak{Q}$, so lässt sich jedes α darstellen in der Form

$$\alpha = \sum_{k=0}^{n-1} q_k s^k \ \ (q_k \in \mathfrak{Q}) \tag{2.13}$$

Das bedeutet im Zerfällungskörper zu f_{α_o} über $\mathfrak{S} = \mathfrak{Q}(\alpha_0)$ für die Konjugierten α_i von α

$$\alpha_i = \sum_{k=0}^{n-1} q_k s_i^k \ \ (1 \leq i \leq n) \tag{2.14}$$

Die zu diesem Gleichungssystem gehörende Determinante ist nach VANDERMONDE [6]

$$D = \det[s_i^k] = \prod_{i<j}(s_i - s_j) \ \ (i = 1, 2, ..., n-1)$$

WEITER: Das Quadrat von D ist eine symmetrische Funktion der s_ν. Folglich ist D^2 in Q enthalten.

Zur Erinnerung: Die elementarsymmetrischen Kombinationen der s_ν liefern die Koeffizienten des zu s gehörenden irreduziblen Polynoms, also liegen die Koeffizienten von D^2 als Polynomwerte der elemetar-symmetrischen Kombinationen in Q.

Da weiter die Konjugierten s_i paarweise verschieden sind – α war separabel vorausgesetzt – , ist $D \neq 0$. Daher kann man das Gleichungssystem 2.14 auflösen und erhält:

$$q_k = \frac{\sum S_{k,i}\alpha_i}{D} \ , \tag{2.15}$$

worin die $S_{k,i} = \det(S_{k,i})(-1)^{i+k}$ und D Polynomergebnisse in den s_i, also ganz in Bezug auf $\mathfrak{R}$ sind. Multiplikation dieser Gleichung mit D^2 ergibt:

$$D^2 q_k = \sum DS_{k.i}\alpha_i \tag{2.16}$$

[6] Beweis nach VANDERMONDE $\mathfrak{Q}[x_1, ..., x_n]$ ist Gauß'sch, d.h. ein IB mit eindeutiger Faktorzerlegung, und $x_i - x_j$ ist irreduzibel. Weiter sind

$$V_n := \det[x_i^k] \text{ und } \prod_{i<j}(x_i - x_j) \ \ (i = 1, 2, ..., n-1)$$

beide *homogen* vom Grade $\binom{n}{2}$. Somit ist $(x_i - x_j)$ ein Teiler von $\det[x_i^k]$ $(i = 1, ..., n\,;\, k = 0, ..., n-1)$ und also $\prod c = V_n$. Es enthalten aber beide Seiten das Glied $x_2^1 \cdot x_3^2 \cdot ... \cdot x_n^{n-1}$. Folglich ist c sogar gleich 1.

Sei nun α aus G, also ganz. Dann sind alle α_i ganz, und es ist demzufolge dann auch die rechte Seite ganz. Die linke Seite wiederum ist ein Element aus Q. Also muss $D^2 q_k =: r_k$ in R liegen. Und das bedeutet mit $q_k = r_k D^{-2}$

$$\alpha = \sum_{k=0}^{n-1} \left(r_k D^{-2}\right) s^k \tag{2.17}$$

Folglich lässt sich jedes Element aus G darstellen als Linearkombination der Elemente

$$D^{-2}s^0, D^{-2}s^1, ..., D^{-2}s^{n-1}\,,$$

weshalb

$$G \subseteq [D^{-2}s^0, D^{-2}s^1, ..., D^{-2}s^{n-1}]_R \tag{2.18}$$

erfüllt ist. Folglich gilt in $\mathfrak{G}$ der Basissatz für $\mathfrak{R}$-Moduln und damit erst recht der Basissatz für Ideale. □

Als nächstes zeigen wir

2. 4. 13 PROPOSITION. *Ist in $\mathfrak{R}$ jedes eigentliche Primideal $(\{0\} \neq \mathfrak{p} \neq \mathfrak{o})$ maximal, so gilt dies auch in $\mathfrak{G}$.*

BEWEIS. Sei $\mathfrak{p}$ ein eigentliches Primideal in $\mathfrak{G}$ und $0 \neq t \in \mathfrak{p}$. Dann gilt wegen $t \in G$ mit geeigneten $a_i \in R$ die Gleichheit

$$a_0 + a_1 t + ... + t^n = 0\,, \tag{2.19}$$

und es darf hierin $a_0 \neq 0$ angenommen werden.

Dieses a_0 ist dann aber ein R-Vielfaches von von t und damit ein Element aus $P \cap R =: B$

B wiederum ist, wie man leicht sieht, ein Primideal aus $\mathfrak{R}$ und da a_0 in B liegt ist dieses Primideal von (0) verschieden und damit maximal.

Sei hiernach $\mathfrak{aq}$ ein Oberideal von $\mathfrak{p}$ und $u \in A \setminus \mathfrak{p}$. Dann gilt mit geeigneten $b_i \in R$

$$b_0 + b_1 u + ... + u^\ell = 0 \tag{2.20}$$

und somit

$$c_0 + c_1 u + ... + u^k \equiv 0 \ \ (\text{mod } \mathfrak{p} \text{ mit } c_0 \not\equiv 0 \text{ mod } \mathfrak{p})\,, \tag{2.21}$$

also in anderer Sprechweise

$$p := c_0 + c_1 u + ... + u^k \in \mathfrak{p} \tag{2.22}$$

also wegen $c_1u + ... + u^k \in \mathfrak{a}$

$$0 \neq c_0 = p - (c_1u + ... + u^k) \in \mathfrak{a}\,.$$

Somit gehört c_0 zu $\mathfrak{a} \cap R \setminus B$, was $1 \in \mathfrak{a} \cap R$ und daher $1 \in \mathfrak{a}$, also $\mathfrak{a} = \mathfrak{o}$ bedeutet. □

ZU B. Axiomatische Begründung der Idealtheorie.

Wir zeigen zunächst: Gelten $(i), (ii), (iii)$, so ist $\mathfrak{R}$ dedekindsch. Hierbei stützen wir uns auf WOLFGANG KRULL (1900-1972), [13].

Zunächst beweisen wir, dass unter $(i), (ii), (iii)$ in $\mathfrak{R}$ der *Teilerkettensatz für Ideale* gilt. Hierzu geben wir eine Serie von Lemmata.

2. 4. 14 LEMMA. *Jedes Ideal* $\mathfrak{a}$ *umfasst ein Produkt* $\prod \mathfrak{p}_i$ *von Primidealen.*

DENN: Ist $\mathfrak{a}$ kein Primideal, so existieren zwei Elemente b, c mit $bc \in \mathfrak{a}$, aber $b, c \notin \mathfrak{a}$. Das bedeutet für die erzeugten Ideale $\mathfrak{b} := (\mathfrak{a}, b) \supset \mathfrak{a}$ und $\mathfrak{c} := (\mathfrak{a}, c) \supset \mathfrak{a}$

$$\mathfrak{b} \cdot \mathfrak{c} \subseteq \mathfrak{a} \;\;\&\;\; \mathfrak{b} \supset \mathfrak{a}\,,\; \mathfrak{c} \supset \mathfrak{a}\,.$$

Gilt nun unsere Behauptung schon für $\mathfrak{b}, \mathfrak{c}$, so sind wir fertig, sonst aber können wir das Verfahren fortsetzen, bis wir wegen der Kettenbedingung nach endlich vielen Schritten ans Ziel gelangen.

(2. Version: Gäbe es ein $\mathfrak{a}$, das der Behauptung nicht genügt, so gäbe es ein maximales.) □

2. 4. 15 LEMMA. *Ist das Ideal* $\mathfrak{p}$ *prim, so gilt:*

$$\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b} \Longrightarrow \mathfrak{p} \supseteq \mathfrak{a}\,\mathsf{V}\,\mathfrak{p} \supseteq \mathfrak{b}.$$

DENN: Anderenfalls gäbe es Elemente $a \in \mathfrak{a} \setminus \mathfrak{p}$ und $b \in \mathfrak{b} \setminus \mathfrak{p}$ mit $ab \notin \mathfrak{p}$, ein Widerspruch! □

2. 4. 16 LEMMA. *Bezeichnen wir mit* $\mathfrak{p}^{-1}$ *die Menge aller* $q \in Q$ *mit* $\mathfrak{p}q \in R$, *so bildet* $\mathfrak{p}^{-1}$ *einen Modul im Quotientenkörper zu* $\mathfrak{R}$, *und es enthält* $\mathfrak{p}^{-1}$ *mindestens ein nicht ganzes Element.*

DENN: Ist $c \neq 0$, ansonsten aber beliebig aus $\mathfrak{p}$, so gibt es mindestens ein unverkürzbares Produkt $\mathfrak{p}_1 \cdot ... \cdot \mathfrak{p}_n \supseteq (c)$ von Primidealen $\mathfrak{p}_i$ $(1 \leq i \leq n)$. Wegen $\mathfrak{p} \supseteq \mathfrak{p}_1 \cdot ... \cdot \mathfrak{p}_n$ und der Maximalität der $\mathfrak{p}_i$ muss dann aber o.B.d.A. etwa $\mathfrak{p} = \mathfrak{p}_1$, also

$$\begin{array}{rrl} & (c) & \supseteq \quad \mathfrak{p} \cdot \mathfrak{p}_2 \cdot ... \cdot \mathfrak{p}_n \\ \text{aber} & (c) & \not\supseteq \qquad \mathfrak{p}_2 \cdot ... \cdot \mathfrak{p}_n \end{array}$$

gelten. Somit gäbe es ein nicht zu (c) gehörendes Element b in $\mathfrak{p}_2 \cdot ... \cdot \mathfrak{p}_n$ mit $(c) \supseteq \mathfrak{p} \cdot (b)$, also mit $(c) \Big| \mathfrak{p} \cdot (b)$. Das bedeutet aber

$$\mathfrak{p} \cdot \frac{b}{c} \subseteq R \text{ und damit } \frac{b}{c} \in \mathfrak{p}^{-1} \text{ mit } c \nmid b. \qquad \square$$

2. 4. 17 LEMMA. *Jedes Primideal $\mathfrak{p} \neq \mathfrak{o}$ ist invertierbar, soll heißen erfüllt $\mathfrak{p} \cdot \mathfrak{p}^{-1} = (1)$.*

BEWEIS. Zunächst ist $\mathfrak{p} = \mathfrak{o} \cdot \mathfrak{p} \subseteq \mathfrak{p}^{-1} \cdot \mathfrak{p}$. Also ist das *ganze Ideal* $\mathfrak{p}\mathfrak{p}^{-1}$ gleich $\mathfrak{o}$ oder gleich $\mathfrak{p}$.

Wäre nun $\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{p}$, so würde $\mathfrak{p} \cdot (\mathfrak{p}^{-1})^n = \mathfrak{p}$ resultieren, also wäre für alle $a \in \mathfrak{p} \ \ \& \ \ b \in \mathfrak{p}^{-1}$ die Beziehung

$$ab^n \in \mathfrak{p} \subseteq R \ \ (\forall n \in \mathbf{N})$$

erfüllt. Dann ist b aber ganz, da alle Potenzen von b mit festem Nenner a dargestellt werden können – man beachte $b \in [a^{-1}]$, weshalb zusammen mit dem Modul $[a^{-1}]$ auch der $\mathfrak{R}$-Modul $[b^n]$ endlich erzeugt ist. $\square$

Hiernach sind wir in der Lage zu zeigen:

2. 4. 18 LEMMA. *Unter der Voraussetzung von $(i), (ii), (iii)$ ist jedes eigentliche Ideal $\mathfrak{a}$ eines Integritätsbereiches Produkt von Primidealen, und es ist diese Darstellung bis auf die Reihenfolge der Faktoren – im wesentlichen – eindeutig.*

DENN: Sei $\mathfrak{p}_1 \cdot ... \cdot \mathfrak{p}_n$ ein möglichst kurzes Idealprodukt unter allen $\mathfrak{p}_1 \cdot ... \cdot \mathfrak{p}_n \subseteq \mathfrak{a}$. Sei hiernach $\mathfrak{p}$ ein Primidealteiler von $\mathfrak{a}$. Dann ist o.B.d.A etwa $\mathfrak{p} = \mathfrak{p}_1$, also

$$\mathfrak{p}_2 \cdot \mathfrak{p}_3 \cdot ... \cdot \mathfrak{p}_n = \mathfrak{p}^{-1}\,\mathfrak{a}$$

mit ganzem $\mathfrak{p}^{-1}\,\mathfrak{a}$ erfüllt.

Wir können also unser Verfahren fortsetzen, bis wir zu einem Primidealprodukt minimaler Länge von der Länge 1 erreichen. Das ist aber die Bedingung (ii).

Bleibt die Eindeutigkeit der Zerlegung zu beweisen. Hier finden wir rasch zum Ziel. Sind nämlich zwei Darstellungen gegeben, so teilt jeder Faktor der einen Darstellung mindestens einen Faktor der anderen Darstellung. Wegen der Maximalität bedeutet dies weiter, dass die beiden Darstellungen die gleichen Faktoren aufweisen. Das bedeutet aber wegen der Invertierbarkeit der Primideale, dass wir sukzessive beidseitig kürzen können, bis wir schließlich zu $(1) = (1)$ gelangen. □

Als eine unmittelbare Folgerung liefert uns das letzte Ergebnis noch:

to contain is to divide

Zu zeigen bleibt der Kehrsatz, nämlich

2. 4. 19 THEOREM. *Zerfällt in einem Integritätsbereich $\mathfrak{R}$ jedes eigentliche Ideal $\mathfrak{a}$ eindeutig in Primideale, so erfüllt $\mathfrak{R}$ die drei Bedingungen $(i), (ii), (iii)$.*

BEWEIS. Die Bedingungen $(i), (ii)$ folgen fast unmittelbar aus der Eindeutigkeit der Primidealzerlegung. Die Bedingung (iii) ergibt sich wie folgt:
Sei $q = \dfrac{a}{b} \in Q$ mit $b \nmid a$ ein Quotient über $\mathfrak{R}$ und sei o.B.d.A.

$$q^n \in [q^0, ..., q^{n-1}]_R =: \mathfrak{l}\,.$$

erfüllt. Dann wäre $\mathfrak{l}^2 = \mathfrak{l}$, und wir erhielten für $[b^{n-1}] =: \mathfrak{b}$

$$\mathfrak{l} \cdot \mathfrak{b} \subseteq \mathfrak{o}\,,$$

und damit – man beachte (2.4.17):

$$\begin{array}{rrcl} & (\mathfrak{lb}) \cdot (\mathfrak{lb}) & = & (\mathfrak{lb})\mathfrak{b} \\ \rightsquigarrow & \mathfrak{l} \cdot \mathfrak{b} & = & \mathfrak{b} \\ \rightsquigarrow & \mathfrak{l} \cdot \mathfrak{b}\mathfrak{b}^{-1} & = & \mathfrak{o} \cdot \mathfrak{b}\mathfrak{b}^{-1} \\ \rightsquigarrow & \mathfrak{l} & = & \mathfrak{o} \end{array}$$

also $q \in R$ mit Widerspruch zu $b \nmid a$. □

2. 4. 20 PROPOSITION. *Ist $\mathfrak{R}$ ein IB, in dem jedes eigentliche Primideal invertierbar ist, so ist $\mathfrak{R}$ ein Dedekind-Bereich.*

BEWEIS. Ist $\mathfrak{p}$ invertierbar, so folgt

$$\mathfrak{p} \cdot \mathfrak{p}^{-1} = (1) \Longrightarrow \mathfrak{p} \cdot \mathfrak{p}^{-1}(b) = (b)\,,$$

also $\mathfrak{p} \supseteq (b) \Longrightarrow \mathfrak{p} \,|\, (b)$ und damit die Implikation

$$\mathfrak{p} \supseteq \mathfrak{a} \Longrightarrow \mathfrak{p} \,|\, \mathfrak{a}\,.$$

Hieraus folgt zunächst, dass jedes eigentliche Primideal maximal ist. Denn, ist $\mathfrak{p}$ ein eigentliches Primideal und $\mathfrak{q}$ ein $\mathfrak{p}$ echt umfassendes Primideal, so folgt:

$$\mathfrak{q} \supset \mathfrak{p} \Longrightarrow \mathfrak{q}\mathfrak{x} = \mathfrak{p} \Longrightarrow \mathfrak{q}\mathfrak{p} = \mathfrak{p} \Longrightarrow \mathfrak{q} = \mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}\,.$$

Weiter erhalten wir für jedes eigentliche Primideal $\mathfrak{p}$ die Implikation

$$\mathfrak{p}^n \supseteq \mathfrak{a} \cdot \mathfrak{b} \;\;\&\;\; \mathfrak{p} \not\supseteq \mathfrak{b} \Longrightarrow \mathfrak{p}^n \supseteq \mathfrak{a}\,. \tag{2.23}$$

DENN:

$$\mathfrak{p} \,|\, \mathfrak{a}\mathfrak{b} \;\;\&\;\; \mathfrak{p} + \mathfrak{b} \Longrightarrow \mathfrak{p} \,|\, \mathfrak{a} \Longrightarrow \mathfrak{p}^{-1}\mathfrak{a} \quad \text{ist ein Ideal}\,, \tag{2.24}$$

was zusammen mit (2.23) zunächst zu

$$\mathfrak{p}^{n-1} \supseteq (\mathfrak{p}^{-1}\mathfrak{a}) \cdot \mathfrak{b} \;\;\&\;\; \mathfrak{p} \not\supseteq \mathfrak{b} \tag{2.25}$$

und demzufolge nach n-facher Wiederholung zu (2.23) führt.

Als unmittelbare Folge von (2.23) erhalten wir, dass mit dem eigentlichen Primideal $\mathfrak{p}$ auch $\sum_1^\infty \mathfrak{p}^n$ prim ist und damit gleich dem 0-Ideal.

DENN: Man bestätigt nach (2.23) sofort die Primeigenschaft von $\sum_1^\infty \mathfrak{p}^n$, also muss $\sum_1^\infty \mathfrak{p}^n = (0)$ erfüllt sein, da jedes eigentliche Primideal maximal ist. Das bedeutet insbesondere:

$$\mathfrak{p}^n \supseteq \mathfrak{b} \;\; (\forall n \in \mathbf{N}) \Longrightarrow \mathfrak{b} = (0). \tag{2.26}$$

Hiernach können wir zeigen:

$$\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \,|\, \mathfrak{b}\,. \tag{2.27}$$

Sei hierzu $\mathfrak{a} \supseteq \mathfrak{b} \;\;\&\;\; \mathfrak{b} \neq (0)$ erfüllt – im Falle $\mathfrak{b} = (0)$ ist nichts zu zeigen. Dann gilt $\mathfrak{b} \supseteq \mathfrak{a}(\mathfrak{b} : \mathfrak{a}) =: \mathfrak{c}$. Wäre nun $\mathfrak{c} \neq \mathfrak{a}(\mathfrak{b} : \mathfrak{a})$, so hätten wir $\mathfrak{a}(\mathfrak{b} : \mathfrak{a}) :$

$\mathfrak{c} \neq \mathfrak{e}$, also für ein geeignetes $\mathfrak{p}$ die Beziehung $\mathfrak{p} \mid \mathfrak{a}(\mathfrak{b} : \mathfrak{a}) : \mathfrak{c}$ und daher $\mathfrak{a}((\mathfrak{b} : \mathfrak{a}) \cdot \mathfrak{p}^{-1}) \subseteq \mathfrak{c}$, also $(\mathfrak{a}(\mathfrak{b} : \mathfrak{a})) \cdot \mathfrak{p} = \mathfrak{a}(\mathfrak{b} : \mathfrak{a}) \Longrightarrow \mathfrak{p}^n \mid \mathfrak{a}(\mathfrak{b} : \mathfrak{a}) \Longrightarrow \mathfrak{a}(\mathfrak{b} : \mathfrak{a}) = (0)$ mit Widerspruch zu $\mathfrak{a} \neq (0) \neq (\mathfrak{b} : \mathfrak{a})$!

Insbesondere folgt aus (2.27) die Kürzungsregel:

$$\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{c} \Longrightarrow \mathfrak{b} = \mathfrak{c}\,, \tag{2.28}$$

denn es ist ja jedes (b) kürzbar.

Endlich gilt der Basissatz, denn haben wir $\mathfrak{a} \supseteq (c)$ so folgt $\mathfrak{a} \cdot \mathfrak{b} = (c)$, und es gilt $c = a_1b_1 + ... + a_nb_n$ für geeignete a_i, b_i, also auch $(a_1, ..., a_n) \cdot \mathfrak{b} = (c) = \mathfrak{a} \cdot \mathfrak{b}$ und damit nach (2.28) die Gleichheit $\mathfrak{a} = (a_1, ..., a_n)$. □

SCHLIESSLICH bringen wir den Klassiker

2. 4. 21 THEOREM. *Ein Integritätsbereich ist schon dann ein Dedekind-Bereich, wenn jedes Ideal in Primideale zerfällt.*

BEWEIS. Sei $\mathfrak{p} \neq (0)$ prim und $0 \neq c \in \mathfrak{p}$. Dann ist $(c) = \mathfrak{p}_1 \cdot ... \cdot \mathfrak{p}_m$, und es ist jedes $\mathfrak{p}_i$ invertierbar, da (c) invertierbar ist.

Weiter haben wir $\mathfrak{p} \supseteq \mathfrak{p}_\mathfrak{i}$ für mindestens ein i. Folglich sind wir am Ziel, wenn wir zeigen können, dass jedes invertierbare Primideal maximal ist. Sei also $\mathfrak{p}$ prim und invertierbar. Wir zeigen

$$a \notin \mathfrak{p} \Longrightarrow \mathfrak{p} + (a) = \mathfrak{o}$$

Annahme:

$$a \notin \mathfrak{p} \Longrightarrow \mathfrak{p} + (a) \neq \mathfrak{o} \tag{2.29}$$

Dann folgt

$$\mathfrak{p} + (a) = \mathfrak{p}_1 \cdot ... \cdot \mathfrak{p}_m \tag{2.30}$$

$$\mathfrak{p} + (a)^2 = \mathfrak{q}_1 \cdot ... \cdot \mathfrak{q}_n \tag{2.31}$$

mit geeigneten *Primidealen* $\mathfrak{p}_i, \mathfrak{q}_j$ $(1 \leq i \leq m, 1 \leq j \leq n)$, die ihrerseits $\mathfrak{p}$ umfassen, und es gilt

$$\mathfrak{p} + (a) \supseteq \mathfrak{p} + (a)^2\,. \tag{2.32}$$

Das liefert in $\mathfrak{R}/\mathfrak{p} =: \mathfrak{R}'$ *via* $\mathfrak{p}_i/\mathfrak{p} =: \mathfrak{p}_i'$, $\mathfrak{q}_j/\mathfrak{p} =: \mathfrak{q}_j'$ $(a)/\mathfrak{p} = (a')$ und $(a)^2/\mathfrak{p} = (a')^2$

$$(a') = \mathfrak{p}_1' \cdot ... \cdot \mathfrak{p}_m' \tag{2.33}$$

$$(a')^2 = \mathfrak{q}_1' \cdot ... \cdot \mathfrak{q}_n' \tag{2.34}$$

mit invertierbaren $\mathfrak{p}'_i$, $\mathfrak{q}'_j$ – beachte: (a') ist invertierbar. Somit gilt

$$\mathfrak{p}'_1{}^2 \cdot \ldots \cdot \mathfrak{p}'_m{}^2 = \mathfrak{q}'_1 \cdot \ldots \cdot \mathfrak{q}'_n\,, \tag{2.35}$$

denn es kann keins der $\mathfrak{p}_i, \mathfrak{q}_j$ auf $\mathfrak{o}$ übergehen, da sonst o.B.d.A.

$$\begin{aligned} 1' \in \mathfrak{p}'_1 \;&\rightsquigarrow\; 1 - p_1 \in \mathfrak{p} \supseteq \mathfrak{p}_1 \;\; (p_1 \in \mathfrak{p}_1) \\ &\rightsquigarrow\; 1 - p_1 \in \mathfrak{p}_1 \\ &\rightsquigarrow\; 1 \in \mathfrak{p}_1 \end{aligned}$$

erfüllt wäre. Daher dürfen wir $n = 2m$ und $\mathfrak{q}_{2i-1} = \mathfrak{q}_{2i} = \mathfrak{p}_i$ annehmen, also

$$(\mathfrak{p} + (a))^2 = \mathfrak{p} + (a)^2 = \mathfrak{p}^2 + \mathfrak{p} \cdot (a) + (a)^2\,, \tag{2.36}$$

weshalb jedes $b \in \mathfrak{p}$ eine Darstellung

$$b = c + da$$

mit $c \in \mathfrak{p}^2$ und $d \in \mathfrak{p}$ besitzt, man beachte $b, c \in \mathfrak{p} \;\;\&\;\; a \notin \mathfrak{p}$.

Daher gilt weiter

$$\mathfrak{p} \subseteq \mathfrak{p}^2 + \mathfrak{p} \cdot (a)\,. \tag{2.37}$$

Nun ist $\mathfrak{p}$ aber nach Voraussetzung invertierbar, was unsere Annahme (2.29), nämlich $\mathfrak{p} + (a) \neq \mathfrak{o}$ zu einem Widerspruch führt, *via*:

$$\mathfrak{o} = \mathfrak{p} \cdot \mathfrak{p}^{-1} \subseteq \mathfrak{p}^2 \cdot \mathfrak{p}^{-1} + \mathfrak{p} \cdot (a) \cdot \mathfrak{p}(a) \cdot \mathfrak{p}^{-1} = \mathfrak{p} + (a)\,. \qquad \square$$

2.5 Ordnungstheoretische Kriterien

In diesem Abschnitt lehnen wir uns an Larsen/McCarthy, [15], an und verweisen auf die dortigen Quellen–Angaben.

Bevor wir weitere Charakterisierungen des Dedekind-Bereiches geben, stellen wir ein auf Krull zurückgehendes außerordentlich bedeutsames Instrument der kommutativen Idealtheorie heraus.

2. 5. 1 DEFINITION. Sei $\mathfrak{R}$ ein IB, $\mathfrak{Q}$ sein *Quotientenkörper* und $\mathfrak{p}$ ein eigentliches Primideal. Dann bezeichnen wir mit $\mathfrak{R}_\mathfrak{p}$ den Ring aller Quotienten $\frac{r}{s}$ mit $r \in \mathfrak{o}$ und $s \notin \mathfrak{p}$, und es bedeute analog $\mathfrak{a}_\mathfrak{p}$ das Ideal aller $\frac{a}{s}$ mit $a \in \mathfrak{a}$ und $s \notin \mathfrak{p}$.

Es wird also durch den Operator $_{\mathfrak{p}}$ jedem Ideal $\mathfrak{a}$ aus $\mathfrak{R}$ ein $\mathfrak{a}_{\mathfrak{p}}$ aus $\mathfrak{R}_{\mathfrak{p}}$ zugeordnet, und man verifiziert leicht die Gleichheit $(\mathfrak{a}_{\mathfrak{p}} \cap \mathfrak{o})_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}}$, weshalb es in $\mathfrak{R}_{\mathfrak{p}}$ keine anderen Ideale gibt als die $\mathfrak{a}_{\mathfrak{p}}$.

Die große Bedeutung des Ringes $\mathfrak{R}_{\mathfrak{p}}$ liegt in zwei Fakten, die wir sogleich beweisen wollen.

2. 5. 2 THEOREM. *Wird $\mathfrak{R}_{\mathfrak{p}}$ gewählt wie oben, so gelten:*

(a) $$(\mathfrak{a} \cdot \mathfrak{b})_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}} \cdot \mathfrak{b}_{\mathfrak{p}}$$

(b) $$(\mathfrak{a} \cap \mathfrak{b})_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}} \cap \mathfrak{b}_{\mathfrak{p}}$$

(c) $$(\mathfrak{a} + \mathfrak{b})_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}} + \mathfrak{b}_{\mathfrak{p}}$$

(d) $$(\mathfrak{a} : \mathfrak{b})_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}} : \mathfrak{b}_{\mathfrak{p}}$$

BEWEIS. Der Beweis darf für $(a), (b), (c)$ dem Leser überlassen bleiben. Für (d) ergibt er sich wie folgt:

Zunächst gilt stets $(\mathfrak{a} : \mathfrak{b})_{\mathfrak{p}} \subseteq \mathfrak{a}_{\mathfrak{p}} : \mathfrak{b}_{\mathfrak{p}}$ vermöge der Implikationskette:

$$\begin{aligned} x \in \mathfrak{a} : \mathfrak{b} &\implies \mathfrak{b}x \subseteq \mathfrak{a} \\ &\implies \mathfrak{b}_{\mathfrak{p}}x \subseteq \mathfrak{a}_{\mathfrak{p}} \\ &\implies \mathfrak{b}_{\mathfrak{p}}\tfrac{x}{s} \subseteq \mathfrak{a}_{\mathfrak{p}} \ \ (\forall s \notin \mathfrak{p}) \\ &\implies \tfrac{x}{s} \in \mathfrak{a}_{\mathfrak{p}} : \mathfrak{b}_{\mathfrak{p}} \\ &\implies (\mathfrak{a} : \mathfrak{b})_{\mathfrak{p}} \subseteq \mathfrak{a}_{\mathfrak{p}} : \mathfrak{b}_{\mathfrak{p}} \end{aligned}$$

Sodann erhalten wir für endlich erzeugte $\mathfrak{b}$, also $\mathfrak{b}$ vom Typ $(b_1, ...b_m)$, auch die Beziehung $\mathfrak{a}_{\mathfrak{p}} : \mathfrak{b}_{\mathfrak{p}} \subseteq (\mathfrak{a} : \mathfrak{b})_{\mathfrak{p}}$ wegen der Implikationskette:

$$\begin{aligned} x \in \mathfrak{a}_{\mathfrak{p}} : \mathfrak{b}_{\mathfrak{p}} &\implies \mathfrak{b}_{\mathfrak{p}}x \subseteq \mathfrak{a}_{\mathfrak{p}} \\ &\implies b_1 x = \tfrac{a_1}{s} \\ &\ \ \& \quad b_2 x = \tfrac{a_2}{s} \\ &\ \ \vdots \\ &\ \ \& \quad b_m x = \tfrac{a_m}{s} \\ &\implies b_j x s = a_j \ \ (1 \leq j \leq m) \\ &\implies \mathfrak{b}xs \subseteq \mathfrak{a} \\ &\implies xs \in \mathfrak{a} : \mathfrak{b} \\ &\implies x \in (\mathfrak{a} : \mathfrak{b})_{\mathfrak{p}} \end{aligned}$$

□

Aus 2.5.2 folgt fast unmittelbar

2. 5. 3 Das Krull'sche Lokalisierungstheorem. *Zwei Ideale* $\mathfrak{a}, \mathfrak{b}$ *aus* $\mathfrak{R}$ *sind genau dann gleich, wenn für alle maximalen Ideale* $\mathfrak{p}$ *die Gleichheit* $\mathfrak{a}_\mathfrak{p} = \mathfrak{b}_\mathfrak{p}$ *erfüllt ist.*

BEWEIS. Sei $a \in \mathfrak{a}$. Dann liegt $\frac{a}{1}$ in jedem $\mathfrak{a}_\mathfrak{p}$ mit maximalem $\mathfrak{p}$. Folglich gibt es für ein jedes maximale $\mathfrak{p}$ aus $\mathfrak{R}$ ein $r_p \notin \mathfrak{p}$ mit $ar_p \in \mathfrak{b}$. Ist nun $\mathfrak{c}$ das von all diesen r_p erzeugte Ideal, so gilt $\mathfrak{c} = \mathfrak{o}$ oder es gäbe nach dem Zornschen Lemma unter den $\mathfrak{c}$ umfassenden Idealen ein maximales $\mathfrak{m}$. Dieser zweite Fall kann aber – nach Konstruktion – nicht eintreten. Wir haben also $\mathfrak{c} = \mathfrak{o}$ und damit $1 \in \mathfrak{c}$, d.h. wir hätten

$$1 = x_1 r_{p_1} + ... + x_n r_{p_n} \tag{2.38}$$

mit $r_{p_i} \notin \mathfrak{p}_i$ ($\mathfrak{p}_i$ maximal) und $x_i \in R$. Und das würde liefern

$$a = x_1(r_{p_1}a) + ... + x_n(r_{p_n}a) \in \mathfrak{b}\,, \tag{2.39}$$

also $\mathfrak{a} \subseteq \mathfrak{b}$ und aus Gründen der Dualität auch $\mathfrak{b} \subseteq \mathfrak{a}$ und damit in der Tat insgesamt $\mathfrak{a} = \mathfrak{b}$. □

Nun können wir beweisen:

2. 5. 4 Das Charakterisierungstheorem. *In einem noetherschen Integritätsbereich sind die Bedingungen äquivalent:*

(1) $\mathfrak{R}$ *ist ein Dedekind-Bereich.*

(2) *Jedes* (a, b) *ist invertierbar.*

(3) $\mathfrak{a} \neq (0) \Longrightarrow \mathfrak{ab} = \mathfrak{ac} \Longrightarrow \mathfrak{b} = \mathfrak{c}\,.$

(4) *Ist* $\mathfrak{p}$ *maximal, so gilt* $(a)_\mathfrak{p} \supseteq (b)_\mathfrak{p} \vee (b)_\mathfrak{p} \subseteq (a)_\mathfrak{p}$

(5) $\mathfrak{a}(\mathfrak{b} \cap \mathfrak{c}) = \mathfrak{ab} \cap \mathfrak{ac}$

(6) $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$

(7) $(\mathfrak{a} + \mathfrak{b}) : \mathfrak{c} = \mathfrak{a} : \mathfrak{c} + \mathfrak{b} : \mathfrak{c}$

(8) $\mathfrak{a} : \mathfrak{b} + \mathfrak{b} : \mathfrak{a} = \mathfrak{o}$

(9) $\mathfrak{a} : (\mathfrak{b} \cap \mathfrak{c}) = \mathfrak{a} : \mathfrak{c} + \mathfrak{b} : \mathfrak{c}$

(10) $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c})$

BEWEIS. Wir führen den Beweis über die beiden Ringschlüsse

$$(\mathbf{1}) \Longrightarrow (\mathbf{2}) \Longrightarrow (\mathbf{3}) \Longrightarrow (\mathbf{4}) \Longrightarrow (\mathbf{5}) \Longrightarrow (\mathbf{6}) \Longrightarrow (\mathbf{2}) \Longrightarrow (\mathbf{1})$$

und

$$(\mathbf{4}) \Longrightarrow (\mathbf{7}) \Longrightarrow (\mathbf{8}) \Longrightarrow (\mathbf{9}) \Longrightarrow (\mathbf{10}) \Longrightarrow (\mathbf{4})$$

AUF DENN:

Zunächst zu

$$(\mathbf{1}) \Longrightarrow (\mathbf{2}) \Longrightarrow (\mathbf{3}) \Longrightarrow (\mathbf{4}) \Longrightarrow (\mathbf{5}) \Longrightarrow (\mathbf{6}) \Longrightarrow (\mathbf{2}) \Longrightarrow (\mathbf{1})$$

$(\mathbf{1}) \Longrightarrow (\mathbf{2})$: Siehe oben.

$(\mathbf{2}) \Longrightarrow (\mathbf{3})$: Gilt $(\mathbf{2})$, so ist jedes Ideal $\mathfrak{c}$ invertierbar. Ist nämlich der Satz richtig für $2 \leq n-1$ und $\mathfrak{c} = (c_1, ..., c_n)$, so erhalten wir mit

$$\begin{array}{rclcrcl} \mathfrak{a} & = & (c_1, ..., c_{n-1}) & , & \mathfrak{b} & = & (c_2, ..., c_n) \\ \mathfrak{d} & = & (c_1, c_n) & , & \mathfrak{c}' & = & (c_1)\mathfrak{a}^{-1})\mathfrak{d}^{-1} + (c_n)\mathfrak{a}^{-1}\,\mathfrak{d}^{-1} \end{array}$$

die Gleichungskette:

$$\begin{array}{rcl} \mathfrak{c}\mathfrak{c}' & = & (\mathfrak{a} + (c_n))(c_1)\mathfrak{a}^{-1}\,\mathfrak{d}^{-1} + ((c_1) + \mathfrak{b})(c_n)\mathfrak{b}^{-1}\,\mathfrak{d}^{-1} \\ & = & (c_1)\mathfrak{d}^{-1} + (c_n c_1)\mathfrak{a}^{-1}\,\mathfrak{d}^{-1} + (c_1 c_n)\mathfrak{b}^{-1}\,\mathfrak{d}^{-1} + (c_n)\mathfrak{d}^{-1} \\ & = & (c_1)\mathfrak{d}^{-1}\,(\mathfrak{o} + (c_n)\mathfrak{b}^{-1}) + (c_n)\mathfrak{d}^{-1}\,(\mathfrak{o} + (c_1)\mathfrak{a}^{-1}) \\ & = & ((c_1) + (c_n))\mathfrak{d}^{-1} \\ & = & \mathfrak{d}\mathfrak{d}^{-1} \\ & = & (1). \end{array}$$

$(\mathbf{3}) \Longrightarrow (\mathbf{4})$: Denn, zunächst gilt im Falle $\mathfrak{a} \neq (0)$ die Implikation $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{c} \Longrightarrow \mathfrak{b} \subseteq \mathfrak{c}$, wegen $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{c} \Longrightarrow \mathfrak{a}\mathfrak{b} = \mathfrak{a}(\mathfrak{b} + \mathfrak{c}) \overset{(3)}{\Longrightarrow} \mathfrak{b} = \mathfrak{b} + \mathfrak{c}$.

Sei nun $a \neq 0 \neq b$. Dann folgt

$$\begin{array}{rcrcl} & & (a,b)\cdot(a,b) & \subseteq & (a^2, b^2)(a,b) \\ \rightsquigarrow & & (a,b) & \subseteq & (a^2, b^2) \\ \rightsquigarrow & & ab & = & xa^2 + yb^2 \;\; (\exists x, y) \end{array}$$

Somit haben wir

$$\begin{array}{rcrcl} & & (yb)(a,b) & \subseteq & (a)(a,b) \\ \rightsquigarrow & & (yb) & \subseteq & (a) \\ \rightsquigarrow & & yb & = & au \;\; (\exists u) \\ \rightsquigarrow & & a & = & b \cdot \dfrac{y}{u} \end{array}$$

und demzufolge

$$\begin{aligned} ab &= xa^2 + uab \\ \rightsquigarrow\ xa^2 &= ab(1-u) \\ \rightsquigarrow\ b &= a \cdot \frac{x}{1-u} \end{aligned}$$

Dies liefert aber für $u \notin \mathfrak{p}$ die Gleichheit $a = b\frac{y}{u} \in (b)_\mathfrak{p}$, und gilt $u \in \mathfrak{p}$, so folgt $1-u \notin \mathfrak{p}$, also $b = a \cdot \frac{x}{1-u} \in (a)_\mathfrak{p}$.

Und das bedeutet $(a)_\mathfrak{p} \subseteq (b)_\mathfrak{p}\,\mathsf{V}\,(b)_\mathfrak{p} \subseteq (a)_\mathfrak{p}$, also in der Tat die Implikation $(\mathbf{4})$.

$(\mathbf{4}) \Longrightarrow (\mathbf{5})$: Ist $\mathfrak{R}$ ein beliebiger *Bewertungsbereich*, d.h. ein IB mit der Eigenschaft $\forall a, b\ \exists x, y : ax = b\,\mathsf{V}\,by = a$, so erfüllen alle $x = \frac{a}{b}$ des Quotientenkörpers die Disjunktion $x \in R\ \mathsf{V}\ x^{-1} \in R$.

Sei nun $\mathfrak{a} \not\subseteq \mathfrak{b}$ und $a \in \mathfrak{a}$, aber $a \notin \mathfrak{b}$ erfüllt. Dann liegen alle $\frac{b}{a}$ $(a, b \in R)$ in R wegen der Implikation

$$\frac{a}{b} \in R \Longrightarrow b \cdot \frac{a}{b} = a \in R \Longrightarrow (a) \subseteq (b) \subseteq \mathfrak{b}\,.$$

Daher sind alle $b \in \mathfrak{b}$ vom Typ ax und somit aus $\mathfrak{a}$.

$(\mathbf{5}) \Longrightarrow (\mathbf{6})$, denn gilt $(\mathbf{5})$, so folgt

$$\begin{aligned} (\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b}) &= (\mathfrak{a}+\mathfrak{b})\mathfrak{a} \cap (\mathfrak{a}+\mathfrak{b})\mathfrak{b} \\ &\supseteq \mathfrak{a}\mathfrak{b} \\ &\supseteq \mathfrak{a}(\mathfrak{a}\cap\mathfrak{b}) + \mathfrak{b}(\mathfrak{a}\cap\mathfrak{b}) \\ &\supseteq (\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b}\,, \end{aligned}$$

also Bedingung $(\mathbf{6})$.

Schließlich erhalten wir

$(\mathbf{6}) \Longrightarrow (\mathbf{2}) \Longrightarrow (\mathbf{1})$, denn sei $\mathfrak{c} = (c_1, c_2$ mit $c_1 \neq 0 \neq c_2)$. Wir setzen $\mathfrak{a} = (c_1)$ und $\mathfrak{b} = (c_2)$. Dann folgt

$$\mathfrak{c}(\mathfrak{a}\cap\mathfrak{b})\mathfrak{b}^{-1}\,\mathfrak{a}^{-1} = (\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b})\mathfrak{b}^{-1}\,\mathfrak{a}^{-1} = \mathfrak{a}\mathfrak{b}\mathfrak{b}^{-1}\,\mathfrak{a}^{-1} = \mathfrak{o}\,,$$

also $(\mathbf{2})$.

Es zeigte sich aber unter $(\mathbf{2}) \Longrightarrow (\mathbf{3})$, dass mit den 2-erzeugten Idealen alle Ideale – eines Noether-Bereiches – invertierbar sind.

Nun gilt in $\mathfrak{R}$ – wegen der Noethereigenschaft – die aufsteigende Kettenbedingung für Ideale, d.h. wir finden bei vorgegebenem $\mathfrak{a}$ ein eigentliches Primideal

$\mathfrak{p}$ mit $\mathfrak{p}\mathfrak{a}_1 = \mathfrak{a}$, also mit $\mathfrak{a}_1 \supset \mathfrak{a}$, da anderenfalls $(1) \cdot \mathfrak{a} = \mathfrak{p} \cdot \mathfrak{a}$, also wegen der Invertierbarkeit $\mathfrak{p} = (1)$ sein müsste mit Widerspruch!

Daher gelangen wir bei sukzessiver Fortsetzung zu einer Primidealzerlegung von $\mathfrak{a}$, und diese ist bis auf die Reihenfolge der Faktoren eindeutig – wegen der Invertierbarkeit aller (Prim-) Ideale.

Hiernach kommen wir zu

$$(\mathbf{4}) \Longrightarrow (\mathbf{7}) \Longrightarrow (\mathbf{8}) \Longrightarrow (\mathbf{9}) \Longrightarrow (\mathbf{10}) \Longrightarrow (\mathbf{4})$$

$(\mathbf{4}) \Longrightarrow (\mathbf{7})$, denn $(\mathbf{4})$ gilt in jedem $\mathfrak{R}_\mathfrak{p}$.

$(\mathbf{7}) \Longrightarrow (\mathbf{8})$, denn

$$\begin{aligned} \mathfrak{a} : \mathfrak{b} + \mathfrak{b} : \mathfrak{a} &= \mathfrak{a} : (\mathfrak{a} + \mathfrak{b}) + \mathfrak{b} : (\mathfrak{a} + \mathfrak{b}) \\ &\overset{(7)}{=} (\mathfrak{a} + \mathfrak{b}) : (\mathfrak{a} + \mathfrak{b}) \\ &= (1) \end{aligned}$$

$(\mathbf{8}) \Longrightarrow (\mathbf{9})$, denn

$$\begin{aligned} (\mathfrak{a} : \mathfrak{b} + \mathfrak{a} : \mathfrak{c}) : (\mathfrak{a} : (\mathfrak{b} \cap \mathfrak{c})) &\supseteq (\mathfrak{a} : \mathfrak{b}) : (\mathfrak{a} : (\mathfrak{b} \cap \mathfrak{c})) \\ &+ (\mathfrak{a} : \mathfrak{c}) : (\mathfrak{a} : (\mathfrak{b} \cap \mathfrak{c})) \\ &\supseteq (\mathfrak{a} : (\mathfrak{a} : (\mathfrak{b} \cap \mathfrak{c}))) : \mathfrak{b} \\ &+ (a : (a : (b \cap c))) : c \\ &\supseteq \mathfrak{c} : \mathfrak{b} + \mathfrak{b} : \mathfrak{c} \\ &\overset{(8)}{=} \mathfrak{o} \qquad (= (1) \end{aligned}$$

$(\mathbf{9}) \Longrightarrow (\mathbf{10})$, denn

$$\begin{aligned} & ((\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{c}) : ((\mathfrak{a} + \mathfrak{c}) \cap (\mathfrak{b} + \mathfrak{c})) \\ \overset{(9)}{=} & ((\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{c}) : (\mathfrak{a} + \mathfrak{c}) + ((\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{c}) : (\mathfrak{b} + \mathfrak{c}) \\ \supseteq & (\mathfrak{a} \cap \mathfrak{b}) : \mathfrak{a} + (\mathfrak{a} \cap \mathfrak{b}) : \mathfrak{b} \\ \overset{(9)}{=} & (\mathfrak{a} \cap \mathfrak{b}) : (\mathfrak{a} \cap \mathfrak{b}) \\ = & \mathfrak{o}\,, \end{aligned}$$

also gilt

$$(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{c} \supseteq (\mathfrak{a} + \mathfrak{c}) \cap (\mathfrak{b} + \mathfrak{c})\,.$$

Es ist aber stets

$$(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{c} \subseteq (\mathfrak{a} + \mathfrak{c}) \cap (\mathfrak{b} + \mathfrak{c})$$

erfüllt.

Das liefert uns insgesamt die Bedingung $(\mathbf{10})$.

$(\mathbf{10}) \Longrightarrow (\mathbf{4})$: Sei $\mathfrak{p}$ ein eigentliches Primideal und seien a, b aus R. Dann folgt nach $(\mathbf{9})$

$$\begin{aligned}(a) &= (a) \cap (b + (a - b)) \\ &= ((a) \cap (b)) + ((a) \cap (a - b))\end{aligned}$$

Sei hiernach $a = t + c(a - b)$ mit $t \in (a) \cap (b)$. Dann gilt $c(a - b) \in (a)$, und es folgt:

$$c \cdot b \in (a) \quad \text{und} \quad (1 - c) \cdot a = t - cb \in (b)\,.$$

Das bedeutet aber $b \in (a)_{\mathfrak{p}}$, falls $c \notin \mathfrak{p}$, und $a \in (b)_{\mathfrak{p}}$, falls $c \in \mathfrak{p}$ und damit $1 - c \notin \mathfrak{p}$. Somit erhalten wir

$$(a)_{\mathfrak{p}} \supseteq (b)_{\mathfrak{p}} \quad \mathsf{V} \quad (b)_{\mathfrak{p}} \supseteq (a)_{\mathfrak{p}}$$

also, wie gewünscht, die Bedingung $(\mathbf{4})$. □

Kapitel 3

DCC-Ringe

3.1 Nil und nilpotent

3. 1. 1 DEFINITION. Sei $\mathfrak{R}$ [1] ein Ring. Dann heißt $x \in R$ *nilpotent,* wenn mindestens eine Potenz x^n verschwindet und damit natürlich auch alle weiteren Potenzen x^{n+k} von x verschwinden.

Der Ring $\mathfrak{R}$ selbst heißt *nil,* wenn jedes $x \in R$ nilpotent ist.

Sind I, J zwei *Unterringe* von R, so meinen wir mit $I \cdot J$ die Menge aller $\sum i_m j_m \ (i_m, j_m \in I \times J)$. Insbesondere können wir damit reden von R^2 und somit sukzessive auch von $R^s \ (s \in \mathbf{N})$.

Wir sagen nun, der $\mathfrak{R}$ sei nilpotent, wenn für mindestens ein $n \in \mathbf{N}$ $R^n = 0$ erfüllt ist.

Klar, ist ein Ring nilpotent, so ist er erst recht nil. Das Umgekehrte ist falsch, wie wir bald sehen werden.

Im weiteren werden wir einen nilen Ring auch einen Nilring.

Offenbar gilt:

3. 1. 2 LEMMA. *Mit $\mathfrak{R}$ ist auch jeder Unterring von $\mathfrak{R}$ und ebenso jedes homomorphe Bild von $\mathfrak{R}$ ein Nilring*

Weiterhin ist mit jedem Ideal I auch jedes $\mathfrak{R}/I$ ein Nilring.

3. 1. 3 LEMMA. *Jede Summe von zwei Nilidealen aus $\mathfrak{R}$ ist ein Nilideal.*

[1] Wir versuchen in diesem Kapitel konsequent zu trennen zwischen den auftretenden Strukturen und ihren Trägermengen. Genauer: wir werden Mengen mit großen lateinischen Buchstaben notieren und Strukturen mit den korrespondierenden Frakturbuchstaben.

BEWEIS. ÜBUNG □

Das bedeutet:

3. 1. 4 PROPOSITION. *Jede endliche Summe von Nilidealen aus* $\mathfrak{R}$ *ist ein Nilideal.*

Und hieraus folgt

3. 1. 5 PROPOSITION. *Die Vereinigung* W *aller Nilideale von* $\mathfrak{R}$ *ist ein Nilideal.*

Wie man leicht sieht gelten die Aussagen 3.1.2 bis 3.1.4 auch für die Verschärfung nil→nilpotent, nicht aber wird sich auch 3.1.5 verschärfen lassen. Allerdings gilt, wie man leicht sieht:

3. 1. 6 PROPOSITION. *Die Vereinigung* V *aller nilpotenten Ideale ist ein Nilideal.*

BEWEIS. ÜBUNG □

Ein Ring, der nil ist, nicht aber nilpotent, lässt sich wie folgt konstruieren:

3. 1. 7 BEISPIEL. *Wir ordnen jedem* x *des Einheitsintervalls* $\mathbf{E}$ *ein Element* α_x *zu und definieren*

$$x_\alpha \odot x_\beta := \begin{cases} x_{\alpha+\beta}, & \textit{falls} \quad \alpha+\beta < 1 \\ 0, & \textit{falls} \quad \alpha+\beta \geq 1 \end{cases}$$

Hiernach „operieren wir auf natürliche Weise" mit der Menge aller endlichen Summen $\sum a_\alpha x_\alpha$ *bezüglich Komponenten-Multiplikation* $(a_\alpha x_\alpha)\cdot(b_\beta x_\beta)$ $:= (a_\alpha b_\beta)(x_\alpha \odot x_\beta)$.

3.2 Die DCCL-Bedingung

Von nun an sei $\mathfrak{R}$ stets ein DCCL-Ring , d.h. ein Ring mit absteigender Kettenbedingung für seine Links-Ideale. Das bedeutet natürlich, dass jede Menge von Linksidealen ein minimales enthält.

Das nachfolgende Theorem wird zeigen, dass in solchen Ringen die Bedingungen „nil" und „nilpotent" gleichwertig sind.

Vorweg: $e \in R$ heiße im weiteren idempotent, wenn es nicht verschwindet, d.h. verschieden ist non 0 und zudem $e^2 = e$ erfüllt.

3. 2. 1 PROPOSITION. *In einem DCCL-Ring ist jedes nile Linksideal L sogar nilpotent und besitzt zudem ein idempotentes Element.*

BEWEIS. Betrachte alle nicht nilpotenten Linksideale, die enthalten sind in L. Unter ihnen existiert ein minimales, sag' L_1. Dann ist aber auch L_1^2 nicht nilpotent und also gleich L_1. Es mögen andere Linksideale enthalten sein in L_1, aber, wenn sie echt enthalten sind in L_1, müssen sie nilpotent sein.

Wir betrachten nun die Menge aller Linksideale I, die enthalten sind in L_1 und zudem $L_1 I \neq 0$ erfüllen. Zum Beispiel L_1 selbst ist ein solches I. Die Menge dieser I enthält ein minimales I_1. Damit haben wir dann $L_1 I_1 \neq 0$ und folglich auch ein $e_1 \in I_1$, derart dass $L_1 e_1 \neq 0$ erfüllt ist. Es ist aber $L_1 e_1$ ein Linksideal, enthalten in I_1 und es gilt $L_1 \cdot L_1 e_1 \neq 0$. Das bedeutet $L_1 e_1 = I_1$, beachte: I_1 war minimal gewählt. Demzufolge existiert ein $e_2 \in L_1$ mit $e_2 e_1 = e_1$. Somit ist auch $e_2^n e_1 = e_1$, weshalb e_2 nicht nilpotent und L daher nicht nil ist.

Zu konstruieren bleibt ein Idempotentes $e \in L$. Klar ist sofort $(e_2^2 - e_2)e_1 = 0$, und es folgt hieraus, dass die Menge J der Elemente $x \in L_1$ mit $xe_1 = 0$ ein in L_1 enhaltenes Linksideal von $\mathfrak{R}$ ist. Also ist J nilpotent und da $e^2 - e_2^2$ in J liegt, ist $e^2 - e_2^2$ nilpotent. Sei nun $x := e^2 - e_2^2$ und $x^n = 0$. Wir definieren $e_3 := e_2 + x - 2e_2 x$. Dann ist e_3 nicht nilpotent, da sonst auch $e_2 = e_3 - x + 2e_2 x$ nilpotent wäre, wie oben gezeigt. (Beachte, dass e_2 und auch e_3 mit x kommutieren.) Jedoch $e_3^2 - e_3 = 4x^3 - 3x^2 = x_1$ ist nilpotent mit $x_1^{n_1} = 0 \quad \& \quad n_1 < n$. Hiernach bilden wir $e_4 := e_3 + x_1 - 2e_3 x_1$ und fahren nach dieser Methode fort bis wir nach endlich vielen Schritten zu einem $e_n =: e$ gelangen, das nicht nilpotent ist und $(e^2 - e)^1 = 0$ erfüllt, also $e^2 = e$. □

Als nächstes zeigen wir

3. 2. 2 PROPOSITION. *Sei $\mathfrak{R}$ ein beliebiger Ring. Dann enthält die Vereinigung alle nilpotenten Ideale auch alle nilpotenten Linksideale und alle nilpotenten Rechtsideale.*

BEWEIS. Aus Gründen der Dualität dürfen wir uns auf Rechtsideale beschränken. Sei also J ein nilpotentes Rechtsideal. Dann ist $J + RJ$ ein zwei-

seitiges Ideal, und es gilt natürlich $(J + RJ)^1 \subseteq J^1 + (RJ)^1$. Ferner erhalten wir

$$\begin{aligned} & (J + RJ)^n \subseteq J^n + (RJ)^n \\ \Longrightarrow\ & (J + RJ)^{n+1} \subseteq (J^n + (RJ)^n)(J + RJ) \subseteq J^{n+1} + (RJ)^{n+1} \end{aligned}$$

und damit induktiv

$$(J + RJ)^m \subseteq J^n + (RJ)^m \ \ (\forall m \in \mathbf{N}).$$

Nun war J nilpotent gewählt, also ist auch $J + RJ$ nilpotent und es ist J enthalten in diesem nilpotenten Ideal und damit erst recht in der Vereinigung aller nilpotenten Ideale. □

3.3 Ideale in halbeinfachen DCCL-Ringen

Ein Ring heiße hier *halbeinfach* wenn sein Nil-Radikal gleich 0 ist. Sei im folgenden $\mathfrak{R}$ stets ein halbeinfacher DCCL-Ring . Dann erhalten wir

3. 3. 1 LEMMA. *Jedes Linksideal L aus $\mathfrak{R}$ ist vom Typ Re mit idempotentem e.*

BEWEIS. Dies ist klar für das 0-Ideal. Sei jetzt L verschieden vom Nullideal. Dann ist L nicht nil, da alle Nil-Linksideale im Nilradikal liegen, das hier degeneriert. Also enthält L nach 3.2.1 ein Idempotentes e. Sei nun M_e die Menge aller $x \in L$ mit $xe = 0$. Dies ist ein Linksideal. Es mögen viele Idempotente in L liegen und zu jedem gehört natürlich ein korrespondierendes M_e. Sei unser M_e schon ein minimales unter ihnen. Ist M_e ein Nichtnullideal, so enthält es ein Idempotentes, sag' e_1, das dann $e_1 e = 0$ erfüllt. Wir definieren $e' := e - ee_1 + e_1$. Dann folgt $e'e' = e'$. Gilt nun $M_e \neq 0$, so ist auch $e_1 \neq 0$ und damit auch $e' \neq 0$, da sonst $e_1 e' = 0 = e_1^2 = e_1$ erfüllt wäre. Es ist also e' ein von 0 verschiedenes Idempotentes und $e'e = ee = e$. Daher annuliert alles, was e' von links annuliert auch e von links. Und das bedeutet $M_{e'} \subseteq M_e$. Es ist aber $e_1 e = 0$, während $e_1 e' e_1 e_1 \neq 0$ erfüllt ist. Und das bedeutet, dass sogar $M_{e'} \subset M_e$ erfüllt ist. Das aber widerspricht der Minimalität von M_e, weshalb eines der M_e gleich 0 gewesen sein muss, also unser M_e als 0 angenommen werden darf. Ist dann aber x aus L, so folgt$(x - te)e = 0$, also $x = xe$ und

damit dann $L = Le$. Und das liefert dann weiter $L = Le \subseteq Re \subseteq L$, also $L = Re$. □

3. 3. 2 PROPOSITION. *Jedes zweiseitige Nichtnullideal I von $\mathfrak{R}$ erfüllt $Re = eR$, worin e ein eindeutig bestimmtes Einheitselement von I ist.*

BEWEIS. Da I insbesondere eine Linksideal ist, folgt $I = Re$ nach Lemma 3.3.1. Sei nun V die Menge der Elemente $x \in I$ mit $ex = 0$. Dann ist V ein Rechtsideal von $\mathfrak{R}$. Nun ist $eV = 0$ während $Ve = V$ ist, und das liefert $V^2 = Ve \ \& \ V = 0$. Also ist V ein nilpotentes Rechtsideal. Wir wissen aber, dass $\mathfrak{R}$ keine nilpotenten Rechtsideale hat. Somit ist $V = 0$. Sei nun $x \in I$. Dann folgt $e(x - ex) = 0$ mit $x - ex \in V$ und also $x = ex \ (\forall x \in I)$. Daher ist $I = Re = eR$ und damit e eine Einheit in I. Und diese Einheit ist eindeutig, da für jede Einheit e' aus I die Gleichung $e = ee' = e'$ erfüllt ist. □

3. 3. 3 KOROLLAR. *Jeder halbeinfache DCCL-Ring besitzt ein Einselement.*

BEWEIS. R ist *zweiseitiges Ideal* aus $\mathfrak{R}$. □

Unter dem *Zentrum eines Ringes* versteht man die Menge der Elemente x mit $xy = yx$. Ein Element x heißt *zentral,* wenn es zum Zentrum gehört.

3. 3. 4 LEMMA. *Ein idempotentes Element aus $\mathfrak{R}$ ist zentral, wenn es Einheit eines Ideals aus $\mathfrak{R}$ ist.*

BEWEIS. Wenn ein Idempotentes zentral ist, gilt $Re = eR$, und es ist e natürlich Einheit zu eRe. Und, ist umgekehrt $eR = Re$ ein Ideal, so liegen alle xe und alle ex in diesem Ideal, woraus dann $ex = ex \cdot e = e \cdot ex = xe$ resultiert, weshalb e dann zentral ist. □

Im allgemeinen ist ein Ideal I des Ideals J von $\mathfrak{R}$, aufgefasst als Ring $\mathfrak{J}$, nicht wieder ein Ideal von $\mathfrak{R}$. Daher mögen Eigenschaften, die allen Idealen von $\mathfrak{R}$ zu eigen sind, Idealen der Ideale fehlen.

JEDOCH: Für die spezielle Klasse derjenigen Ringe, die wir jetzt studieren wollen, nämlich die Klasse der halbeinfachen DCCL-Ringe, gilt:

3. 3. 5 PROPOSITION. *Sei $I = Re = eR$ ein Ideal aus $\mathfrak{R}$. Dann ist auch jedes Links-, Rechts-, zweiseitige Ideal von $\mathfrak{I}$ ein Links-, Rechts-, zweiseitiges Ideal aus $\mathfrak{R}$.*

BEWEIS. Ist L ein Linksideal von I, so folgt $L = Le$ und $RL = Re \cdot L = IL \subseteq L$, weshalb L ein Linksideal von $\mathfrak{R}$ ist. Der Rest folgt analog. □

3. 3. 6 KOROLLAR. *Ist I ein Ideal aus $\mathfrak{R}$, so ist $\mathfrak{I}$ ein DCCL-Ring .*

3. 3. 7 KOROLLAR. *Mit $\mathfrak{R}$ ist auch jedes Ideal aus $\mathfrak{R}$ halbeinfach.*
Problem Man zeige, dass in jedem beliebigen Ring ein Idempotentes genau dann zentral ist, wenn es mit allen Idempotenten kommutiert.

3.4 Direkte Summen

Sind $\mathfrak{A}$ und $\mathfrak{B}$ zwei Unterringe von $\mathfrak{R}$, so mag es sein, dass R sich auffassen lässt als Summe $A + B$, was meint, dass jedes $x \in R$ von der Form $x = a + b$ sei. Eindeutig müsste diese Darstellung aber nicht sein. In diesem Falle hilft die Darstellbarkeit uns nicht wirklich weiter. Anders jedoch verhält es sich, wenn die Darstellung eindeutig ist. In diesem Falle gehen die Strukturmerkmale der beiden Unterringe deutlicher ein in die Struktur von $\mathfrak{R}$.

Wie schon bekannt aus der LinAl lässt sich die Überprüfung der Eindeutigkeit stark reduzieren, denn es genügt auch hier, dass sich die 0 eindeutig darstellen lasse.

BEWEIS. Übung.

Entsprechend haben wir auch hier ein zweites Kriterium, nämlich $R = A + B$ ist eindeutig genau dann, wenn $A + B = R$ ist und $A \cap B = 0$.

BEWEIS. Übung.

Gilt $A + B = R$ und $A \cap B = 0$, so sagt man R sei *supplementäre Summe* der Unterringe A und B. Entsprechend definieren wir

3. 4. 1 DEFINITION. $\mathfrak{R}$ heißt supplementäre Summe der Unterringe $A_1, A_2, \ldots, A_n$, wenn gilt

$$R = A_1 + A_2 + \ldots + A_n \tag{3.1}$$

$$0 = \sum a_i \ (a_i \in A_i) \Longrightarrow a_i = 0 \ (\forall 1 \leq i \leq n) \tag{3.2}$$

Supplementäre Summen sind gut, für uns aber noch nicht gut genug. Denn noch haben wir ja keine Forderung mit Blick auf die Multiplikation gestellt. Hier haben wir noch eine weitere Chance der Strukturprägung. Fordern wir nämlich, dass $A_i \cdot A_j = 0 \ \ (i \neq j)$ sei, so bedeutet dies natürlich eine Einengung, und wir sehen sofort, dass diese Einengung erzwingt, dass jedes A_i ein Ideal in $\mathfrak{R}$ sei, wegen

$$RA_i = (A_1 + A_2 + \ldots + A_n)A_i = A_iA_i \subseteq A_i \tag{3.3}$$

und der rechtsdualen Gleichung hierzu.

Und ist umgekehrt $R = A_1 + A_2 + \ldots + A_n$ supplementär und jedes A_i ein Ideal in R, so folgt für jedes $i \neq j$ die Beziehung $A_iA_j \subseteq A_i \cap A_j = 0$, wegen $A_i \supseteq A_iA_j \subseteq A_j$.

3. 4. 2 DEFINITION. Wir nennen $\mathfrak{R}$ eine direkte Summe der Unterringe $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$, wenn $\mathfrak{R}$ supplementäre Summe der A_i und zudem jedes A_i ein Ideal in $\mathfrak{R}$ ist. Ist diese der Fall, so schreiben wir

$$R = A_1 \oplus A_2 \oplus \ldots \oplus A_n.$$

Um zu zeigen, dass $\mathfrak{R}$ direkte Summe von Unterringen B_i ist, genügt es zu zeigen, dass jedes dieser B_i ein Ideal in $\mathfrak{R}$ ist und dass die 0 eine eindeutig in Summanden aus der Menge dieser B_i zerfällt. Wir nehmen nun weiter an, dass $\mathfrak{R}$ ein halbeinfacher DCCL-Ring ist.

3. 4. 3 DEFINITION. Ein Ideal I von $\mathfrak{R}$ heißt einfach, wenn es als Ring betrachtet kein echtes Nichtnullideal enthält, also nach 3.3.5 kein Nichtnullideal $A \neq I$ von $\mathfrak{R}$ enthält.

3. 4. 4 LEMMA. *Sind $I_1, I_2, \ldots, I_m$ paarweise verschiedene einfache Ideale aus $\mathfrak{R}$ mit $R = I_1 + I_2, \ldots + I_m$, so gilt sogar $\mathfrak{A} = \mathfrak{I}_1 \oplus \mathfrak{I}_2 \oplus \ldots \oplus \mathfrak{I}_m$.*

BEWEIS. Da A Summe der $I_j's$ ist und da jedes I_j ein Ideal aus $\mathfrak{R}$ und damit aus $\mathfrak{A}$ ist, genügt es zu zeigen, dass sich die 0 eindeutig als Summe von Komponenten aus den einzelnen $I_j's$ ist.

Sei also in diesem Sinne $0 = x_1 + x_2 + \ldots + x_n$. Wir haben zu zeigen, dass alle diese x_i gleich 0 sind. Hierzu betrachten wir zu einem $i \neq j$ ein $I_i \cap I_j$. Dies ist ein Ideals aus $\mathfrak{R}$, das in beiden der betrachteten Ideale enthalten ist,

also auch in $I_i \cap I_j$. Nun sollten aber I_i, I_j einfach sein. Das bedeutet dann $I_i \cap I_j = 0$, denn wir waren ja ausgegangen von $I_i \neq I_j$.

Nach 3.3.2 ist aber jedes I_j vom Typ $Re_{=}e_jR$, wobei e_j die Einheit von I_j ist und nach 3.3.4 im Zentrum von $\mathfrak{R}$ liegt. Ist nun x ein Element aus $I_i \ \ (i \neq j)$. Dann folgt $e_jx_i = 0$. Das bedeutet:

$$0e_j = x_1e_j + x_2e_j + \ldots + x_ne_j \Longrightarrow x_j = x_je_j = 0,$$

also ganz allgemein $x_1 = x_2 = \ldots x_n = 0$, q.e.d. □

3.5 Zentrale idempotente Elemente

In diesem Abschnitt präsentieren wir fundamentale Sätze über eine Klasse von speziellen Idempotenten.

3. 5. 1 DEFINITION. Wir nennen ein idempotentes Element semi-primitiv, wenn es zentral ist und keine Zerlegung in zwei zentrale idempotente Summanden uu mit $uv = 0$ zulässt. Wir nennen zwei (beliebige) Idempotente uu orthogonal, wenn sie $uv = 0 = vu$ erfüllen, und wir sagen die Elemente $u_1, u_2, \ldots, u_n$ seien paarweise orthogonal, wenn sie $u_iu_j = 0 \ \ (\forall i \neq j)$ erfüllen.

3. 5. 2 LEMMA. *Ein zentrales idempotentes Element e ist semiprimitiv gdw. kein zentrales idempotentes $u \neq e$ existiert mit $eu = u$, also wenn e das einzige idempotente Element in dem Ideal eR ist.*

BEWEIS. Existiert ein zu e ein u im Sinne des Satzes, so ist $v = e - u$ zentral und idempotent mit $e = u + v$ und $uv = 0$, ein Widerspruch!

Andererseits: Ist e nicht semiprimitiv, so existieren zentrale idempotente Elemente $u \neq e \neq v$ mit $u + v = e \ \ \& \ \ uv = 0$, und wir erhalten sofort $eu = (u + v)u = u$.

Schließlich ist die letzte Bemerkung im Lemma natürlich äquivalent dazu, dass kein zentrale idempotentes u mit $eu = u$ existiert. □

Als nächstes Kriterium erhalten wir:

3. 5. 3 LEMMA. *Das zentrale idempotente Element e ist semiprimitiv gdw. das Ideal Re einfach ist.*

BEWEIS. Ist e semiprimitiv, so enthält das Ideal Re keine weiteren zentralen idempotenten Elemente. Nehmen wir nun an, das Ideal Re enthielte ein echtes Ideal J, so wäre J nach 3.3.5 auch ein Ideal aus $\mathfrak{R}$, also nach 3.3.2 $J = Ru$ mit zentralem idempotenten u erfüllt. Da u aber gleich e sein müsste hätten wir $J = Re$. Also ist Re einfach.

Sei nun umgekehrt das zentrale idempotente Element e nicht semiprimitiv. Dann enthält Re nach dem vorherigen Lemma 3.5.2 ein zentrales Idempotentes $u \neq e$ und es ist Ru ein Nichtnullideal, enthalten in Re. Weiterhin ist $Ru \neq Re$, denn andernfalls hätten wir $e = xu$ und damit

$$e - u = (e - u)e = (e - u)ux = (u - u)x = 0, \text{ also } e = u,$$

mit Widerspruch. Daher ist in diesem Falle Re nicht einfach und damit das Lemma bewiesen. □

Schließlich zeigen wir noch

3. 5. 4 LEMMA. *Jedes nicht semiprimitive zentrale idempotente Element e ist eine endliche Summe von paarweise orthogonalen semiprimitiven idempotenten Elementen.*

BEWEIS. Wir betrachten alle endlichen Summen paarweise verschiedener idempotenter Elemente aus Re. Da Re ein minimales und daher ein einfaches Ideal enthalten muss, enthält Re auch ein semiprimitives Element. Jede Summe der betrachteten Art besteht nun aus paarweise orthogonalen semiprimitiven idempotenten Elementen.
DENN, sind u, v verschieden, semiprimitiv und idempotent, so sind nach 3.5. 4 Ru und auch Rv einfach. Wäre nun $uv \neq 0$, so hätten wir $Ru \cap Rv \supset Ru \cdot Rv \neq 0$, wegen $uuvv = uv$. Da aber Ru und auch Rv einfach sind, würde dies zu $Ru = Rv$ führen. Also wäre nach 3.5.3 $u = v$, mit Widerspruch zu der Annahme $u \neq v$.

SEI HIERNACH $\sum_i^n u_i$ solch eine Summe paarweise orthogonaler semiprimitiver idempotenter Elemente aus Re. Dann ist $e - \sum_i^n u_i$ idempotent, wegen $eu_i = u_i \ (1 \leq i \leq n)$, und natürlich auch zentral, also $R(e - \sum_i^n u_i)$ ein (zweiseitiges) Ideal. Unter allen Idealen dieses Typs erhalten wir aber wegen DCCL

ein minimales, von dem wir jetzt zeigen werden, dass es gleich dem Nullideal ist.

ANGENOMMEN, dieses Ideal wäre nicht das Nullideal, so wäre es vom Typ Re' mit einem zentralen idempotenten Element $e' = e - \sum_{i}^{m} v_i$ mit paarweise orthogonalen semiprimitiven idempotenten Elementen v_i. Nun erfüllt Re' aber DCCL nach 3.3.5. Also enthielte es ein minimales Ideal, das auch minimal in $\mathfrak{R}$ wäre, also von der Form Rv_{m+1} mit zentral idempotenten v_{m+1}. Dieses v_{m+1} läge dann aber auch in Re' und da Ideale von Idealen aus $\mathfrak{R}$ ebenfalls Ideale aus $\mathfrak{R}$ sind, müsste Rv_{m+1} einfach und v_{m+1} demzufolge nach 3.5.4 semiprimitiv sein. Es muss aber weiterhin v_{m+1} verschieden sein von allen v_i $(1 \leq i \leq n)$. Denn, sonst wäre zunächst

$$v_j = xe' = x(e - \sum_{1}^{m} v_j).$$

Und hieraus ergäbe sich weiter $v_j = (v_j - v_j) = 0$, mit Widerspruch. Folglich wäre $\sum_{i}^{m+1} v_i$ eine Summe von paarweise verschiedenen semiprimitiven Elementen aus Re.

Wir betrachten nun

$$R(e - \sum_{1}^{m+1} v_i) = R(e' - v_{m+1}).$$

Wegen $e' - v_{m+1} = R(e' - v_{m+1})e'$ gilt zunächst $R(e' - v_{m+1}) \subseteq Re'$. Jedoch, e' liegt in Re', nicht aber in $R(e' - v_{m+1})$, da wir andernfalls $e' = x(e' - v_{m+1})$ erhielten und hieraus nach Multiplikation von rechts mit v_{m+1} die Gleichheit $v_{m+1} = x(v_{m+1} - v_{m+1}) = 0$, mit Widerspruch. Folglich wäre $R(e' - v_{m+1}) = R(e - \sum_{1}^{m+1} v_i)$ ein Ideal des betrachteten Typs und echt enthalten in Re', mit Widerspruch zur Minimalität von Re'. Also muss Re' gleich dem Nullideal sein.

FAZIT: Es existiert eine endliche Summe paarweise orthogonaler semiprimitiver idempotenter Elemente $\sum_{1}^{m} v_i$ mit $R(e - \sum_{1}^{m} v_i) = 0$ und demzufolge ein $\sum_{1}^{m} v_i$ mit $e = \sum_{1}^{m} v_i$. □

Nun sind wir in der Lage, einen ersten Hauptsatz zu beweisen.

3. 5. 5 Das erste Strukturtheorem.

Erfüllt ein halbeinfacher Ring $\mathfrak{R}$ DCCL, so hat er nur eine endliche Anzahl einfacher Ideale I_i $(1 \leq i \leq n)$. Ist $\mathfrak{R}$ zudem nicht der Zeroring, so sind diese nicht nilpotente einfache DCCL-Ringe und $\mathfrak{R}$ ist direkte Summe von ihnen. Demzufolge kann ein jeder Ring dieses Typs bis auf die Reihenfolge der Summanden eindeutig ausgedrückt werden in der Form

$$\mathfrak{R} = \mathfrak{I}_1 \oplus \mathfrak{I}_2 \oplus \ldots \oplus \mathfrak{I}_n \ ,$$

worin die Komponenten A_i nicht nilpotente einfache DCCL-Ringe sind.

BEWEIS. Nach 3.3.3 hat $\mathfrak{R}$ ein Einselement, das wir hier mit 1 bezeichnen wollen. Natürlich ist 1 zentral idempotent. Weiter gilt $1 = e_1 + e_2 + \ldots + e_n$, nach Lemma 3.5.4, mit paarweise orthogonalen zentralen semiprimitiven idempotenten Elementen e_i. Möglicherweise ist 1 selbst schon semiprimitiv. Dann wäre $\mathfrak{R}$ einfach nach 3.5.3. Doch im allgemeinen Fall gilt:

$$R = R1 = R(e_1 + 2_2 + \ldots + e_n) = Re_1 + Re_2 + \ldots Re_n \, .$$

Da jedes e_i semiprimitiv ist, sind die Ideale Re_i nach 3.5.3 einfach, also ist $\mathfrak{R}$ nach 3.4.4 direkte Summe der $\mathfrak{R}e_i$.

Ist J nun irgendein Ideal aus $\mathfrak{R}$, so folgt $J = JR = JRe_1 + JRe_2 + \ldots + JRe_n$. Ist hierin $JRe_i \neq 0$, so ist auch $J \cap Re_i \neq 0$ und deshalb $JRe_i \subseteq J$ und daher $Re_i \subseteq J$. Folglich ist jedes Ideal direkte Summe von Idealen Re_j die in ihm enthalten sind.

Sei nun I ein einfaches Ideal aus $\mathfrak{R}$. Dann lässt sich I schreiben als Summe $I = IR + IRe_1 + IRe_2 + \ldots + IRe_n$ und ist $I \neq 0$, so ist auch mindestens ein $IRe_i \neq 0$, also auch $I \cap Re_i \neq 0$. Da aber I und auch Re_i einfach sind, folgt hieraus $I = Re_i$. Und das bedeutet, dass die Re_i die einzigen einfachen Ideale aus $\mathfrak{R}$ sind. Also hat $\mathfrak{R}$ nur eine endliche Anzahl von einfachen Idealen, und es ist keines von ihnen nilpotent, wegen $ee = e \neq 0$. □

3.6 Idempotente Elemente

Um weitere wichtige Informationen über halbeinfache DCC-Ringe zu erhalten, fragen wir jetzt natürlich nach der Struktur der obigen Komponenten, also der

nicht nilpotenten einfachen Ringe. Wir wissen schon, dass solche Ringe ein Einselement haben. Um weitere Einsichten zu gewinnen, analysieren wir die Struktur der nicht zentralen idempotenten Elemente aus $\mathfrak{R}$ und werden Sätze erhalten, die denen unter 3.5.2 bis 3.5.4 entsprechen. Nach Voraussetzung haben wir nur ein einziges zentrales idempotentes in $\mathfrak{R}$, aber es mag eine Fülle von nicht zentralen Idempotenten geben.

Wir nennen ein idempotentes Element e primitiv, wenn es keine Darstellung $e = u + v$ mit orthogonalen idempotenten Elementen u, v besitzt.

3. 6. 1 LEMMA. *Ein idempotentes Element e aus $\mathfrak{R}$ ist primitiv, wenn R kein idempotentes $u \neq e$ enthält, derart dass $eu = u = ue$ erfüllt ist oder anders formuliert, wenn e das einzige idempotente Element in eAe ist.*

BEWEIS. Sei e primitiv idempotent, dann existiert ein idempotentes u mit $eu = ue = u$. Wir setzen $v = e - u$. Dann folgt

$$v^2 = (e-u)(e-u) = e - u - u + u = e - u = v$$

und $vu = uv = 0$. Daher ist $e = u + v$ mit idempotenten orthogonalen Elementen u, v, ein Widerspruch. Also kann kein solches u existieren.

Ist nun andererseits e nicht primitiv, so haben wir $e = u + v$ mit orthogonalen idempotenten Elementen u, v. Dann folgt aber $u \neq e$ mit $u = eu = ue$.

Man beachte jetzt noch, dass die abschließende Bemerkung des Lemmas äquivalent ist mit der Aussage, es existiere kein $u \neq e$ mit $u = ue = eu$. □

3. 6. 2 LEMMA. *Ein idempotentes Element e aus $\mathfrak{R}$ ist primitiv in $\mathfrak{R}$ gdw. Re ein minimales Linksideal ist.*

BEWEIS. Ist Re kein minimales Linksideal, so enthält es ein minimales Linksideal und dieses hat nach 3.3.1 die Form Ru mit idempotentem u. Wegen $u \in Re$ gilt aber $ue = u$. Wir definieren $u' = eu$ und $v := e - eu$. Weder u noch u' sind gleich 0. Denn $u' = 0$ würde zu $u = uu = ueu = 0$ führen und $v = 0$ würde bedeuten $e = eu$, also $e \in Au$ und damit $Au = Ae$, ein Widerspruch.

Beachte nun die Gleichheit $e = u' + v$. Sie impliziert:

$$u'u' = eueu = euu = eu = u' \tag{3.4}$$

$$
\begin{aligned}
(3.5) \qquad vv &= (e-u)(e-u) = e - eu - eu + eu = e - eu = v \\
(3.6) \qquad u'v &= eu(e-eu) = eu - eu = 0 \\
(3.7) \qquad v'u &= (e-eu)eu = eu - eu = 0\ .
\end{aligned}
$$

Daher ist e im angenommenen Fall nicht primitiv. Und das bedeutet, dass für ein primitives e die Untermenge Re ein minimales Linksideal ist.

Sei nun umgekehrt e nicht primitiv, also vom Typ $e = u + v$ mit orthogonalen idempotenten Elementen u, v. Dann folgt zunächst $eu = ue = u$ und $Ru = Rue \subseteq Re$. Es liegt e aber in Re, nicht hingegen in Ru, denn $e = xu$ würde zu $ev = v = xuv = 0$ führen, mit Widerspruch. Folglich enthält Re das Nichtnull-Linksideal Ru echt und ist aus diesem Grund nicht minimal. □

Man beachte an dieser Stelle, dass e, obwohl primitiv, nicht notwendig das einzige idempotente Element aus in Re ist.

Schließlich kommen wir zu

3. 6. 3 LEMMA. *Ein idempotentes Element aus $\mathfrak{R}$ ist genau dann primitiv, wenn $\mathfrak{R}$ ein Divisionsring, d.h. ein nicht kommutativer Körper, sprich Schiefkörper, ist.*

BEWEIS. Klar doch, Schiefkörper enthalten exakt ein Idempotentes, nämlich ihre Eins.

Sei hiernach e primitiv. Dann ist nach dem vorhergehenden Lemma Ae ein minimales Linksideal. Sei weiter exe irgendein nicht verschwindendes Element aus R. Dann ist $Rexe$ ein Linksideal enthalten in Re, und es ist $Rexe$ nicht das Nullideal, wegen $e \cdot exe = exe$. Es ist aber Re minimal, also ist dann $Rexe = Re$. Da e zu Re gehört, liegt es dann aber auch in $Rexe$, was $e = yexe$ bedeutet. Und dies führt zu

$$eye \cdot exe = e \cdot yexe = ee = e\,.$$

Folglich ist eye ein Linksinverses zu exe in $eRe - 0$, und es ist e Linkseins von $eRe - 0$. Daher bildet $eRe - 0$ nach der Vorlesung zur Algebra eine Gruppe bezüglich der Multiplikation.

ALTERNATIV kommen wir NACH DIVINSKY [6] wie folgt zum Ziel:

Wir betrachten $z := exe \cdot eye$. Hier gilt

$$z^2 = exeeye \cdot exeeye = exe \cdot e \cdot eye = exeeye = z$$

und es liegt z in eRe und es ist $z \neq 0$, wegen

$$exeeye = 0 \Longrightarrow exeeyeexe = exe \cdot e = exe \neq 0\,.$$

Es ist also z idempotent und verschieden von 0, und es liegt z in eRe.

Da e primitiv ist, ist es nach 3.6.1 das einzige idempotente Element in eRe und daher gleich e, also

$$eye \cdot exe = exe \cdot eye = e\,.$$

Somit hat jedes Element aus eRe ein Inverses in eRe. Daher ist $e\mathfrak{R}e$ ein Divisionsring. □

Schließlich erhalten wir analog zu 3.5.4

3. 6. 4 LEMMA. *Jedes nicht primitive idempotente Element e aus $\mathfrak{R}$ kann ausgedrückt werden als endliche Summe paarweise orthogonaler primitiver idempotenter Elemente.*

BEWEIS. Ist das idempotente Element e nicht primitiv, so ist nach Lemma 3.6.1 Re kein minimales Linksideal. Anwendung von DCCL liefert jedoch über $A \subset Ae \subseteq \ldots$ ein minimales Linksideal von A, das enthalten ist in Ae, und hieraus folgt, dass Ae ein primitives idempotentes Element enthält, das – natürlich – auch zu A gehört.

Wir betrachten nun alle endlichen Summen paarweise verschiedener orthogonaler primitiver idempotenter Elemente aus Re. Möglicherweise enthält Re nur ein einziges primitives Element oder aber es sind nicht zwei der primitiven Elemente aus Re orthogonal. In diesem Falle haben wir nur einelementige orthogonale Summen der gewünschten Art.

Hiernach betrachten wir die Menge aller Linksideale aus Re von der Form $e - \sum_i^n u_i$, worin $\sum_i^n u_i$ eine endliche Summe paarweise orthogonaler primitiver idempotenter Elemente aus Re sei.

Unter allen Linksidealen dieses Typs erhalten wir wegen DCCL ein minimales, von dem wir jetzt zeigen werden, dass es gleich dem Nullideal ist.

ANGENOMMEN, dieses Linksideal wäre nicht das Nullideal, so wäre es vom Typ Rv mit $v = e - \sum_1^m v_i$. mit paarweise orthogonalen primitiven idempotenten Elementen v_i. Da diese v_i alle aus Re stammen, folgt unmittelbar

$v_i e = v_i$ $(1 \leq i \leq m)$. ev_i mag aber verschieden sein von v_i, klar. Aus diesem Grunde arbeiten wir mit den $ev_i{}'s$.

Sie sind erstens verschieden von 0 wegen $ev_i = 0 \Longrightarrow v_i v_i = v_i e v_i = 0$, ein Widerspruch. Sie sind zweitens idempotent wegen $ev_i ev_i = ev_i v_i = ev_i$. Sie sind drittens primitiv, da nach 3.6.1 $Ae_{v_i} = Av_i$ erfüllt ist, wegen der Primitivität von v_i und $Aev_i \neq 0$. Folglich sind viertens, erneut nach 3.6.1, mit den v_i auch die ev_i primitiv. Und fünftens sind die ev_i paarweise orthogonal, wegen $i \neq j \Longrightarrow ev_i ev_j = ev_i v_j = 0$. Schließlich haben wir

$$R(e - \sum ev_i) = Re(e - \sum ev_i) \subseteq R(e - \sum ev_i) = Rv \ .$$

Es sollte aber Rv ein minimales Linksideal dieses Typs sein, also erhalten wir $Rv = R(e - \sum ev_i)$.

Wir setzen nun $v' = e - \sum ev_i$. Dann ist v' idempotent wegen

$$(e - \sum ev_i)(e - \sum ev_i) = e - \sum ev_i - \sum ev_i + \sum ev_i = e - \sum ev_i$$

und verschieden vom Nullideal. Also ist Av' ein minimales Linksideal oder es enthält ein minimales Linksideal, in jedem Falle aber enthält es aus diesem Grunde ein primitives Idempotentes w.

KLAR, wv' ist ebenfalls idempotent, $v'w$ hingegen muss – siehe oben – nicht idempotent sein. Und – erneut wie oben – arbeiten wir auch hier weiter mit $v'w := w'$ statt mit w und gelangen so zu $w' \neq 0$, $w'^2 = w'$, $Rw' = Rw$, woraus resultiert, dass w' primitiv idempotent ist.

WEITERHIN erhalten wir

$$ev_k \cdot v'w = ev_k(e - \sum ev_i)w = (ev_k - ev_k)w = 0$$

und damit für alle für alle $1 \leq k \leq m$ die Gleichheit

$$v'w \cdot ev_k = v'wv'ev_k = v'w(e - \sum ev_i)ev_k = v'w(ev_k - ev_k) = 0\,.$$

Demzufolge ist $w' + \sum ev_i$ eine endliche Summe des gewünschten Typs. Es gilt aber

$$R(v' - w') = R(e - [w' + \sum ev_i]) \subseteq Rv'$$

wegen $(v' - w')v' = v' - w'$, was man leicht nachrechnet.

Nun liegt aber v' in Rv', nicht hingegen in $R(v' - w')$, da aus $v' = x(v' - w')$ durch Rechtsmultiplikation mit w' folgen würde $w' = 0$, mit Widerspruch.

Also ist $R(e-[w'+\sum ev_i])$ echt in Rv' enthalten und vom gewünschten Typ. Das allerdings widerspricht unserer Minimalitätsforderung an $Rv = Rv'$. Somit muss das betrachtete Minimalideal vom Typ $R(e-\sum u_i)$ gleich dem Nullideal sein.

FAZIT: Unser $e-\sum u_i$ verschwindet, also ist e gleich $\sum u_i$ und damit eine endliche Summe von paarweise orthogonalen primitiven Idempotenten. □

3.7 Ein Struktursatz im einfachen Fall

In diesem Abschnitt werden wir mit Hilfe der Lemmata 3.6.1 bis 3.6.4 einen Struktursatz für einfache Ringe herleiten. Doch zuvor noch das folgende Resultat:

3. 7. 1 LEMMA. *Besitzt ein DCCL-Ring eine Eins, so gilt mit $xy = 1$ stets auch $yx = 1$.*

BEWEIS. Wir betrachten die absteigende Kette der Linksideale

$$Rx \supseteq Rx^2 \supseteq Rx^3 \supseteq \ldots \supseteq Rx^n \supseteq \ldots$$

Wegen DCCL existiert hier ein m mit $Rx^m = Rx^{m+1}$, also existiert ein $z \in R$ mit $zx^{m+1} = x^m$ und also mit $(zx-1)x^m = 0$. Das liefert dann weiter $(zx-1)\cdot x^m y^m = (zx-1)\cdot 1 = 0$, also $zx = 1$ und damit wegen $z = zxy = y$ auch $yx = 1$, wie behauptet. □

Hiernach lässt sich herleiten:

3. 7. 2 Ein Struktursatz für einfache DCCL-Ringe. *Jeder einfache DCCL-Ring $\mathfrak{R}$ lässt sich auffassen als Ring $\mathcal{M}$ aller Matrizen einer (geeigneten) Ordnung n über einem Divisionsring $\mathfrak{D}$.*

BEWEIS. Sei zunächst $\mathfrak{R}$ ein halbeinfacher DCCL-Ring. Dann besitzt $\mathfrak{R}$ eine 1, die ihrerseits nach Lemma 3.6.4 eine endliche Summe paarweise orthogonaler primitiver idempotenter Elemente ist, etwa vom Typ $1 = e_1 + e_2 \ldots + e_n$. Des weiteren sind nach Lemma 3.6.3 alle $e_l R e_i$ Divisionsringe. Darüber hinaus ist jedes $Re_iR = R$, da R einfach und zudem ein Ideal aus $\mathfrak{R}$ ist und zwar verschieden vom Nullideal wegen $e_ie_ie_i = e_i \in Re_iR$.

WIR DEFINIEREN NUN

$$R_{ij} := e_i R e_j \ .$$

Dann folgt zunächst:

$$R_{ij}R_{jk} = e_i R e_j R e_k = e_i R e_k = R_{ik}\,.$$

Ist hingegen $j \neq h$, so folgt $R_{ij}R_{hk} = 0$. Weiterhin sind die R_{ij} Unterringe wegen $R_{ij}R_{ij} = 0$, falls $i \neq j$ und $R_{ii}R_{ii} = R_{ii}$. Liegt nun a_{ij} in R_{ij}, so haben wir $e_{ij}a_{ij} = a_{ij} = a_{ij}e_{ij}$ und gelten $h \neq i$ bzw. $k \neq j$, so erhalten wir $e_h a_{ij} = 0 = a_{ij}e_k$. Insbesondere ist damit $R_{1j}R_{j1} = R_{11}$. Wegen $R_{11} = e_1 R e_1$ liegt aber e_1 in R_{11}, das folglich verschieden ist vom Nullideal. Daher liegt e_1 in allen $R_{1j}R_{j1}$, ist also eine endliche Summe von Produkten, gebildet aus Elementen aus R_{1j} mit Elementen aus R_{j1}. Tatsächlich gilt aber mehr, nämlich:

Es ist e_1 Produkt eines einzigen Elementes aus R_{1j} mit einem einzigen Element aus R_{j1}. Um dies einzusehen, beachte man zunächst, dass in R_{j1} ein Element e_{j1} existiert mit $R_{1j}e_{j1} \neq= 0$. Also existiert auch ein a_{1j} in R_{1j} mit $a_{1j}e_{j1} \neq 0$. Wir bezeichnen dieses a_{1j} mit a_j und beachten, dass es zu R_{11} gehört, was zu einem $b_j \in R_{11}$ mit $b_j a_j = e_1$ führt. Für dieses b_j erhalten wir weiter $b_j a_{1j} e_{j1} = e_1$. Wir setzen nun $e_{1j} = b_j a_{1j}$. Dieses Element liegt in R_{1j}, und es gilt $e_{1j}e_{j1} = e_1$. Auf diese Weise erhalten wir für alle $1 \leq j \leq n$ Elemente e_{ij} und e_{ji} mit $e_{ij}e_{j1} = e_1$, und es liegen e_{1j} in R_{ij} und e_{j1} in R_{j1}.

Hiernach definieren wir $e_{ij} := e_{i1}e_{1j}$ und werden zeigen, dass sich diese Elemente exakt verhalten wie die Matrizen über einem Divisionsring, die ihrerseits belegt sind mit 1 an der Stelle i, j und mit Null an allen anderen Stellen.

Hierzu beachten wir zunächst

$$e_{ij}e_{jk} = e_{i1}e_{1j}e_{j1}e_{1k} = e_{i1}e_1e_{1k} = e_{i1}e_{1k} = e_{ik} \tag{3.8}$$

$$e_{ij}e_{hk} = e_{i1}e_{1j}e_{h1}e_{1k} = 0 \quad \text{im Falle} \quad j \neq h \tag{3.9}$$

$$e_{ij} \in e_i R e_j \tag{3.10}$$

und betrachten danach den Unterring $\mathcal{M}$, der von diesen n^2 vielen Elementen e_{ij} erzeugt wird. Dieser Unterring hat $e_{11} + e_{22} + \ldots + e_{nn}$ als Einheit. Nun ist aber $e_{ii}^2 = e_{ii}$ idempotent und ein Element aus $e_i R e_i$ und da e_i primitiv idempotent ist, ist $e_{ii} = e_i$ nach Lemma 3.6.1. Also ist $e_{11} + e_{22} + \ldots + e_{nn} = e_1 + e_2 + \ldots + e_n = 1$. Demzufolge enthält $\mathfrak{R}$ einen Unterring $\mathcal{M}$, dessen Einselement das Einselement 1 aus $\mathfrak{R}$ ist und dessen Generatoren sich verhalten wie die Matrixgeneratoren.

Sei nun D die Menge aller Elemente aus $\mathfrak{R}$, die mit allen Elementen m aus $\mathcal{M}$ kommutieren, d.h. $mx = xm$ erfüllen, und sei a ein Element aus R. Wir definieren

$$a_{ij} := \sum_{k=1}^{n} e_{ki} \cdot a \cdot e_{jk} \,.$$

Dann folgt $a_{ij}e_{rs} = e_{ri}ae_{js}$. Also liegt a_{ij} in D. Dies führt aber zu $a \in D$ vermöge

$$\sum_{i,j=1}^{n} a_{ij}e_{ij} = \sum_{i,j,k} e_{ki}ae_{jk}e_{ij} = \sum_{j,k} e_{kk}ae_{jj} = 1 \cdot a \cdot 1 = a \,,$$

also zu $MD = R = DM$.

Schließlich bildet $\mathfrak{D}$ einen Divisionsring. Denn zunächst haben wir:

$$R = \sum_{k,l}(e_{k,l}D)$$

und damit weiter

$$e_iRe_i = e_i \sum_{k,l}(e_{k,l}De_i) = e_{ii}D = e_iD \,.$$

Also ist $e_i\mathfrak{D}$ ein Divisionsring, da (jedes) $e_i\mathfrak{R}e_i$ ein Divisionsring ist. Wir zeigen, dass $\mathfrak{D}$ und $e_i\mathfrak{D}$ isomorph sind unter $d \longmapsto e_id$. Es folgt unmittelbar, dass diese Abbildung einen Homomorphismus bildet.

Bleibt die Frage nach dem Kern. Sei hierzu $e_id = 0$. Dann ist auch jedes e_jd gleich 0, wegen $e_jd = e_{ji}e_{ii}e_{ij}d = e_{ji}e_{ii}de_{ij} = 0$. Und das bedeutet $d = 1d = (e_1 + e_2 + \ldots + e_n) = 0$.

Also ist $\mathfrak{D}$ isomorph zu $e_i\mathfrak{D} = e_i\mathfrak{R}e_i$. Somit sind alle $e_i\mathfrak{R}e_i$ zueinander isomorph und, was noch wichtiger ist, es ist auch $\mathfrak{D}$ ein Divisionsring.

Sei hiernach B die Menge aller $n \times n$ Matrizen über dem Divisionsring $\mathfrak{D}$. Es gilt

$$B = \{ \sum_{ij}(E_{ij}d)\} \,,$$

worin E_{ij} diejenige Matrix sei, deren Stelle (i, j) mit 1 belegt ist, während alle anderen Stellen mit 0 belegt sind. Wir bilden B nach A ab vermöge

$$\sum_{ij}(E_{ij}d_{ij}) \longmapsto \sum_{ij}(e_{ij}d_{ij})$$

Dies liefert natürlich einen Homomorphismus. Wir zeigen dass $\longmapsto$ sogar einen Isomorphismus liefert. Sei hierzu $\sum_{ij}(e_{ij}d_{ij}) = 0$. Dann ist auch $e_k \cdot \sum_{ij}(e_{ij}d_{ij}) \cdot e_l = 0 = e_{kl}d_{kl}$.

Und hieraus folgt weiter $e_{lk}e_{kl}d_{kl} = 0 = e_l d_{kl}$ und damit, wie oben, $e_i d_{kl} = 0$ für alle i, also – erneut wie oben – wie oben $d_{kl} = 0$. Folglich liefert $\longmapsto$ einen Isomorphismus. □

Es ist üblich, in diesem Falle $R = \mathcal{M} \times D$ zu schreiben.

Wir betrachten abschließend den Gegenfall.

3. 7. 3 PROPOSITION. *Sei $R = \mathcal{M} \times D$. Dann ist $\mathfrak{R}$ nicht nilpotent und einfach.*

BEWEIS. Sei $R = \mathcal{M} \times D$. Dann besitzt $\mathfrak{R}$ eine Eins und ist demzufolge nicht nilpotent.

Um zu zeigen, dass $\mathfrak{R}$ einfach ist, sei I ein Ideal und $0 \neq x = \sum e_{ij}d_{ij} \in I$. Dann muss mindestens eine der Komponenten, etwa d_{uv}, verschieden sein von 0. Damit enthält I in diesem Falle aber auch

$$\begin{aligned} {d_{uv}}^{-1} \sum_r (e_{ru} x e_{vr}) &= {d_{uv}}^{-1} \left(\textstyle\sum_{i,j,r} e_{ru}e_{ij}e_{vr}d_{uv}\right) \\ &= {d_{uv}}^{-1} \left(\sum_r e_{rr}d_{uv}\right) = \sum_r e_{rr} = 1 \end{aligned}$$

Also ist $\mathfrak{R}$ einfach. □

Literaturverzeichnis

[1] Borewicz, S. I. & I. R. Šafarevič: *Zahlentheorie.* Birkhäuser Verlag Basel und Stuttgart, 1966.

[2] Bosbach, B.: *Magister-Aspekte.* Lecture Note,1994-2010, 611 S. KOBRA Kassel, 2015.

[3] Bosbach, B.: *Topics in Divisibility*, 1994-2010, 928 S., KOBRA Kassel, 2015.

[4] Dedekind, R. & H. Weber: *Theorie der algebraischen Funktionen einer Veränderlichen.* J. Reine Angew. Math. **92** (1882), 181 - 290.

[5] Dirichlet, P. G.: *Vorlesungen über Zahlentheorie.* Vieweg und Sohn, Braunschweig, 1.,2.,3.,4. Auflage 1872 - 1894.

[6] Divinsky, N.J.: *Rings and Radicals.* Allen and Unwin, London, 1965

[7] 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.

[8] 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.

[9] Hensel, K.: *Gedächtnisrede auf E. E. Kummer.* Abh. Gesch. Math. Wiss. Teubner, Berlin und Leipzig, 1910.

[10] Hermes, H.: *Einführung in die Vebandstheorie*, Grundlehren der Mathematischen Wissenschaften, zweite, erweiterte Auflage, Springer, 1967.

[11] Kaplansky, I.: *Commutative Rings.* Allyn and Bacon, Boston, Massachusetts, 1969.

[12] Krull, W.: *Ein neuer Beweis für die Hauptsätze der allgemeinen Idealtheorie.* Math. Ann. **90** (1923), 55 - 64.

[13] Krull, W.: *Die Theorie der allgemeinen Zahlringe.* Math. Ann. **99** (1928), 51 - 70.

[14] 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.

[15] LARSEN, M. D. & P. J. MCCARTHY: *Multiplicative Theory of Ideals.* Academic Press, New York and London, 1971.

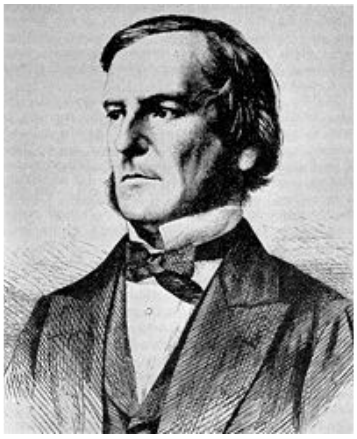
[16] NOETHER, EMMY.: *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern.* Math. Ann. **96** (1927), 26 - 61.

[17] VAN DER WAERDEN, B. L.: *Algebra* I/II, etwa 5. Auflage. Springer, Berlin-Heidelberg-New York, 1967.

Index

Ordnungs-Architektur
Ein Faszinosum !

Bruno Bosbach
1997/2003/2008



George Boole

1815-1864

Inhaltsverzeichnis

Vorwort

An der *Gruppe* führt kein Weg vorbei, jeder Student wird irgendwann mit ihr konfrontiert, sei es in der Geometrie, der Linearen Algebra, der Algebra oder der Zahlentheorie, sei es in der Analysis, sei es in der Topologie, immer wieder scheint sie auf als Struktur gebende Komponente. Es gibt mathematische Theorien, die aus der Physik erwachsen, man denke an die Analysis, doch gelegentlich hilft eine ausgebaute mathematische Theorie auch in der Physik weiter, wie die Theorie der *Quaternionen* oder die Theorie der Gruppen, man google „van der Waerden" oder mit Blick auf die Feldtheorie „Emmy Noether", aus deren Theorie der hyperkomplexen Systeme HEISENBERG wesentliche Anstöße für seine Begründung der Quantenmechanik erhielt. So dürfte denn eigentlich kein Lehramts-Kandidat ohne elementare Kenntnisse der Gruppentheorie „verabschiedet" werden.[1)]

Anders hingegen verhält es sich mit der Struktur des *Verbandes*. Sie ist nicht weniger fundamental, durchwebt die Mathematik in ähnlicher Weise, beschreibt die Mengenlehre und die Geometrie in weiten Teilen, erfasst die Logik und die Theorie der Schaltwerke, und PASCUAL JORDAN hat gar eine nicht kommutative verbandstheoretische Fassung einer Quanten-Logik verfolgt. Jedoch – selbst angesehenen Mathematikern ist diese Struktur nicht notwendig bekannt, wie sonst wäre es zu erklären, dass es Mathematische Institute in erheblicher Zahl gibt, die Ihren Ausbildungsauftrag zielsicher vorbei an jedweder Ordnungstheorie wahrzunehmen wissen.

Ausgangsstruktur für den Verband ist die *Poset*, englich *po-set*, das ist eine Menge mit einer Relation $\leq$, die den Gesetzen genügt:

(R) $\quad a \leq a$

(A) $\quad a \leq b \leq a \Longrightarrow a = b$

(T) $\quad a \leq b \leq c \Longrightarrow a \leq c\,.$

[1)] Übrigens für alle Kasseler Freaks: hier gibt es eine Emmy-Noether-Straße im „Physikerviertel".

Diese Struktur „durchweht" unseren Alltag, in dem immer wieder zu vergleichen, gar zu bewerten ist, nicht selten selbst Unvergleichbares. Ordnen ist Alltags-Kombinatorik, Ordnen überwindet das Chaos.

Welch' wunderbare Mathematik sich schon auf Posets entwickeln lässt, ist bereits in [**?**] angeklungen und wird hier weiter sichtbar werden.

Existieren zu je zwei Elementen a, b einer po-set Elemente c, d mit

$$(1) \qquad a, b \leq x \iff c \leq x$$
$$(2) \qquad a, b \geq x \iff d \geq x\,,$$

so heißt $\mathfrak{V}$ ein Verband. Diese Elemente c, d sind dann eindeutig bestimmt, wir bezeichnen sie mit $c := \sup(a, b)$ und $d := \inf(a, b)$.

Der Verband als Struktur wurde von Dedekind als *Dualgruppe* eingeführt, er wurde im Rahmen seiner Untersuchungen zur algebraischen Zahlentheorie auf diese Struktur aufmerksam, siehe [11]. Und – noch heute steht ein von Dedekind in [10] gestelltes Problem der Verbandstheorie ungelöst im Raum, siehe hierzu [6].

Aus einer anderen Richtung war die Struktur des Verbandes schon zuvor von George Boole im Gewande der Logik „erfasst" worden, vgl. [4] und [5], doch es sollte bis in die 1930-er Jahre dauern, ehe Garret Birkhoff in [2] den Grundstein zu einer eigenständigen Theorie der Verbände legte, die sich dann zu einer faszinierenden, groß angelegten mathematischen Disziplin entfaltete. Inzwischen gibt es eine Flut von Lehrbüchern, unter denen das deutschsprachige von Hans Hermes, [22], und das englischsprachige von T. S.Blyth, an dieser Stelle besonders hervorgehoben seien.

Ist $\mathfrak{V}$ ein Verband, so lässt sich seine Struktur auch als Algebra beschreiben. Denn offenbar gelten die Gleichungen

$$(\mathrm{I}\vee) \quad a \vee a = a \qquad (\mathrm{I}\wedge) \quad a \wedge a = a$$
$$(\mathrm{K}\vee) \quad a \vee b = b \vee a \qquad (\mathrm{K}\wedge) \quad a \wedge b = b \wedge a$$
$$(\mathrm{A}\vee) \quad a \vee (b \vee c) = (a \vee b) \vee c \qquad (\mathrm{A}\wedge) \quad a \wedge (b \wedge c) = (a \wedge b) \wedge c$$
$$(\mathrm{V}\vee) \quad a \vee (b \wedge a) = a \qquad (\mathrm{V}\wedge) \quad a \wedge (b \vee a) = a$$

und umgekehrt lassen sich aus (I$\vee$) bis (V$\wedge$) bezüglich $a :\leq b \iff a \wedge b = a$ die Bedingungen einer sup- und inf-abgeschlossenen Partialordnung herleiten.

Ein Verband heißt distributiv, wenn er die beiden Gleichungen

$$a \wedge (b \vee c) \;=\; (a \wedge b) \vee (b \wedge c) \tag{7}$$

$$a \vee (b \wedge c) \;=\; (a \vee b) \wedge (b \vee c) \tag{8}$$

erfüllt, von denen jede schon aus der anderen folgt. Lange Zeit hat man irrtümlicherweise angenommen, jeder Verband sei distributiv.

Als elementare Beispiele seien erwähnt die Klassiker $\mathbf{N}$ betrachtet bezüglich $\leq$, $\mathbf{N}$ betrachtet bezüglich $|$, $\mathfrak{P}(\mathbf{N})$ betrachtet bezüglich $\subseteq$, die Menge der linearen Unter-Räume eines vorgegebenen Vektor-Raums $\mathfrak{V}$ betrachtet bezüglich Durchschnitt und Erzeugnis, $\mathfrak{A}$ (eine Menge von Aussagen) betrachtet bezüglich $\& :\Longleftrightarrow et$, und $\mathsf{V} :\Longleftrightarrow vel$, eine Menge von Schalt-Stationen, betrachtet bezüglich s (für serien-geschaltet) und p (für parallel-geschaltet). Und als Klassiker aller Klassiker sei erwähnt die reelle Achse $\mathbf{R}$, bezüglich ihrer natürlichen Ordnung.

Diese Note strahlt aus in Richtung Analysis, Algebra, Geometrie, Topologie und Kombinatorik unter dem Aspekt der Ordnung und bietet kurze Wege hin zu Themen, die sich nicht zuletzt zu einer vertieften Förderung von Lehramts-Kandidaten eignen dürften. Doch auch zu Bachelor-Arbeiten könnten die nachfolgenden Kapitel als Anregung und Basis dienen, zumal ihr Studium keine besonderen Kenntnisse voraussetzt, wohl aber natürlich eine erste mathematische Schulung. Angeboten werden u. a.:

1. Das Zorn'sche Lemma und das Auswahlaxiom,
2. Eine Fundamental-Gleichung für die Klasse der Verbände,
3. $\mathbf{R}$ als ein ordnungs-theoretisches Erzeugnis,
4. Das Axiom von der oberen Grenze und seine „Geschwister",
5. Eine „Prise" Ω-Analysis,
6. Zum Extremalverhalten beliebiger Funktionen über Ketten,
7. Eine nicht lineare Verbands-Ordnung der reellen Zahlen,
9. Algebra – ganz allgemein,
10. Geometrie – ganz allgemein,

lauter Themen, mit denen der Autor im Rahmen von Seminaren oder Staatsexamens-Arbeiten, auch von mündlichen Vertiefungs-Prüfungen zum Diplom erfreuliche Erfahrungen machen konnte.

Betont werden soll schließlich nachdrücklich, dass diese Note im Verbund mit den einschlägigen Beiträgen der Note [6] studiert werden sollte, wo der Leser

u. a. in die *Boolesche Algebra* als *Aussagen-* und *Schalt-Algebra* eingeführt wird und eine Zusammenstellung interessanter Aufgaben findet.

Mit anderen Worten: es gibt noch mehr „bei uns" zum Thema ORDNUNG.

Kassel, im Herbst 2013

B. B.

Kapitel 1

Posets

1.1 Allgemeines

1. 1. 1 Definition. $(P, \leq) =: \mathfrak{P}$ heißt eine *partial geordnete Menge*, englisch *po-set* bzw. auf „denglisch" *Poset* synonym auch eine *geordnete Menge,* wenn für alle $a, b, c \in P$ gilt:

(R) $a \leq a$

(A) $a \leq b \leq a \Longrightarrow a = b$

(T) $a \leq b \leq c \Longrightarrow a \leq c\,.$

Gilt $a \leq b$ oder $a \geq b$, so nennen wir a und b *vergleichbar.*

Beispiele für partial geordnete Mengen sind etwa die Menge der natürlichen Zahlen, betrachtet bezüglich der Relation „teilt", oder die Menge aller Menschen, betrachtet bezüglich der Relation „ist Nachkomme von".

Sprechweisen für $\leq$ bzw. $\geq$ sind auch: *liegt unterhalb* oder *links von* bzw. *liegt oberhalb* oder *rechts von.*

1. 1. 2 Lemma. *Sei* $\mathfrak{P} =: (P, \leq)$ *eine Poset. Dann ist auch* $(P, \geq)$ *eine Poset.*

BEWEIS. Evident. □

1. 1. 3 Das Hasse-Diagramm. *Ist* $(P, \leq)$ *eine endliche Poset, so lässt sich* $(P, \leq)$ *darstellen durch ein Diagramm.*

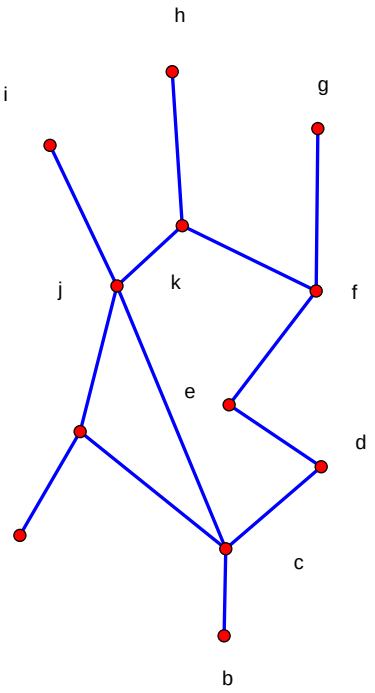


Abbildung 1.1: Ein Hasse-Diagramm

DENN: man ordne jedem $a \in M$ einen Punkt der cartesischen Ebene derart zu, dass sich alle $x \geq a$ „von unten nach oben" erreichen lassen. □

1. 1. 4 Definition. Sei $\mathfrak{P}$ eine Poset. Gilt dann zusätzlich für alle Paare a, b aus P $a \leq b$ oder $b \leq a$, so heißt $\mathfrak{P}$ *total* oder auch *linear* geordnet, auch eine *Kette*.
Gilt hingegen für jedes Paar $a \neq b$ aus P weder $a \leq b$ noch $b \leq a$, so heißt $\mathfrak{P}$ eine *Antikette*.

Mit P wird natürlich auch jedes $Q \subseteq P$ induktiv von $\leq$ partial geordnet. Wird Q hierbei sogar total geordnet, so nennen wir die Menge Q eine *Kette aus* $\mathfrak{P}$. Wird Q hierbei zu einer Antikette geordnet, so nennen wir die Menge Q – analog – eine *Antikette aus* $\mathfrak{P}$.

Offenbar ist eine Teilmenge T von P zugleich Kette und Antikette aus $\mathfrak{P}$ gdw. T ein *singleton* ist.

Ist K eine Kette oder A eine Antikette aus $\mathfrak{P}$, so nennen wir K bzw. A *maximal*, wenn es keine Kette bzw. Antikette in $\mathfrak{P}$ gibt, die K bzw. A – als Menge – echt enthält.

Eine Kette bzw. eine Antikette heiße *längenmaximal*, wenn keine Kette bzw.

Antikette – echt – mehr Elemente enthält. $a \in P$ heißt ein *maximales Element aus* $\mathfrak{P}$, , wenn gilt $x \geq a \Longrightarrow x = a$. Dual erklärt man den Begriff *minimales Element aus* $\mathfrak{P}$.

$s \in P$ heißt eine *obere Schranke* zu der Teilmenge A von P, wenn alle $a \in A$ der Bedingung $a \leq s$ genügen. Dual ist der Begriff *untere Schranke* erklärt.

Schließlich nennen wir A *nach oben begrenzt* (*nach unten begrenzt*), wenn die Menge der oberen Schranken ein (und damit genau ein) kleinstes Element besitzt, das wir dann als die *obere* bzw. *untere Grenze* bzw. als *Supremum,* symbolisch Sup, bzw. *Infimum,* symbolisch Inf bezeichnen.

Ist $\mathfrak{P}$ eine Poset , so lässt sich $\mathfrak{P}$ *zerlegen* in *paarweise disjunkte* Ketten aus $\mathfrak{P}$. Denn, es bildet ja jedes *singleton* aus $\mathfrak{P}$ eine Kette. Liegt eine endliche Zerlegung dieser Art vor, so schreiben wir auch

$$P = K_1 \uplus K_2 \uplus \ldots \uplus K_n$$

und nennen $K_1 \uplus \ldots \uplus K_n$ eine *Kettenzerlegung* von $\mathfrak{P}$ der *Länge* n

Kettenzerlegungen können natürlich unterschiedlich viele *Summanden* aufweisen. So haben wir im Falle einer Kette sogar eine Zerlegung der Länge 1, im Falle einer Antikette hingegen keine Zerlegung außer derjenigen in singletons. In jedem Falle aber besitzt jedes endliche $\mathfrak{P}$ eine Zerlegung minimaler Länge $k(\mathfrak{P})$.

Neben den Ketten aus $\mathfrak{P}$ betrachten wir nun die Antiketten aus $\mathfrak{P}$. Sie können natürlich nicht mehr Elemente besitzen als P. Doch mag es sein, dass keine Antikette mehr als 1 Element besitzt, man betrachte etwa eine Kette.

In jedem Falle aber besitzt ein endliches $\mathfrak{P}$ Antiketten von maximaler Länge. Diese maximale Länge bezeichnet man auch als die *Dimension von* $\mathfrak{P}$*,* abgekürzt als $d(\mathfrak{P})$.

Es wird sich im folgenden zeigen, dass $k(\mathfrak{P})$ und $d(\mathfrak{P})$ in endlichen partial geordneten Mengen stets gleich sind. Dies ist

The celebrated Theorem of DILWORTH

für den endlichen Fall, vergleiche: Annals of Mathematics 1951.

Er soll hier als Einstieg in die Theorie der partial geordneten Mengen dienen. Er ist ebenso zentral wie elementar wie fundamental, ganz zu schweigen von seiner Eleganz und inneren Schönheit. Das sei geschwärmt? Richtig! Schwärmen sei unwissenschaftlich? Falsch, ganz falsch !!!

1. 1. 5 Der Satz von Dilworth. *Sei $\mathfrak{P}$ eine endliche Poset . Dann gilt:*

(DW) $$k(\mathfrak{P}) \;=\; d(\mathfrak{P})\,.$$

BEWEIS. Es gilt natürlich stets

$$k(\mathfrak{P}) \;\geq\; d(\mathfrak{P})\,,$$

denn es kann nicht weniger Summanden in der Kettenzerlegung geben als eine (und damit jede) *längenmaximale Antikette* Elemente besitzt.

Zu zeigen bleibt demnach

$$k(\mathfrak{P}) \;\leq\; d(\mathfrak{P})\,.$$

Hierzu beachten wir, dass die Menge der maximalen Elemente aus $\mathfrak{P}$ eine Antikette bildet, bezeichnet mit A_{max}, und dual die Menge der minimalen Elemente aus $\mathfrak{P}$ eine Antikette bildet, bezeichnet mit A_{min}, und führen den Beweis induktiv.

Offenbar ist der Satz richtig für $|\,P\,| = 1$.

Er sei nun schon bewiesen für alle $|\,P\,| \leq n$, und es sei $\mathfrak{P}$ jetzt von der Mächtigkeit $n+1$.

Wir unterscheiden die beiden einander ausschließenden Fälle

(a) Es existiert eine längenmaximale Antikette A mit $A_{max} \neq A \neq A_{min}$ und

(b) Jede längenmaximale Antikette A aus $\mathfrak{P}$ erfüllt $A = A_{max} \vee A = A_{min}$.

Zu (a): Sei A^0 eine längenmaximale Antikette und $A_{max} \neq A^0 \neq A_{min}$. Wir bilden die Mengen

$$\begin{aligned} A^+ &:= \{x|\, x \geq a \;\; (\exists a \in A^0)\} \\ A^- &:= \{x|\, x \leq a \;\; (\exists a \in A^0)\}\,. \end{aligned}$$

Dann verifiziert man leicht

$$A^+ \cap A^- = A^0 \qquad \text{und} \qquad A^+ \cup A^- = P\,.$$

Weiter haben wir sofort

$$A^+ \neq P \neq A^-\,.$$

Somit erfüllen A^+ und A^- die Induktionsvoraussetzung, was bedeutet, dass es eine Zerlegung von A^+ und dual eine Zerlegung von A^- in $|\,A^0\,|$ viele paarweise disjunkte Ketten gibt, die jeweils genau ein Element aus A^0 enthalten, da A^0 ja auch Antikette zu A^+ und A^- ist.

Das bedeutet aber, dass sich diese Ketten zusammenlegen lassen zu $|\,A^0\,|$ vielen paarweise disjunkten Ketten von $\mathfrak{P}$. Damit ist eine disjunkte Zerlegung mit $d(\mathfrak{P})$ Summanden gefunden , also haben wir $k(\mathfrak{P}) \leq d(\mathfrak{P})$.

Zu (b): Nach Voraussetzung gibt es in diesem Falle keine längenmaximale Antikette, zugleich verschieden von A_{max} und A_{min}. Also dürfen wir o. B. d. A. annehmen, dass A_{max} eine längenmaximale Antikette ist und jede längenmaximale Antikette A der Bedingung $A_{max} = A \vee A = A_{min}$ genügt.

Dann existiert eine maximale[1)] Kette K mit – etwa $g \in A_{max}$ – als größtem und $k \in A_{min}$ als kleinstem Element, und wir können $\mathfrak{P}$ zerlegen in $K \uplus P \setminus K$ bzw. mit $R := P \setminus K$ in $K \uplus R$.

Nun gilt nach Induktionsvoraussetzung der Satz für $\mathfrak{R}$, da R mindestens ein Element weniger als P besitzt.

Also sind wir am Ziel, wenn wir zeigen können, dass $A_{max} \setminus \{g\}$ eine längenmaximale Antikette in R ist. Denn dann lässt sich $\mathfrak{R}$ ja in $(|A_{max}| - 1)$ viele Ketten zerlegen und damit $\mathfrak{P}$ in $|A_{max}|$ viele, was $k(\mathfrak{P}) \leq d(\mathfrak{P})$ liefert.

Wäre $A_{max} - \{g\}$ aber nicht längenmaximal in $\mathfrak{R}$, so gäbe es in $\mathfrak{R}$ eine Antikette A_R von der Länge $|\,A_{max}\,|$, weshalb diese Antikette auch eine Antikette maximaler Länge von $\mathfrak{P}$ wäre mit Widerspruch, denn sie ist ja in $\mathfrak{P}$ verschieden von A_{max}, wegen $g \notin A_R$, und verschieden von A_{min}, wegen $k \notin A_R$. □

1.2 Das Zorn'sche Lemma

Hatten wir es im vorauf gegangenen Abschnitt vornehmlich mit endlichen Posets zu tun, wenden wir uns nun beliebigen Posets zu.

Dabei beginnen wir mit einem „Endlichkeitsersatz", benannt nach dem „in Konkurrenz mit Euklid" wohl am häufigsten zitierten Mathematiker.

[1)] es würde etwas weniger genügen, die maximale Kette erleichtert aber die Formulierung

1. 2. 1 (ZL) Das Zorn'sche Lemma. *Sei $\mathfrak{P}$ eine nicht leere Poset, deren Ketten nach oben begrenzt sind. Dann enthält $\mathfrak{P}$ mindestens ein maximales Element.*

Später werden wir zeigen, dass **(ZL)** äquivalent ist zu dem nachfolgenden Auswahlaxiom

1. 2. 2 (AC) Das Auswahlaxiom. *Sei $\{A_i\}$ $(i \in I)$ eine Familie paarweise disjunkter nicht leerer Mengen. Dann existiert eine Menge A, die aus jedem A_i genau ein Element enthält.*

Genauer müsste man von Zorn's Prinzip sprechen. In seiner Arbeit [41] zeigte Zorn, dass das Maximum-Prinzip, besagend dass jedes Mengen-System, das zusammen mit jeder Kette auch die Vereinigung seiner Glieder enthält, mindestens ein maximale Menge enthält, in vielen Situationen der abstrakten Mathematik zu Resultaten führt, die zu jener Zeit mittels des Auswahlaxioms bewiesen waren, siehe weiter unten. Wie der Leser leicht sieht, folgt dies aus dem Umstand, dass **(ZL)** $\Longrightarrow$ **(AC)** fast evident ist – man betrachte das System aller Mengen, die aus jedem A_i höchstens ein Element enthalten, während der Nachweis **(AC)** $\Longrightarrow$ **(ZL)** einigen Scharfsinn und einige Kraft erfordert.

Dies bedeutet, dass bei Zugrundelegung von **(ZL)** dieser Scharfsinn und diese Kraft implizit wirkt und gelegentlich zu einer extremen Abkürzung führt.

Als Beispiele, die wir hier dem Leser überlassen, seien genannt: der Basissatz der Linearen Algebra und der Satz vom maximalen Ideal für Ringe mit 1.

Eine andere, offenbar logisch gleichwertige Aussage zum **(ZL)**, ist

1. 2. 3 (HK) Das Theorem von Hausdorff/Kuratowski. *Jede Poset besitzt eine maximale Kette.*

Heute allerdings ist die Zorn'sche Formulierung Standard.

Wir wollen uns hier auf diese wenigen Informationen beschränken. Später werden wir noch den *Wohlordnungssatz* kennen lernen. Auch werden wir das Zorn'sche Lemma an einigen Stellen anwenden.

Der echte Freak sei hingegen auf Rubin/Rubin [35]. verwiesen, wo mehr als 200 Äquivalenzen vorgestellt werden, verstreut über fast alle Gebiete der abstrakten Mathematik.

Mit Blick auf **(ZL)** $\Longleftrightarrow$ **(AC)** ist die Implikation **(ZL)** $\Longrightarrow$ **(AC)** fast evident, wie schon oben angedeutet.

Daher bleibt zu zeigen:

1. 2. 4 Theorem. $\qquad$ **(AC)** $\Longrightarrow$ **(ZL)**

BEWEIS. Wir führen den Beweis nach HELLMUTH KNESER, [24] in Anlehnung an HERMES in [22].

Dabei gehen wir aus von einer Poset $\mathfrak{H} = (H, \leq)$ ohne maximales Element, dessen nicht leeren Ketten K jeweils durch $g(K)$ nach oben begrenzt seien, um später zu zeigen, dass diese Annahme zum Widerspruch führt.

Weiter bilden wir zu jedem $x \in H$ die Menge $s(x) := \{y \,|\, y > x\}$, und wir bezeichnen die Menge all dieser $S(x)$ mit M.

Dann existiert wegen **AC** zu M eine Funktion φ mit $\varphi(S(x)) := f(x) \in S(x)$. Dies bedeutet insbesondere

$$x < f(x) \,.$$

Schließlich wählen und fixieren wir ein Element $a_0 \in H$.

Auf der Basis dieser „Ingredienzen" argumentieren wir nun wie folgt:

Wir bezeichnen als eine Zorn'sche Menge jedes $Z \subseteq H$, das die drei nachfolgenden Bedingungen (i) bis (iii) erfüllt:

(i) $\quad a_0 \in Z$.

(ii) $\quad x \in Z \Longrightarrow f(x) \in Z$.

(iii) $\quad \emptyset \neq K(\text{ette}) \subseteq H \Longrightarrow g(K) \in Z$.

Triviale Zorn'sche Mengen sind H selbst oder auch $[a_0) := \{x \,|\, a_0 \leq x\}$. Weiterhin ist der Durchschnitt Z_0 aller Zorn'schen Mengen offenbar eine Zorn'sche Menge. Folglich ist Z_0 die engste Zorn'schen Menge und jedes Element von Z_0 liegt oberhalb von a_0, da $[a_0)$ zum Durchschnitt *beiträgt*.

Wir werden zeigen, dass Z_0 sogar eine Kette ist. Das schließt den Beweis dann ab, da (Z_0) nach (ii) das Element $f(g(Z_0)) > g(Z_0)$ enthalten müsste, mit Widerspruch zur sup-Eigenschaft von $g(Z_0)$.

AUSFÜHRUNG: Sei im weiteren z stets ein Element aus Z_0. Ein Element $a \in Z_0$ soll *ausgezeichnet* heißen, wenn es $z < a \Longrightarrow f(z) \leq a$ erfüllt.

Offenbar ist a_0 eine ausgezeichnetes Element, da kein $z < a_0$ existiert.

Wir assoziieren nun mit jedem ausgezeichneten Element a die Menge

$$B(a) := \{z \in Z_0 \,\big|\, z \leq a \vee f(a) \leq z\} \subseteq Z_0$$

und betrachten ein solches ausgezeichnetes Element a. Dann folgt

(a) $a_0 \in B(a)$, wegen $a_0 \leq a$.

(b) Im Falle $z \in B(a)$ gilt einer der drei nachfolgenden Fälle:

$$(i) \quad z < a \ , \qquad (ii) \quad z = a \ , \qquad (iii) \quad f(a) \leq z \, ,$$

denn im Falle (i) schließen wir $f(z) \leq a$, da a ausgezeichnet ist, und in den beiden anderen Fällen folgern wir sofort $f(a) \leq f(z)$.

Das bedeutet dann, dass in jedem der drei Fälle $f(z) \in B(a)$ resultiert.

(c) Sei hiernach K eine nicht leere Kette von Elementen aus $B(a)$.

Wir unterscheiden

Fall 1. Es liegen alle Elemente aus K unterhalb von a.

Dann liegt auch $g(K) \leq a$ unterhalb von a, also wegen $g(K) \in Z_0$ dann auch $g(K)$ in $B(a)$.

Fall 2. Es existiert ein $k \in K$, das nicht unterhalb von a liegt.

Dann folgt $f(a) \leq k \leq g(K)$, weshalb erneut $g(K)$ in $B(a)$ liegt.

Kombinieren wir nun (a), (b), (c), so folgt, dass $B(a)$ eine Zorn'sche Menge bildet, woraus weiter $Z_0 \subseteq B(a)$ resultiert. Das bedeutet aber insbesondere, dass jedes ausgezeichnete Element a vergleichbar ist mit jedem Element aus Z_0.

In einem letzten Schritt zeigen wir nun, dass die Menge A aller ausgezeichneten Elemente eine Zorn'sche Menge bilden, was zu $Z_0 = B(a)$ und damit zur Vergleichbarkeit eines jeden Paares a, b von ausgezeichneten Elementen führt.

(a) a_0 ist ausgezeichnet, wie oben gezeigt wurde.

(b) Sei nun a ausgezeichnet. Dann ist auch $f(a)$ ausgezeichnet.

DENN, man betrachte ein $z < f(a)$. Nach unseren bisherigen Ausführungen gehört z zu $B(a) = Z_0$. Daher ist $z \leq a$ oder $f(a) \leq z$. Das bedeutet aber im vorliegenden Fall $z \leq a$.

Sei zunächst $z = a$. Dann ist nichts mehr zu zeigen.

Sei hiernach $z < a$. Dann folgt $f(z) \leq a < f(a)$, da a ausgezeichnet ist.

(c) Sei schließlich K eine nicht leere Kette ausgezeichneter Elemente. Wir haben noch zu zeigen, dass dann auch $g(K)$ ausgezeichnet ist. Natürlich liegt $g(K)$ in Z_0, da alle ausgezeichneten Elemente zu Z_0 gehören.

We betrachten nun ein $z < g(K)$.

Existiert dann ein $k > z$ in K, so folgt $f(z) \leq k$, da k ausgezeichnet ist, und deshalb dann auch $f(z) \leq g(K)$.

Andernfalls aber kommt es zum Widerspruch:

DENN: Alle $k \in K$ sind ausgezeichnet. Folglich ist jedes k vergleichbar mit jedem z. Also wäre in diesem (Gegen-) Fall z eine obere Schranke von K und daher $g(K) \leq z$ mit Widerspruch zu $z < g(K)$.

DAMIT GILT: Die Menge aller ausgezeichneten Elemente bildet eine Zorn' sche Menge und ist damit gleich Z_0. Das aber bedeutet, dass jedes Element aus Z_0 ausgezeichnet und folglich vergleichbar mit jedem anderen Element aus Z_0 ist.

FAZIT: Z_0 ist eine Kette und $g(Z_0)$ ist maximal in $(H, \leq)$. □

Wie beenden diesen Abschnitt mit einem Satz über vollständige partial geordnete Mengen, das sind Posets, in denen zu jeder Teilmenge das Supremum existiert. Als klassische Beispiele seien genannt: die abgeschlossenen Einheitsintervalle $I = [\,a, b\,]$ und die Potenzmengen $\mathcal{P}(M)$.

Für solche Posets gilt:

1. 2. 5 Ein Fixpunktsatz. *Sei $\mathfrak{P}$ eine nicht leere vollständige Poset mit Minimum 0 und Maximum 1 sowie $f : P \to P$ eine monotone Funktion $(a \leq b \Longrightarrow f(a) \leq f(b))$. Dann besitzt f mindestens einen Fixpunkt.*

DENN: Sei A die Teilmenge aller Elemente mit $a \leq f(a)$ – diese Menge ist nicht leer, es gehört ja mindestens 0 zu ihr – und sei Ω das Supremum dieser Menge. Dann gehört mit jedem a auch $f(a)$ zu A, klar. Also folgt $a \leq f(a) \leq \Omega \Longrightarrow a \leq f(a) \leq f(f(a)) \leq f(\Omega)$ und damit $\Omega \leq f(\Omega)$.

Es kann aber nicht $\Omega < f(\Omega)$ gelten, da dann auch $f(\Omega)$ zu A gehören würde, mit Widerspruch zur Bedeutung von Ω. □

Als eine Anwendung des soeben vorgestellten Fixpunktsatzes bringen wir nun einen alternativen Beweis zum

1. 2. 6 Satz von Bernstein. *Seien E und F zwei Mengen. Sind dann die Abbildungen $f : E \longmapsto F$ und $g : F \longmapsto E$ jeweils injektiv, so folgt $|E| = |F|$.*

BEWEIS. Wir bezeichnen die Funktion, die jeder Teilmenge einer Menge X ihr Komplement zuordnet mit c_X und betrachten die Abbildung $\zeta : \mathcal{P}(E) \longmapsto \mathcal{P}(E)$, gegeben vermöge

$$\zeta := f \circ c_F \circ g \circ c_E \,,$$

Diese Abbildung ist isoton und besitzt demzufolge ein Fixelement $G \subseteq E$, das also

$$G(f \circ c_F \circ g \circ c_E) = c_E(g(c_F(f(G)))) = G,$$

erfüllt. Dann gilt aber $c_E(G) = g(c_F(f(G)))$, vgl. Abb. 1.2 mit $G, B = f(G), C = c_F(f(G)), D = g(c_F(f(G)))$,

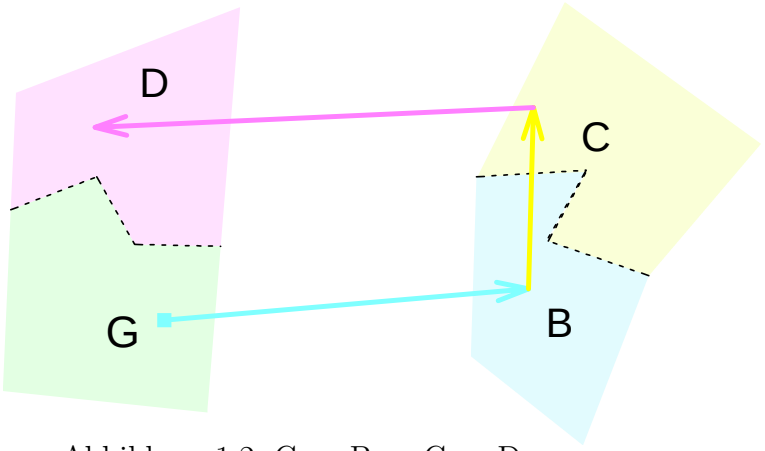


Abbildung 1.2: G⟼B⟼C⟼D

und das bedeutet, dass jedes $x \in c_E(G)$ als Bild unter g erfasst wird, also, dass in $c_F(f(G))$ ein (eindeutig bestimmtes) $g^{\leftarrow}(x)$ existiert, so dass die Festsetzung

$$h(x) \;\; (x \in E) \;\; := \begin{cases} f(x) & , \text{falls } x \in G \\ g^{\leftarrow}(x) & , \text{falls } x \notin G \end{cases}$$

eine Bijektion von E auf F liefert. □

1.3 Zur Darstellung von Posets

Ist $\mathfrak{P} = (P, \leq)$ eine Poset, so ist $\leq$ definitionsgemäß eine zweistellige Relation, also eine Teilmenge von $P \times P$. Folglich können wir Posets behandeln wie Mengen. So macht es u. a. Sinn, vom Durchschnitt $\bigcap \leq_i \ (i \in I)$ zu sprechen.

Das Ziel dieses Abschnitts ist nun ein doppeltes.

Zum einen werden wir zeigen, dass jede Partialordnung auf P sich auffassen lässt als Durchschnitt von Totalordnungen.

Zum anderen werden wir zeigen, dass sich jedes $\mathfrak{P}$ auffassen lässt als ein *Mengensystem*, betrachtet bezüglich der *Inklusion*.

An den Anfang sei ein Satz gestellt, der im Alltag immer wieder indirekt bemüht wird.

Häufig ist eine Menge von Objekten oder auch von Subjekten auf höchst natürliche Weise (partial) geordnet, gefordert wird aber, etwa von einer Institution, eine (lineare) *Reihung* bzw. eine Entscheidung für eine Person, so dass weitere – und nicht selten – *sehr subjektive* Argumente verdeckt oder versteckt in den Entscheidungsprozess einfließen, man denke in Ruhe über seine Selbsterfahrungen nach ....

Abstrakt bedeutet dies, dass Elemente künstlich verglichen werden, die (vorher) unvergleichbar waren (schienen), was aber immer möglich ist. Denn, es gilt:

1. 3. 1 Der Ausdehungssatz. *Sei $\leq$ eine Partialordnung auf P. Dann lässt sich $\leq$ einbetten in eine Totalordnung auf P.*

BEWEIS. Offenbar erfüllt die Menge aller Partialordnungen auf P, die $\leq$ als Teilmenge enthalten, die Bedingungen des ZORNschen LEMMAS. Also gibt es eine maximale $\leq$ enthaltende Partialordnung auf P, etwa $\ll$.

Wir zeigen, dass $\ll$ eine Totalordnung ist.

Wäre dies nicht der Fall, so gäbe es in P bezüglich $\ll$ unvergleichbare Elemente, etwa a, b.

Wir setzen nun $x \preceq y$ genau dann, wenn $x \ll y$ oder aber $x \ll a \ \ \& \ \ b \ll y$ erfüllt ist. Dann verifiziert der Leser leicht, dass die so definierte Relation in der Tat eine Partialordnung wäre, die $\ll$ als echte Teilmenge enthielte, mit Widerspruch zur Maximalität von $\ll$.

Folglich ist $\ll$ eine Totalordnung. $\square$

Aus diesem Ausdehnungssatz folgt leicht

1. 3. 2 Der Durchschnittssatz. *Sei $\leq$ eine Partialordnung auf P. Dann lässt sich $\leq$ auffassen als Durchschnitt von Totalordnungen auf P.*

BEWEIS. Wir bilden den Durchschnitt τ aller Totalordnungen, die $\leq$ enthalten. Er existiert natürlich, ist offenbar eine Partialordnung und enthält $\leq$. Wäre nun etwa $(a, b) \in \tau$, aber $(a, b) \notin \leq$, so könnte auch nicht $(b, a) \in \leq$ erfüllt sein, da sonst (b, a) auch in τ läge, mit Widerspruch zu $(a, b) \in \tau$. Damit wären a und b in $\leq$ unvergleichbar. Das würde dann aber nach Proposition 1.3.1 eine Ausdehnungsmöglichkeit von $\leq$ *via* $b \ll a$ bedeuten, wie im letzten Satz gezeigt, was zu einem Widerspruch führt. Denn mit $(a, b) \in \tau \subseteq \ll$, kann nicht auch $(b, a) \in \ll$ gelten. $\square$

Im zweiten Teil dieses Abschnitts befassen wir uns mit der *Darstellung* von Posets. Zum Problem der Darstellung einige Anmerkungen vorweg:

Ist $\mathfrak{S}$ irgendeine *Struktur,* etwa ein *Vektorraum* oder eine *Gruppe* oder ein *Ring* oder ein *topologischer Raum* oder ein *Verband* oder aber auch eine Poset, so sind die Elemente dieser Struktur in der Regel inhaltlich völlig undefiniert. Gelingt es aber zu zeigen, dass die vorgegebene (abstrakte) Struktur isomorph ist zu einer konkreten Struktur, so können hieraus Vorteile für die weitere Behandlung bzw. Untersuchung dieser Struktur erwachsen.

Dies sei erläutert am Beispiel *endlich erzeugter Vektorräume.*

Zunächst geht man aus von einem abstrakten Vektorraum. Es zeigt sich dann aber, dass er eine *Basis* besitzt, was dazu führt, dass wir die Vektoren des vorgegebenen Raumes auch auffassen können als *n-Tupel von Skalaren* des zugrunde liegenden *Skalarenkörpers.* Hierdurch wird der vorgegebene abstrakte Vektorraum konkret, zumindest so konkret wie der unterliegende Skalaren-Körper. Und noch jeder Student hat diesen Sachverhalt erleichtert zur Kenntnis genommen.

Ähnliches wäre zu sagen zur Darstellung des Vektorraums der *linearen Abbildungen* von einem $\mathfrak{K}^m$ in einen $\mathfrak{K}^n$, der sich auffassen lässt als ein Vektorraum von *Matrizen.*

An dieser Stelle nun gilt es, *geordnete* Mengen zu *repräsentieren.* Der Wert dieser Prozedur wird natürlich einmal in den Resultaten und gewissen An-

wendungen liegen. Doch kann darüber hinaus der wissenschafts-didaktische Wert der nachfolgenden Passagen gar nicht überschätzt werden. Denn es wird eine extrem elementare Methode alles Wesentliche eines Darstellungsvorgangs beinhalten.

Die Grundidee ist einfach. Wir möchten die Elemente aus P *kodieren* mittels geeigneter *Dualfolgen,* d.h. $0,1$-*Folgen.* Dies wird uns im Nachhinein weitere Darstellungsmöglichkeiten eröffnen.

1. 3. 3 Definition. Sei $\mathfrak{P}$ eine Poset. Dann verstehen wir unter einem *Ordnungsfilter* von $\mathfrak{P}$ jede Teilmenge aus P, die mit jedem Element x auch alle Elemente oberhalb von x enthält. Dual verstehen wir unter einem *Ordnungsideal* jede Teilmenge aus P, die mit jedem Element y auch alle Elemente unterhalb von y enthält.

Ist insbesondere $F = [x) := \{u \,|\, x \leq u\}$, so nennen wir F einen *Hauptfilter*, und wir erklären dual den Begriff des *Hauptideals.*

Offenbar ist das *Mengenkomplement* eines jeden nicht leeren Ordnungsfilters ein Ordnungsideal und das *Mengenkomplement* eines jeden nicht leeren Ordnungsideals ein Ordnungsfilter.

Auch sehen wir sofort, dass es – knapp gesagt – *genug* Ideale und Filter gibt, was meint, dass es zu jedem Paar $a \neq b$ mindestens ein Ideal und mindestens einen Filter gibt, derart dass eins der beiden Elemente in diesem Ideal (Filter) liegt, das andere hingegen nicht, oder?

Wir betrachten die Menge aller *Filter/Ideal-Zerlegungen* $P = A_i \dot{+} B_i \ \ (i \in I)$. Für ein fest vorgegebenes $x \in P$ gilt dann jeweils $x \in A_i \ aut^{2)} x \in B_i$.

Das bedeutet aber, dass die Abbildung $f_x : i \longmapsto x_i \in \{0,1\}$ mit

$$\begin{aligned} f_x(i) &= x_i = 1 \Longleftrightarrow x \in A_i \\ f_x(i) &= x_i = 0 \Longleftrightarrow x \notin A_i \end{aligned}$$

eine eindeutige Kodierung für das Element x liefert und zwar derart, dass

$$x \leq y \Longleftrightarrow x_i \leq y_i \ \ (\forall i \in I)$$

erfüllt ist.

[2)] Gemeint ist hiermit das „ausschließende oder" des Lateiners, d.h. das „entweder oder", i.S. von „entweder das eine oder das andere, nicht aber beides zugleich".

Damit hat sich ergeben

1. 3. 4 Der Darstellungssatz. *Jede Poset lässt sich auffassen als eine Menge von* $0, 1$*-Folgen, betrachtet bezüglich des* Komponentenvergleichs.

Und dies impliziert:

Jede Poset lässt sich auffassen als ein Mengensystem, betrachtet bezüglich der Inklusion.

BEWEIS. Teil 1 ist nach der oben beschriebenen Konstruktion klar.

Zum Nachweis von Teil 2 ordnen wir jeder Folge $\{x_i\}$ diejenige Teilmenge von I zu, die genau jene i enthält, für die $x_i = 1$ erfüllt ist. □

HINWEIS: Angemerkt werden sollte noch, dass die Menge der Filter und dual die Menge der Ideale einer Poset abgeschlossen ist bezüglich $\bigcap$ und $\bigcup$. Somit hätten wir auch zunächst zeigen können, dass sich jede Poset auffassen lässt als ein System von Mengen, betrachtet bezüglich der Inklusion. Dabei wären dann die Elemente aus $\mathfrak{P}$ repräsentiert durch die Hauptfilter bzw. Hauptideale aus $\mathfrak{P}$ und wir erhielten eine Kodierung der Elemente durch Zugrundelegung der Menge aller Filter bzw. Ideale als Menge I.

Kapitel 2

Total geordnete Mengen

2.1 Wohlgeordnete Mengen

Eine Poset heißt *wohlgeordnet*, wenn jede nichtleere Teilmenge ein kleinstes Element besitzt. In diesem Abschnitt sollen einige grundlegende Fakten über wohlgeordnete Mengen zusammengestellt werden.

Sei also im folgenden $(W, <) =: \mathfrak{W}$ eine wohlgeordnete Menge. Dann ist $(W, \leq)$ natürlich total geordnet.

2. 1. 1 Definition. Wir nennen $A \subseteq W$ einen *Anfang* von $\mathfrak{W}$, wenn A ein *Ordnungsideal* ist, also $y < x \in A \Longrightarrow y \in A$ erfüllt.

Ist A sogar vom Typ $A(a) := \{x | x < a\}$, so nennen wir A den von a erzeugten *Abschnitt*.

Zur Unterscheidung von den Mengen A bzw. $A(x)$ bezeichnen wir $(A, <)$ mit $\mathfrak{A}$ und $(A(x), <)$ mit $\mathfrak{A}(x)$.

Ist $A \neq W$, so gibt es unter den Elementen aus $W \setminus A$ ein *erstes* Element, das A dann als Abschnitt erzeugt. Dies bedeutet, dass jeder Anfang von $\mathfrak{W}$, der W nicht ausschöpft, ein Abschnitt von $\mathfrak{W}$ ist. Umgekehrt ist jeder Abschnitt von $\mathfrak{W}$ ein Anfang von $\mathfrak{W}$.

2. 1. 2 Definition. Seien hiernach $\mathfrak{U} = (U, <_U)$ und $\mathfrak{V} = (V, <_V)$ zwei wohlgeordnete Mengen. Dann heißen $\mathfrak{U}$ und $\mathfrak{V}$ *(ordnungs-) ähnlich,* i.Z. $\mathfrak{U} \cong \mathfrak{V}$, wenn es mindestens einen *Ordnungsisomorphismus*, d.h. eine ordnungserhaltende bijektive Abbildung von $\mathfrak{U}$ auf $\mathfrak{V}$ gibt.

Wie man sofort sieht, ist $\cong$ eine Äquivalenzrelation. Daher stiftet $\cong$ unter den wohlgeordneten Mengen Klassen ähnlicher Mengen, die wir als *Ordinalzahlen* bezeichnen wollen. Eine *Ordinal-* oder auch *Ordnungszahl* ist demzufolge nichts anderes als ein $\mathfrak{W}_{\cong}$. Als Symbole für Ordinalzahlen wählt man in der Regel griechische Buchstaben oder auch für *die ersten Ordinalzahlen* die Bezeichnungen der natürlichen Zahlen. Als festgelegt gilt weiter ω als die Bezeichnung der von $\mathbf{N}$ *gestifteten* Ordinalzahl.

Aus Gründen der Praktikabilität wollen wir in diesem Abschnitt jedoch die von der wohlgeordneten Menge $\mathfrak{W}$ gestiftete Ordinalzahl mit $\mathfrak{W}_0$ bezeichnen.

Um den Namen Ordinalzahl zu rechtfertigen, haben wir zumindest nachzuweisen, dass jede Menge von Ordinalzahlen eine kleinste Ordinalzahl enthält, was einschließt, dass je zwei Ordinalzahlen vergleichbar sind und dass wir entlang der Reihe der Ordinalzahlen zu *zählen* vermögen. Wir beginnen hierzu mit einem

2. 1. 3 Lemma. *Seien $A(x)$ und $A(y)$ zwei Abschnitte der wohlgeordneten Menge $\mathfrak{W}$. Dann gilt*

$$A(x) \cong A(y) \Longrightarrow x = y\,. \tag{2.1}$$

BEWEIS. Wäre o. B. d. A. $x < y$, so läge x in $A(y)$, d. h. so wäre $x = f(u)$ mit u aus $A(x)$, also $u \in A(x) \rightsquigarrow u < x = f(u)$ erfüllt. Somit gäbe es auch ein *erstes* $z \in A(x)$ mit $z < f(z)$. Dann wäre dieses z aber als Bild nicht berücksichtigt, da die kleineren Elemente aus $A(x)$ von dem Ordnungsisomorphismus f auf sich selbst und die größeren Elemente auf größere Elemente als x abgebildet würden, mit Widerspruch. □

Mitgeliefert hat das letzte Lemma

2. 1. 4 Korollar. *Bildet f die wohlgeordnete Menge $\mathfrak{U}$ ähnlich ab auf die wohlgeordnete Menge $\mathfrak{V}$, so gibt es keine weitere Ähnlichkeitsabbildung von $\mathfrak{U}$ auf $\mathfrak{V}$.*

DENN: Gäbe es eine weitere Ähnlichkeitsabbildung g, o.B.d.A. mit $\exists x \in U$: $f(x) < g(x)$, so ergäbe sich $\mathfrak{A}(f(x)) \cong \mathfrak{A}(x) \cong \mathfrak{A}(g(x))$ & $f(x) \neq g(x)$ mit Widerspruch zu 2.1.3. □

Totalgeordnete Mengen, die neben der Identischen Abbildung keinen weiteren Ordnungs-Automorphismus besitzen, heißen *rigide totalgeordnet.*

FRAGE: Gibt es neben den wohlgeordneten Mengen noch andere rigide linear geordnete Mengen?

ANTWORT: Ja, und dies sollte ein Seminarthema sein.

2. 1. 5 Proposition. *Sind* $\mathfrak{U}$ *und* $\mathfrak{V}$ *zwei wohlgeordnete Mengen, so gilt genau eine der drei Beziehungen:*

$$\begin{aligned} \mathfrak{U} &\cong \mathfrak{A}(b) \;\&\; A(b) \subseteq V \\ \mathfrak{U} &\cong \mathfrak{V} \\ U \supseteq A(a) \;\&\; \mathfrak{A}(a) &\cong \mathfrak{V}\,. \end{aligned}$$

BEWEIS. Zunächst ist nach 2.1.4 klar, dass *höchstens* eine der drei Aussagen zutreffen kann. Zu zeigen bleibt also, dass *mindestens* eine der drei Aussagen zutrifft.

Wir betrachten zunächst die Elemente 0_U und 0_V. Sie liefern *via* $f(0_U) := 0_V$ ein Paar von Elementen $x \in U\,,\ f(x) \in V$ mit $\mathfrak{A}(0_U) \cong \mathfrak{A}(f(0_U))$.

Hiernach betrachten wir die Menge X aller $x \in U$ zu denen in V ein y existiert mit

$$\mathfrak{A}(x) \;\cong\; \mathfrak{A}(y)\,.$$

Ist x, y ein Paar dieser Art, so ist y eindeutig bestimmt, da es sonst in $\mathfrak{V}$ zwei ähnliche Abschnitte gäbe, die von verschiedenen Elementen erzeugt würden, mit Widerspruch zu 2.1.3

Ferner ist unmittelbar klar, dass X einen Anfang von $\mathfrak{U}$ und die Menge Y aller erfassten y einen Anfang von $\mathfrak{V}$ bildet. Wir setzen nun für die Menge aller $x \in X$:

$$f(x) \;:=\; y$$

mit dem eindeutig bestimmten $y \in V$. Auf diese Weise wird ein Anfang von $\mathfrak{U}$, nämlich X, ähnlich abgebildet auf einen Anfang von $\mathfrak{V}$, nämlich $f(X)$.

Schöpft nun X ganz U aus, so tritt der erste oder der zweite Fall ein, und schöpft Y ganz V aus, so tritt der zweite oder der dritte Fall ein.

Würde aber X nicht ganz U und zugleich Y nicht ganz V ausschöpfen, so käme es bei *Anhängen* der ersten Elemente aus $U \setminus A$ bzw. $V \setminus f(A)$ zum Widerspruch. □

Hiernach können wir unter den Ordinalzahlen, deren *Repräsentanten* ähnlich sind zu einem Anfang von $\mathfrak{W}$, eine *natürliche* Wohlordnung stiften, indem wir festsetzen:

2. 1. 6 Definition. Sind $\mathfrak{U}_0$ und $\mathfrak{V}_0$ zwei Ordinalzahlen, so setzen wir genau dann $\mathfrak{U}_0 < \mathfrak{V}_0$, wenn es Repräsentanten $\mathfrak{U}$ von $\mathfrak{U}_0$ und $\mathfrak{V} = \mathfrak{A}(x)$ $(x \in V)$ von $\mathfrak{V}_0$ gibt mit

$$\mathfrak{U} \cong \mathfrak{A}(x)\,.$$

Wie man sofort sieht ist die soeben getroffene Definition unabhängig von der Wahl der Repräsentanten und es stiftet, wie aus der vorhergehenden Proposition folgt, die erklärte Relation eine lineare Ordnung.

Zu zeigen bleibt also, dass die Menge der Ordinalzahlen unterhalb von $\mathfrak{W}$ sogar wohlgeordnet ist bezüglich $<$. Dies ergibt sich aber unmittelbar daraus, dass die Menge der Abschnitte von $\mathfrak{W}$ wohlgeordnet ist.

Daher können wir resümieren:

2. 1. 7 Theorem. *Ist $\mathfrak{W}$ wohlgeordnet, so ist die Menge der Ordinalzahlen unterhalb von $\mathfrak{W}_0$ ebenfalls wohlgeordnet.*

Die Menge der Ordinalzahlen unterhalb von $\mathfrak{W}_0$ gibt uns u.a. eine Möglichkeit an die Hand, *transfinit induktiv* zu definieren, indem wir festlegen, was $\mathrm{D}(0)$ sein soll und was $\mathrm{D}(\tau)$ sein soll, sofern $\mathrm{D}(\sigma)$ (schon) für alle $\sigma < \tau$ erklärt ist.

Neben dieser Möglichkeit der *transfiniten Definition* erlaubt uns die Wohlordnung einer Menge das Verfahren der transfiniten Induktion. Sie besagt:

2. 1. 8 Lemma. *Sei $\mathfrak{W}$ wohlgeordnet und sei E eine Eigenschaft, die dem ersten Element aus $\mathfrak{W}$ zukommt und die sich bei Gültigkeit für alle $x \in A(b)$ überträgt auf b. Dann besitzt jedes $x \in W$ die Eigenschaft E.*

Die Gültigkeit dieses Lemmas ist evident. Denn, andernfalls gäbe es ein erstes Element in $\mathfrak{W}$, für das die Aussage nicht zuträfe.

Im übrigen wurde diese transfinite Induktion bereits oben der Idee nach eingesetzt.

Natürlich stellt sich die Frage, welche Mengen eine Wohlordnung zulassen.

Georg Cantor war wohl davon überzeugt, dass dies für jede Menge zutrifft seine Idee: Wähle ein erstes Element, hiernach ein zweites Element,...., und wähle – sobald auf diese Weise eine wohlgeordnete Teilmenge ausgesondert wurde, als nächstes ein Element aus der korrespondierenden Restmenge.

Doch erst Ernst Zermelo hat die Verhältnisse klar analysiert. Die Grundidee war natürlich angemessen, doch hatte man vor Zermelo nicht klar genug

begriffen, dass die hingenommene Auswahl eine Auswahlmenge voraussetzte, deren Annahme einen mutigen Schritt erforderte. Denn, betrachten wir etwa **N**, so lässt sich jeder nicht leeren Teilmenge von **N** ihr kleinstes Element zuordnen. Was aber im Falle **Q**? Auch hier gelangen wir zum Erfolg. Wir wählen aus jeder nicht leeren Teilmenge T die Menge aller Brüche $\frac{a}{b} \in T$ von minimalem $a + b$ aus und definieren dann denjenigen unter diesen Brüchen mit dem kleinsten Nenner als $f(T)$.

Doch was tun im Falle **R**?

Bertrand Russel hat dem Problem eine wunderbare Einkleidung gegeben, siehe oben, verständlich für jedermann:

Gegeben eine unendliche Menge von Paaren von Schuhen, wir wählen aus jedem Paar den linken Schuh.

Aber, was im Fall einer unendlichen Menge von Paaren von Socken?

Der Leser beachte: eine Auswahlmenge ist im Vorhinein zu definieren, nicht sukzessive zu generieren. Der Grund? Schritt für Schritt würden wir über abzählbar viele Elemente niemals hinaus gelangen. Doch nicht jede Menge ist abzählbar, wie wir schon gesehen haben.

Mit anderen Worten: Wir dürfen nicht mehr erwarten, als dass sich jede Menge wohlordnen lässt, zu der sich eine Auswahlfunktion $f : \mathcal{P}(M) \to M$ mit $f(A) \in A \ (\forall : \emptyset \neq A \subseteq M)$ finden lässt. Unter dieser Prämisse aber gilt

2. 1. 9 Der Wohlordnungssatz von Ernst Zermelo. *: Sei M eine nicht leere Menge und sei $f : \mathcal{P}(M) \to M$ eine Auswahlfunktion zu M. Dann lässt M eine Wohlordnung zu – und umgekehrt.*

BEWEIS. (a) Die eine Richtung ist evident.

(b) Wir betrachten die Menge $W(M) =: W$ aller wohlgeordneten Mengen $(A, <_A)$ mit $A \subseteq M$. Diese Menge ist nicht leer, denn jedes $\{a\} \subseteq M$ ist ja wohlgeordnet. Auf W definieren wir eine Partialordnung $\lhd$ vermöge der Festsetzung

$$(A, <_A) \lhd (B, <_B) \text{ wenn } (A, <_A) \text{ ein Abschnitt von } (B, <_B) \text{ ist.}$$

Dann erfüllt W die Bedingungen des Zorn'schen Lemmas. Denn, wir sehen sofort: Ist K eine Kette solcher $(A, <_A)$, so ist auch die Vereinigungsmenge aller Glieder dieser Kette ein $(V, <_V)$.

Folglich gibt es ein maximales Element in W, und dieses muss die Elemente von M ausschöpfen, also vom Typ $(M, <_M)$ sein. □

2.2 Kinna's Theorem

Wir betrachten die reelle Achse. Ist hier eine Teilmenge A von mindestens 2 Elementen gegeben, so existiert für jedes offene Intervall (a, b) eine erste rationale Zahl, die in dieses Intervall fällt. Diese Zahl „spaltet" die Menge A in einen nicht leeren Anfang A' und ein nicht leeres Ende A'', formal: erzeugt einen Anfang A' und ein Ende A'' mit $A' \cap A'' = \emptyset$ & $A' \cup A'' = A$. Damit ist eine Funktion ' gefunden, die jeder mindestens 2-elementigen Teilmenge von $\mathbf{R}$ eine nicht leere Teilmenge $A' \subset M$ zugeordnet. Ist hingegen M eine beliebige Menge, so können wir uns nicht auf eine Ordnung beziehen, wohl aber, so sie denn existiert, auf eine Funktion ' der oben betrachteten Art. Dies darf man als Ausgangspunkt des nachfolgenden Beitrags sehen. Genauer: W. Kinna formuliert(e) in seiner Dissertation als Abschwächung des Auswahlpostulats exakt diese Bedingung und zeigt(e), dass das abgeschwächte Auswahlpostulat die Existenz einer spaltbaren Ordnung garantiert, dass also diese beiden Bedingungen äquivalent sind, und dass darüber hinaus diese beiden Bedingungen genau dann erfüllt sind, wenn sich M in die Potenzmenge einer wohlgeordneten Menge einbetten lässt. In der Fundamenta-Publikation wird – leider – nur einer der beiden von Kinna in seiner Dissertation hergeleiteten und an Zermelo orientierten Beweise vorgestellt. Aus seinen Gesprächen mit Klaus Wagner weiß der Autor zusätzlich zu berichten, dass K.Wagner bewiesen hatte, dass das abgeschwächte Auswahlpostulat eine Anordnungsmöglichkeit gewährleistet, dass es dann aber W. Kinna war, der als Doktorand von K. Wagner mittels des von ihm kreierten Begriffes der spaltbaren Ordnung die interessante Untersuchung fortzusetzen und zum Abschluss zu bringen vermochte. Alles entscheidend für die Herleitung der Beweise ist die Einsicht, dass sich aufgrund des schwachen Auswahlpostulats jedes Element als eine wohlgeordnete 0,1-Folge auffassen lässt, so wie dies auch für reelle Zahlen gilt, die sich ja als natürliche 0,1-Folgen auffassen lassen. Beachtet man noch, dass sich unter Annahme der Kontinuumhypothese auch das Potenzmengenkriterium in diesem Sonderfall sehr schön abbildet, so ist man versucht anzunehmen, dass Kinna durch diesen Sachverhalt zu seinem 2. Kriterium angeregt wurde. Wir übernehmen:

Über eine Abschwächung des Auswahlpostulates

von

W. Kinna (Solingen) und **K. Wagner** (Köln)

Es sei M eine Menge. Wir bezeichnen die Elemente von M mit $a, b, ...$, hingegen die Teilmengen von M mit $A, B, ...$ Die Potenzmenge von M (d.h. die Menge sämtlicher Teilmengen von M einschließlich der leeren Menge 0) bezeichnen wir mit M^*.

D e f i n i t i o n. Wir sagen, eine Menge M habe die Eigenschaft (E), wenn es eine eindeutige Abbildung φ von M^* in sich gibt, so dass für jedes aus mindestens 2 Elementen bestehende $A \subseteq M$ gilt:

$$0 \subset \varphi(A) \subset A\,.^{1}$$

Unsere Bedingung (E) steht in einem engen Zusammenhang mit dem bekannten [2] Auswahlpostulat.

Wie man ohne weiteres sieht, ist (E) formal schwächer als das Auswahlpostulat. Man kann aber außerdem leicht zeigen, dass das Kontinuum C noch (E) erfüllt. Denn mittels der unendlichen Folge der rationalen Zahlen gelingt es, da diese relativ zu C dicht liegen, jedes aus mindestens zwei Zahlen bestehende $A \subseteq C$ in ein echtes Anfangsstück und ein echtes Endstück von A zu zerlegen. Versteht man dann unter $\varphi(A)$ dieses echte nicht leere Anfangsstück von A, so folgt unmittelbar unsere Behauptung. Wir sehen unser (E) ist nichts weiter als eine gewisse Abschwächung des Auswahlpostulates.

Satz 1. Jede Menge M mit der Eigenschaft (E) lässt sich ordnen.

B e w e i s. Wir setzen[3] $\overline{\varphi}(A) = A - \varphi(A)$ für jedes $A \subseteq M$. Dann folgt auch

$$0 \subset \overline{\varphi}(A) \subset (A)$$

für jedes aus mindestens zwei Elementen bestehende $A \subseteq M$. Ferner folgt

$$\varphi(A) \cup \overline{\varphi}(A) = A$$

[1] D.h. also, $\varphi(A)$ ist eine echte, nicht leere Teilmenge von A. Die vorliegende Arbeit enthält die wesentlichen Ergebnisse der (unveröffentlichten) Dissertation (Köln 1952) des erstgenannten Verfassers, der durch diese vom letztgenannten Verfasser stammende Definition sowie durch Satz 1 angeregt wurde.

[2] Siehe [7], Abschnitt 2, S. 514.

[3] Es ist im folgenden bequem, für die aus nur einem Element bestehenden A, also (kurz geschrieben) für die $a \in M$ einfach $\varphi(a) = a$ vorauszusetzen. Ferner setzen wir im folgenden für die Nullmenge $\varphi(0) = 0$ voraus.

für jedes $A \subseteq M$. Nach einem Vorbild von E. Zermelo ([8, S. 108]) nennen wir eine Teilmenge $\mathbf{K}$ von M^* eine Kette wenn

($1_{\mathbf{K}}$) $M \in \mathbf{K}$ und
($2_{\mathbf{K}}$) für den Durchschnitt D beliebig (endlich oder unendlich) vieler $A \in \mathbf{K}$ stets auch $\varphi(D) \in \mathbf{K}$ und $\overline{\varphi}(D) \in \mathbf{K}$ gilt.

Es gibt Ketten; z.B. ist das ganze M^* eine Kette. Aus den beiden Ketteneigenschaften folgt leicht, dass der Durchschnitt von Ketten stets wiederum eine Kette ist. Wir betrachten den Durchschnitt sämtlicher Ketten und bezeichnen diesen mit $\mathbf{K}_0$. Dieses ist also die „kleinste" Kette (von M^* bezüglich φ).

Wir werden zeigen, dass sich M mit Hilfe von $\mathbf{K}_0$ ordnen lässt. Hierzu denken wir uns M^* teilweise geordnet, indem wir $A < B$ dann und nur dann setzen, wenn $B \subseteq A$ gilt. Dann ist M das erste Element von M^*. Eine wohlgeordnete Teilmenge $\mathbf{F}$ von M^* (d.h. eine Teilmenge von M^* die als teilweise geordnete Untermenge von M^* aufgefasst, wohlgeordnet ist) heiße ein Filter, wenn

($1_{\mathbf{F}}$) $M \in \mathbf{F}$ und
($2_{\mathbf{F}}$) für jedes $A \neq M$ aus $\mathbf{F}$, unter D den Durchschnitt sämtlicher $B \in \mathbf{D}$ mit $B < A$ verstanden, entweder $\varphi(D) = A$ oder $\overline{\varphi}(D) = A$ gilt.

Wir sagen im folgenden statt Element eines Filters $\mathbf{F}$ auch Glied von $\mathbf{F}$. Z.B. ist, von dem aus dem nur einen Glied M bestehenden (trivialen Filter abgesehen, das zweite Glied jedes Filters entweder gleich $\varphi(M)$ oder $\overline{\varphi}(M)$. Aus den beiden Ketteneigenschaften $1_{\mathbf{K}}$ und $2_{\mathbf{K}}$ folgt mittels einfacher Anwendung transfiniter Induktion, dass jedes Filter in jeder Kette als Teilmenge, also auch in $\mathbf{K}_0$ als Teilmenge enthalten ist. Folglich ist auch die Vereinigungsmenge sämtlicher Filter eine Teilmenge von $\mathbf{K}_0$. Wir werden später aus dem weiteren Verlauf dieses Beweises sehen, dass bereits diese Vereinigungsmenge gleich $\mathbf{K}_0$ ist.

Zunächst folgt unmittelbar:

(I) *Ist* $\mathbf{F}$ *ein Filter, dann ist auch jedes Anfangsstück von* $\mathbf{F}$ *ein Filter.*

Entscheidend ist im weiteren

(II) *Der Durchschnitt je zweier Filter* $\mathbf{F}_1$ *und* $\mathbf{F}_2$ *ist ein gemeinsames Anfangsstück* $\mathbf{F}'$ *von beiden* (*das nach* (I) also wieder ein Filter ist), und ferner gilt, dass der Durchschnitt eines jeden Gliedes von $\mathbf{F}_1 - \mathbf{F}'$ mit jedem

Glied von $\mathbf{F}_2 - \mathbf{F}'$ leer ist. Allgemein gilt: Der Durchschnitt von beliebig vielen Filtern ist gleich einem gemeinsamen Anfangsstück derselben, also nach (I) wiederum ein Filter.

Zum Beweis von (II) sei $\mathbf{F}_1$ eins der vorgegebenen Filter. der Durchschnitt $\mathbf{D}$ der vorgegebenen Filter ist natürlich eine Teilmenge von $\mathbf{F}_1$. Wegen $(1_{\mathbf{F}})$ ist $\mathbf{D}$ nicht leer. Im Falle $\mathbf{D} = \mathbf{F}_1$ ist nichts mehr zu beweisen. im entgegen gesetzten Falle $\mathbf{D} \subset \mathbf{F}_1$ gibt es ein erstes Element $A \in \mathbf{F}_1$, das in $\mathbf{D}$ nicht vorkommt. Nach (I) ist die Menge sämtlicher in $\mathbf{F}_1$ vorkommenden Vorgänger von diesem A ein Filter $\mathbf{F}'$; offenbar ist dieses $\mathbf{F}'$ das größte gemeinsame Anfangsstück von $\mathbf{F}_1$ und $\mathbf{D}$. Da A nicht in $\mathbf{D}$ vorkommt, gibt es unter den vorgegebenen Filtern ein $\mathbf{F}_2$, worin A nicht vorkommt. Nach $(2_{\mathbf{F}})$ ist $\mathbf{F}'$ auch ein Anfangsstück von $\mathbf{F}_2$. Im Falle $\mathbf{F}' = \mathbf{F}_2$ folgt $\mathbf{D} = \mathbf{F}'$. Dann ist unsere Behauptung (II) bewiesen. Im entgegen gesetzten Falle $\mathbf{F}' \subset \mathbf{F}_2$ folgt, unter D' den Durchschnitt sämtlicher Glieder von $\mathbf{F}'$ verstanden, nach $(2_{\mathbf{F}})$ entweder $\varphi(D') = A$ und weiter, da A in $\mathbf{F}_1$ aber nicht in $\mathbf{F}_2$ vorkommt, $\varphi(D') \in \mathbf{F}_1$ und $\overline{\varphi}(D') \in \mathbf{F}_2$ oder nach $(2_{\mathbf{F}})$ folgt $\overline{\varphi}(D') = A$ und wegen $A \in \mathbf{F}_1$ dann $\overline{\varphi}(D') \in \mathbf{F}_1$ und $\varphi(D') \in \mathbf{F}_2$. Da $\varphi(D') \cap \overline{\varphi}(D')$ leer ist und außerdem die Glieder eines jeden Filters, als Teilmengen von M aufgefasst, wegen $(2_{\mathbf{F}})$ monoton abnehmen, folgt hieraus unmittelbar die erste Behauptung von (II). Die letzte Behauptung von (II) ergibt sich daraus, dass der Durchschnitt von Anfangsstücken von $\mathbf{F}_1$ stets wiederum ein Anfangsstück von $\mathbf{F}_1$ ist.

Schließlich gilt noch

(III) Zu jedem Element $a \in M$ gibt es genau ein Filter $\mathbf{F}$ derart, dass der Durchschnitt sämtlicher Glieder von $\mathbf{F}$ aus diesem einen Element a besteht.

Denn es sei $\mathbf{V}$ die Vereinigungsmenge sämtlicher Filter, in denen a in jedem Glied vorkommt. Aus (II) folgt leicht, dass $\mathbf{V}$ die Bedingung $(2_{\mathbf{F}})$ erfüllt. Da $(1_{\mathbf{F}})$ selbstverständlich für $\mathbf{V}$ gilt, ist $\mathbf{V}$ ein Filter. Nach Definition von $\mathbf{V}$ kommt a in jedem Glied von $\mathbf{V}$ vor. Bestünde der Durchschnitt D sämtlicher Glieder von $\mathbf{V}$ aus mindestens zwei Elementen, so läge unser a entweder in $\varphi(D)$ oder in $\overline{\varphi}(D)$. Eine dieser beiden Mengen käme dann aber in $\mathbf{V}$ vor im Widerspruch zur Bedeutung von D. Schließlich sei $\mathbf{V}'$ ein Filter, das ebenfalls noch die in (III) genannte Bedingung erfülle. Dann stimmen $\mathbf{V}$ und $\mathbf{V}'$ nach $(1_{\mathbf{F}})$ mindestens in ihrem ersten Element überein. Nun sei allgemein $\mathbf{V}''$ ein gemeinsames echtes Anfangsstück von $\mathbf{V}$ und $\mathbf{V}'$. Es sei

D'' der Durchschnitt sämtlicher Glieder von $\mathbf{V}''$. Nach $(2_{\mathbf{F}})$ folgt in dem wohlgeordneten $\mathbf{V}$ bzw. $\mathbf{V}'$ entweder $\varphi(D'')$ oder $\overline{\varphi}(D)$ unmittelbar hinter den Gliedern von $\mathbf{V}''$. Da jedes Glied von $\mathbf{V}$ und $\mathbf{V}'$ aber a als Element enthält und $\varphi(D'') \cap \overline{\varphi}(D'')$ leer ist folgt entweder für $\varphi(D'')$ oder aber für $\overline{\varphi}(D'')$, das dasselbe in $\mathbf{V}$ und in $\mathbf{V}'$ gleichzeitig vorkommt. Also folgt mittels transfiniter Induktion $\mathbf{V}' = \mathbf{V}$.

Wir bezeichnen dieses $\mathbf{V}$ im folgenden mit $\mathbf{V}(a)$. Ein Filter $\mathbf{F}$ heiße *vollständig*, wenn es entweder mit der leeren Menge 0 oder mit einem Element von M als letztes Glied von $\mathbf{F}$ schließt. Unsere $\mathbf{V}(a)$ sind vollständig, weil nach (III) und wegen $\varphi(a) = a$ jedes $\mathbf{V}(a)$ mit seinem a als letztes Glied schließt.[4]

Es folgt nun leicht der vollständige Beweis von Satz 1. Man habe zwei verschiedene Elemente $a, b \in M$. Wir betrachten nach (III) die beiden Filter $\mathbf{V}(a)$ und $\mathbf{V}(b)$. Wegen $a \neq b$ folgt aus (III) zunächst $\mathbf{V}(a) \neq \mathbf{V}(b)$. Gemäß (II) betrachten wir das gemeinsame Anfangsstück $\mathbf{F}$ von $\mathbf{V}(a)$ und $\mathbf{V}(b)$. Es sei D der Durchschnitt sämtlicher Glieder von $\mathbf{F}$. In D liegen dann also a und b noch beide. Aber $\varphi(D)$ und $\overline{\varphi}(D)$ enthalten je genau eins unserer beiden Elemente a, b. Anschaulich gesprochen, werden a und b in $\mathbf{V}(a)$ und $\mathbf{V}(b)$ durch $\varphi(D)$ und $\overline{\varphi}(D)$ zum ersten Male (und von da ab natürlich dauernd) getrennt! Wir setzen nun $a < b$, wenn $a \in \varphi(D)$ und damit also $b \in \overline{\varphi}(D)$ gilt. Es bleibt nun allein nur noch zu zeigen übrig, dass diese Relation „<" in M transitiv ist. Hierzu habe man drei Elemente $a_1, a_2, a_3 \in M$ mit $a_1 < a_2$ und $a_2 < a_3$. Wir bezeichnen $\mathbf{V}(a_\nu)$ kurz durch $\mathbf{V}_\nu$, $(\nu = 1, 2, 3)$. Ferner sei entsprechend (II) das gemeinsame Anfangsstück von $\mathbf{V}_\nu, \mathbf{V}_\mu$ mit $\mathbf{F}_{\nu\mu}$ bezeichnet $(\nu, \nu = 1, 2, 3)$. Unter $D_{\nu\mu}$ sei der Durchschnitt sämtlicher Glieder von $\mathbf{F}_{\nu\mu}$ verstanden.

Zunächst ergibt sich $\mathbf{F}_{12} \neq \mathbf{F}_{2,3}$, da wegen $a_1 < a_2$ nach unserer „<"-Relation $a_2 \in \varphi(D_{12})$ folgt und natürlich $a_2 < a_3$ analog $a_2 \in \varphi(D_{23})$ zur Folge hat, also $D_{12} \neq D_{23}$ und daher auch $\mathbf{F}_{12} \neq \mathbf{F}_{23}$ folgt. Da $\mathbf{F}_{12}$ und $\mathbf{F}_{23}$ Anfangsstücke desselben $\mathbf{V}_1$ sind, bleibt nur allein noch $\mathbf{F}_{12} \subset \mathbf{F}_{23}$ oder $\mathbf{F}_{23} \subset \mathbf{F}_{12}$ übrig.

Es sei $\mathbf{F}_{12} \subset \mathbf{F}_{23}$. Dann folgt aus (II) unmittelbar

$$\mathbf{F}_{13} = \mathbf{F}_{12}$$

[4]Es können aber auch noch vollständige Filter existieren, die unter unseren $\mathbf{V}(a)$ und $\mathbf{V}(a) \cup 0$ nicht vorkommen. Z. B. betrachte man ein aus den offenen Intervallen $(0, 1/n), n = 1, 2, ...$, und 0 (leere Menge) zusammengesetztes Filter

also $D_{13} = D_{12}$. Dann ist $a_1 \in \varphi(D_{13})$, wegen $a_1 < a_2$. Wegen $D_{13} = D_{12}$ folgt $a_1 \in \varphi(D_{13})$, also auch $a_1 < a_3$.

Umgekehrt sei $\mathbf{F}_{23} \subseteq \mathbf{F}_{13}$. Dann folgt durch Vertauschung der Indizes 1 und 3 analog $D_{13} = D_{32}$ und wegen $a_2 < a_3$ weiter ...

Aus unserem Beweis ergibt sich noch leicht, dass die Kette $\mathbf{K}_0$ nichts anderes ist als die Vereinigungsmenge sämtlicher Filter $\mathbf{V}(a)$ unter Hinzunahme noch des einen Elementes 0 ist. Denn diese Menge erfüllt offenbar die erste der beiden Kettenbedingungen $(1_{\mathbf{K}})$. Sie erfüllt auch die zweite Bedingung $(2_{\mathbf{K}})$. Denn der Durchschnitt beliebig vieler Glieder unserer $\mathbf{V}(a)$ (zu beliebigen $a \in M$, also nicht notwendig alle zu demselben a gehörig) ist stets entweder leer oder nach (II) liegen diese vorgegebenen Glieder sämtlich in demselben $\mathbf{V}(a)$. Hieraus folgt ohne weiteres wegen $(2_{\mathbf{F}})$ und wegen des monotonen Fallens der Glieder eines jeden Filters, dass die Vereinigungsmenge sämtlicher Filter auch $(2_{\mathbf{K}})$ erfüllt. Also ist diese Menge eine Kette. Diese ist, wie wir früher sahen, eine Teilmenge von $\mathbf{K}_0$. Unser $\mathbf{K}_0$ ist aber die kleinste Kette, also fallen beide zusammen.

Wir wollen im weiteren den Satz 1 noch etwas verschärfen. Hierzu nennen wir eine geordnete Menge *spaltbar geordnet,* wenn es eine eindeutige Abbildung ψ von M^* in sich derart gibt, dass für jedes aus mindestens zwei Elementen bestehende $A \subseteq M$ die Bildmenge $\psi(A)$ ein echtes, nicht leeres Anfangsstück von A ist.

Dann gilt:

Satz 2. *Eine Menge M besitzt dann und nur dann die Eigenschaft* (E)*, wenn es eine spaltbare Ordnung von M gibt.*

Denn ist M spaltbar geordnet, so hat M trivialerweise die Eigenschaft (E). Wir setzen nun umgekehrt voraus, M besitze die Eigenschaft (E). Wir denken uns M mittels unserer $\mathbf{V}(a)$ gemäß Beweis von Satz 1 geordnet. Dann sei A eine aus mindestens zwei Elementen bestehende Teilmenge von M. Nach (II) ist der Durchschnitt sämtlicher $\mathbf{V}(a)(a \in A)$, ein gemeinsames Anfangsstück $\mathbf{F}$ dieser $\mathbf{V}(a)$. Es sei D der Durchschnitt sämtlicher Glieder von $\mathbf{F}$. Dann folgt $A \subseteq D$. Ferner folgt $\varphi(D) \cup \overline{\varphi}(D) = D$. In jeder der beiden Menge $\varphi(D)$ und $\overline{\varphi}(D)$ liegt dann mindestens ein Element von A. Denn enthielte $\varphi(D)$ oder $\overline{\varphi}(D)$ das ganze A als Teilmenge, so käme ja auch noch dieses $\varphi(D)$ bzw. $\overline{\varphi}(D)$ in unserem $\mathbf{F}$ als ein Glied vor im Widerspruch zur Bedeutung von D. Ferner geht in dem von uns gemäß Satz 1 geordneten

M jedes Element von $\varphi(D)$ jedem Element von $\overline{\varphi}(D)$ voraus. Diese folgt natürlich dann auch für die Elemente der Durchschnitte $\varphi(D) \cap A$ und $\overline{\varphi}(D) \cap A$. Aus $\varphi(D) \cup \overline{\varphi}(D) = D$ folgt weiter $(\varphi(D) \cap A) \cup (\overline{\varphi}(D) \cap A) = A$. Da jeder der beiden Summanden dieser Zerlegung von A nicht leer ist, ergibt die Abbildung $\psi(A) = \varphi(D) \cap A$ die gesuchte spaltbare Ordnung von M, w.z.b.w.

An dieser Stelle ist ein Rückblick auf das Auswahlpostulat und unsere Bedingung (E) besonders interessant. Ist speziell jedem $A \subseteq M$ je ein aus nur einem Element $\varphi(A)$, d.h. also ein Element von A zugeordnet, so besteht natürlich auch unser voriges $\psi(A) = \varphi(D) \cap A$ nur aus einem Element. Dieses ist dann das erste Element von A. Unser Beweis von Satz 1 ergibt also, wenn φ jedem nicht leeren $A \subseteq M$ eine aus nur einem Element bestehende Teilmenge von A zuordnet, ist die im Beweis von Satz 1 definierte Ordnung eine Wohlordnung. Der Satz 1 und sein Beweis enthalten also als Spezialfall den Wohlordnungssatz.

Wir wollen im folgenden weiter zeigen, dass die Potenzmenge jeder wohlgeordneten Menge die Eigenschaft (E) besitzt und dass auch umgekehrt, sich jede Menge mit der Eigenschaft (E) in die Potenzmenge einer wohlgeordneten Menge einbetten lässt. Ungenau gesagt, führen also die Mengen mit unserer Eigenschaft (E) nicht über die Potenzmenge wohlgeordneter Mengen hinaus.

Genauer gesagt, gilt:

Satz 3. *Eine Menge M besitzt dann und nur dann die Eigenschaft* (E), *wenn es eine wohlgeordnete Menge N und hierzu eine [zu M] äquivalente Teilmenge der Potenzmenge N^* von N gibt.*

Beweis. Wir setzen zunächst voraus, M habe die Eigenschaft (E). Wir betrachten die Menge sämtlicher Filter von M (bezüglich des vorgegebenen φ). Mit Hilfe dieser Menge konstruiere man die folgende wohlgeordnete Menge N. Es seien $\mathbf{F}_1$ und $\mathbf{F}_2$ zwei Filter. Man setze $\mathbf{F}_1 < \mathbf{F}_2$, wenn es ein echtes mit $\mathbf{F}_1$ ähnliches (d.h. auf $\mathbf{F}_1$ ähnlich abbildbares) Anfangsstück von $\mathbf{F}_2$ gibt. Dagegen setze man $\mathbf{F}_2 < \mathbf{F}_1$, wenn es ein echtes mit $\mathbf{F}_2$ ähnliches Anfangsstück von $\mathbf{F}_1$ gibt. Dann denke man sich die Menge sämtlicher Filter in die (elementfremdem) Teilmengen je untereinander ähnlicher Filter zerlegt und fasse diese Teilmengen als die Elemente einer Menge N auf. Durch Übertragung unserer vorigen Relation „$<$" für die Filter auf die Elemente von N folgt leicht, dass N wohlgeordnet ist. ferner folgt, da je zwei verschiedene Anfangsstücke desselben Filters niemals miteinander ähnlich sind, dass jedes

Filter mit genau einem Anfangsstück von N ähnlich ist. Nunmehr ordnen wir jedem Element $a \in M$ jeweils die folgende Menge N_a zu: ein Element $a \in M$ werde in die Menge N_a aufgenommen, wenn bei der ähnlichen Abbildung von $\mathbf{V}(a)$ auf das ähnliche Anfangsstück von N das a in diesem Anfangsstück vorkommt und für sein Urbild A in $\mathbf{V}(a)$ entweder $A = M$ oder die erste der beiden Gleichungen von $2_{\mathbf{F}}$, also $\varphi(D) = A$ gilt. Kommt dagegen a in dem Anfangsstück von N nicht vor oder kommt es vor und gilt für sein Urbild A in $\mathbf{V}(a)$ die letzte Gleichung in $2_{\mathbf{F}}$ $\overline{\varphi}(D) = A$, so werde das betreffende a nicht in N_a aufgenommen. Unsere Abbildung $a \to N_a$ ist eineindeutig, da für je zwei verschiedene Elemente $a, b \in M$ nach (II) und (III) $N_a \neq N_b$ folgt. Also gibt es eine mit M äquivalente Teilmenge von N^*.

Wir setzen nun umgekehrt voraus, es existiere eine wohlgeordnete Menge N, deren Potenzmenge N^* mit M äquivalent sei. Wir dürfen hier sogleich die Äquivalenz von M mit dem ganzen N^* voraussetzen, da die Eigenschaft (E), wenn sie für eine Menge zutrifft, dann ja auch für jede Teilmenge dieser Menge zutrifft.

Man habe nunmehr ein aus mindestens zwei Elementen bestehendes $A \subseteq M$. Das Bild von $a \in A$ vermöge der Äquivalenz $M \sim N^*$ bezeichne man mit N_a. Wir betrachten die Vereinigungsmenge sämtlicher $N_a (a \in A)$ und bezeichnen sie mit N_A. Da A aus mindestens zwei Elementen besteht, ist N_A nicht leer. Es existiert somit eine erstes Element von A, dieses bezeichnen wir mit a. Kommt a in mindestens einem der $N_a (a \in A)$ nicht vor, so sei $\varphi(A)$ die Menge derjenigen $a \in A$, in deren N_a unser a vorkommt.

Kommt dagegen a in jedem $N_a\,(a \in A)$ vor, so betrachten wir den Durchschnitt Δ sämtlicher $N_a\,(a \in A)$. Wegen $a \in \Delta$ ist ist Δ nicht leer. Da A aus mindestens zwei Elementen besteht, ist auch $N_A - \Delta$ nicht leer. Es existiert somit ein erstes Element β von $N_A - \Delta$. Dieses β kommt dann also in mindestens einem N_a, aber nicht in allen N_a gleichzeitig vor. Dann verstehe man unter $\varphi(A)$ die Menge derjenigen $a \in A$, in deren N_a das β vorkommt. In jedem Falle hat sich eine echte, nicht leere Teilmenge $\varphi(A)$ von A ergeben, womit Satz 3 bewiesen ist.

Wir schließen mit einem allgemeinem B e i s p i e l für Mengen, die stets die Eigenschaft (E) besitzen.

Hierzu sei M eine geordnete Menge. *Gibt es (mindestens) eine relativ zu M dichte Teilmenge $N \subseteq M$, die sich außerdem wohlordnen lässt,* so wollen

wir zeigen, dass dann M die Eigenschaft (E) hat.

Denn ist $A \subseteq M$ vorgegeben und besteht A aus mindestens zwei Elementen, so gibt es Elemente $n \in N$, die zwischen mindestens zwei Elementen von A liegen. Folglich gibt es in N auch ein erstes Element n_A dieser Art. Dann verstehe man unter $\varphi(A)$ die Menge sämtlicher $a \in A$ mit $a < n_A$. Offenbar ist $\varphi(A)$ ein echtes nicht leeres Anfangsstück von A.

Dieses Beispiel zeigt uns nochmals als Spezialfall, dass das Kontinuum die Eigenschaft (E) besitzt.

In Untersuchungen von A. Fraenkel (([15] und [16]), A. Mostowski ([31] und [32]) und A. Lindenbaum mit A. Mostowski in [26] wurde u. a. gezeigt, dass das Ordnungstheorem von den üblichen Axiomen der Mengenlehre [5] (das Auswahlaxiom aber nicht mit dazu genommen) unabhängig ist. Da nach Satz 1 das Ordnungstheorem aus (E) folgt, ist auch (E) unabhängig von den Axiomen der Mengenlehre. Ob aber unser (E) auch unabhängig vom Ordnungstheorem bzw. ob das Auswahlpostulat unabhängig von (E) ist, ist uns nicht bekannt. [6]

[5] Vgl. [16], [39] und [40].

[6] A. Fraenkel und A. Tarski schlugen uns vor, die Unabhängigkeit des Auswahlaxioms von unserem (E) mittels der in der Arbeit von Mostowski [31] entwickelten Methoden nachzuweisen.

Kapitel 3

Zum AOG

3.1 Dichte Ketten

Zur Wiederholung:

3. 1. 1 Definition. $(P, <) =: \mathfrak{P}$ heißt eine *total geordnete Menge*, synonym auch eine *linear geordnete Menge* bzw. *Kette*, wenn für alle $a, b, c \in P$ gilt:

(i) $a \not< a$,
(ii) $a < b \;\&\; b < c \Longrightarrow a < c$,
(iii) $a \neq b \Longrightarrow a < b$ aut $b < a$.

Wie üblich setzen wir in Ketten $a \leq b :\Longleftrightarrow a = b \vee a < b$. Offenbar ist $\leq$ eine Partialordnung.

3. 1. 2 Definition. Sei $\mathfrak{T}$ eine Kette. Dann sagen wir, *z liege zwischen a und b*, wenn $a < z < b$ erfüllt ist. Sei weiter $S \subseteq T$. Dann nennen wir *S dicht in $\mathfrak{T}$*, wenn zwischen je zwei verschiedenen Elementen aus T mindestens ein Element aus S liegt. Insbesondere nennen wir $\mathfrak{T}$ *dicht* (*in sich selbst*), wenn T dicht liegt in $\mathfrak{T}$.

Als Beispiele seien genannt $\mathbf{R}$ und etwa $\mathbf{Q}$ in $\mathbf{R}$.

3. 1. 3 Definition. Sei $\mathfrak{K}$ eine Kette und $A \subseteq K$. Dann heißt m *Maximum* der Menge A, wenn m in A liegt und alle $a \in A$ der Beziehung $a \leq m$ genügen. Dual erklären wir den Begriff *Minimum*.

Die Begriffe *obere, untere Schranke* wurden schon erklärt, ebenso die Begriffe *Supremum* und *Infimum* sowie die Begriffe *nach oben, nach unten begrenzt.*

3. 1. 4 Definition. Sei $\mathfrak{K}$ eine Kette. Dann nennen wir $\mathfrak{K}$ *stetig*, wenn $\mathfrak{K}$ dicht ist und jede nach oben beschränkte Teilmenge $A \subseteq K$ *nach oben begrenzt ist.*

Wie man unmittelbar erkennt, ist die Menge der unteren Schranken zu A, falls sie nicht leer ist, nach oben beschränkt, so dass in einem stetigen $\mathfrak{K}$ auch jede nach unten beschränkte Teilmenge nach unten begrenzt ist, nämlich durch die obere Grenze der unteren Schranken.

Als nächstes erklären wir – erwartungsgemäß:

3. 1. 5 Definition. Seien $\mathfrak{A} := (A, <_A)$ und $\mathfrak{B} := (B, <_B)$ zwei Ketten. Dann heißen $\mathfrak{A}$ und $\mathfrak{B}$ *ordnungsisomorph*, auch *ähnlich*, wenn sich zwischen A und B eine Bijektion ϕ derart stiften lässt, dass

$$x <_A y \implies \phi(x) <_B \phi(y)$$

erfüllt ist.

Hiernach wenden wir uns als erstes den abzählbaren, dichten Ketten zu.

3. 1. 6 Definition. Sei K eine Kette. Dann versteht man unter dem *offenen* Intervall (a, b) die Menge $\{\, x \mid a < x < b \,\}$, unter dem *abgeschlossenen* Intervall $[\, a, b \,]$ die Menge $\{\, x \mid a \leq x \leq b \,\}$ unter dem *linksoffenen, rechtsabgeschlossenen* Intervall $(a, b\,]$ die Menge $\{\, x \mid a < x \leq b \,\}$, etc.

Weiter heiße eine Kette *rechts-* bzw. *links-berandet*, wenn sie einen rechten bzw. linken *Endpunkt* hat, und demzufolge *berandet*, wenn sie rechts- und links-berandet ist.

Zu den abzählbaren dichten Ketten gehören natürlich die rationalen Intervalle $[\, 0, 1 \,]$, $(0, 1\,]$, $[\, 0, 1)$, $(0, 1)$. Denn, wie man leicht sieht, liefert die oben für $\mathbf{Q}$ konstruierte Auswahlfunktion ein Abzählverfahren.

Tatsächlich gilt aber mehr, nämlich

3. 1. 7 Proposition. *Ist $\mathfrak{K}$ eine abzählbare dichte Kette, so ist $\mathfrak{K}$ ordnungsisomorph zu einem der vier soeben vorgestellten Intervalle.*

BEWEIS. Offenbar sind wir am Ziel, sobald wir gezeigt haben, dass jede *unberandete* abzählbare dichte Kette ordnungsisomorph ist zu der geordneten Menge der rationalen Zahlen $\mathfrak{Q} := (Q, \leq)$. Sei also $\mathfrak{K}$ unberandet, abzählbar und dicht.

Dann können wir K und auch Q annehmen in abgezählter Form, also etwa:

$$\begin{aligned} K &= \{\, a_1, a_2, a_3, \ldots, a_n, \ldots \} \\ Q &= \{\, b_1,\, b_2,\, b_3,\, \ldots, b_n,\, \ldots \}\,. \end{aligned}$$

Wir bilden nun ab:

a_1 auf b_1, b_2 auf das Element von kleinstem Index unter den Elementen aus K in ähnlicher Lage zu a_1 wie b_2 zu b_1, hiernach das noch nicht berücksichtigte Element aus K von kleinstem Index auf dasjenige Element aus Q in ähnlicher Lage von kleinstem Index usw.

Dieses Verfahren lässt sich Schritt für Schritt durchführen, da $\mathfrak{K}$ als dicht und unberandet angenommen wurde, und es kommt zu einer Bijektion, da jedes Element aus Q und auch jedes Element aus K berücksichtigt wird. □

Vor dem nächsten Satz geben wir als eine weitere Erklärung:

3. 1. 8 Definition. Sei $\mathfrak{K}$ eine Kette. Dann heiße das Teilmengenpaar A, B ein *Schnitt* von $\mathfrak{K}$, wenn gilt

(i) $A \cup B = K$

(ii) $A \cap B = \emptyset$

(iii) $a < b$ für alle $a \in A, b \in B$

Genauer nennen wir einen Schnitt einen *Sprung*, wenn es sowohl A ein letztes als auch B ein erstes Element gibt, und eine *Lücke*, wenn weder A ein letztes noch B ein erstes Element besitzt.

Als zusätzliche Vereinbarung bezeichnen wir den Schnitt $(K|\emptyset)$ als Rechtsschnitt und den Schnitt $(\emptyset|K)$ als Linksschnitt.

Beispielsweise bestimmt π einen Sprung in $\mathfrak{Z}$ und eine Lücke in $\mathfrak{Q}$. Wie üblich notieren wir Schnitte im weiteren mit $A \,|\, B$.

Nach der letzten Definition ist klar, dass jede *irrationale* Zahl in der Menge der rationalen Zahlen in eindeutiger Weise einen Schnitt bestimmt, auch bezeichnet als *Schnittzahl.* Und natürlich bestimmt auch jede rationale Zahl einen Schnitt in der Menge der irrationalen Zahlen.

Als eine unmittelbare Folgerung aus 3.1.7 erhalten wir

3. 1. 9 Proposition. *Sei $\mathfrak{K}$ eine stetige unberandete Kette und liege eine abzählbare Teilmenge A dicht in $\mathfrak{K}$. Dann ist $\mathfrak{K}$ ordnungsisomorph zu $\mathfrak{R} := (\mathbf{R}, \leq)$.*

DENN: man stifte eine *Ähnlichkeitsabbildung* zwischen $\mathfrak{Q}$ und $\mathfrak{A}$. Gilt dann $\alpha \notin A$, so bestimmt α einen Schnitt in $(A, \leq)$ und damit eine eindeutig bestimmte Schnittzahl in Q. □

Fragen.

(a) Nach dem soeben bewiesenen Satzes ist das Intervall $((0,1), \leq)$ ordnungsisomorph zu $\mathfrak{R}$.

Welche elementare (Mittelstufen-) Vorschrift leistet dies ebenfalls in diesem Sonderfall?

(b) Nach dem soeben bewiesenen Satz ist $\mathfrak{R}^+$ ordnungsisomorph zu $\mathfrak{R}$.

Welche klassische Funktion leistet dies – und noch sehr viel mehr darüber hinaus.

Wir schließen mit einem Verfahren, das ebenso elementar wie fundamental ist. Sei $\mathfrak{L}$ eine linear geordnete Menge und sei $A|B$ ein Schnitt. Dann ist dieser Schnitt verschieden von allen Elementen aus L. Nehmen wir $A|B$ zu L hinzu, so lässt sich $L \cup \{A|B\}$ in natürlicher Weise ordnen, indem man $a < A|B$ genau denn setzt, wenn $a \in A$ erfüllt ist und $(A|B < b$ genau dann, wenn $b \in B$ erfüllt ist.

Analog verfahren wir mit je zwei Schnitten $(A|B), (C|D)$. Hier bietet sich in natürlicher Weise die Festsetzung $A|B < C|D :\Longleftrightarrow A \subset C$ an. Dies zu überprüfen bleibe dem Leser überlasen.

Somit gelangen wir von einer Kette $\mathfrak{K}$ in natürlichster Weise zu einer Kette $\mathfrak{K}_1$ durch *Schnittauffüllung.*

Dieses Verfahren lässt sich dann entlang jeder vorgegebenen Ordinalzahlreihe fortsetzen. Denn ist allen Ordinalzahlen echt unterhalb von η bereits eine Schnittauffüllung zugeordnet, so bilde man die Vereingungsmenge alle beteiligten Elemente bzw. Schnitte. Diese ist geordnet, wie man leicht sieht – und also eine Schnittauffüllung $\mathfrak{K}_\eta$ zugänglich.

Wir wollen uns hier auf die Reihe der natürlichen (Ordinal-) Zahlen beschränken. Hier ist das induktive Vorgehen durchschaubarer, weil jede natürliche Zahl nach endlich vielen Schritten berücksichtigt wird.

3. 1. 10 Proposition. *Die geordnete Menge der natürlichen Zahlen entsteht aus der geordneten leeren Menge durch sukzessive Rechts-Schnittergänzung.*

Die geordnete Menge der ganzen Zahlen entsteht aus der geordneten leeren Menge durch alternative Rechts/Links-Schnittergänzung.

Die geordnete Menge der rationalen Zahlen entsteht aus der leeren Menge durch abzählbar wiederholte sukzessive Schnittauffüllung.

Die geordnete Menge der reellen Zahlen entsteht aus der Menge der rationalen Zahlen durch Dedekind'sche Schnittauffüllung, d. h. Lückenschließung.

3.2 Das AOG

Vor dem nun folgenden Satz erinnern wir daran, dass ein Punkt P in $\mathbf{R}$ ein *Häufungspunkt* zur Menge A heißt, wenn in jeder Umgebung von P, also in jedem offenen Intervall, das P enthält, mindestens noch ein weiterer Punkt von A liegt. Dies sei auch die Definition eines Häufungspunktes in unserem Fall. Ebenso wollen wir „großzügig" die Elemente aus K, wie im Sonderfall $\mathfrak{R}$, als Punkte von $\mathfrak{K}$ bezeichnen.

Weiter erinnern wir:

3. 2. 1 Definition. Sei $\mathfrak{K}$ eine Kette und (a_n) eine Folge von Elementen aus K. Dann sagt man (a_n) konvergiere gegen a, in Zeichen

$$(a_n) \to a\,, \qquad \text{auch} \qquad lim\ a_n = a\,,$$

wenn (a_n) in jedem offenen Intervall $I \ni a$ *endet*, soll heißen: mit einem ganzen Ende a_N, a_{N+1}, a_{N+2} ..... in I liegt.

3. 2. 2 Definition. Seien $\mathfrak{K}_1, \mathfrak{K}_2$ zwei Ketten und f eine Funktion $K_1 \longrightarrow K_2$. Dann heißt f stetig an der Stelle $x_o \in K_1$, wenn gilt:

$$x_n \to x_o \Longrightarrow f(x_n) \to f(x_o)\,,$$

bzw. wenn gilt: Zu jedem offenen Intervall $K_2 \supseteq U_2 \ni f(x_0)$ existiert ein offenes Intervall $K_1 \supseteq U_1 \ni x_0$ mit $f(U_1) \subseteq U_2$.

3. 2. 3 Theorem. *Sei $\mathfrak{K}$ eine dichte Kette. Dann sind paarweise äquivalent:*

(AO) Das Axiom von der oberen Grenze: *Jede nichtleere nach oben beschränkte Teilmenge von K ist in $\mathfrak{K}$ nach oben begrenzt.*

(HB) Der Satz von Heine-Borel: *Jede $[\,a,b\,]$ überdeckende Familie offener Intervalle (a_i,b_i) $(i\in I)$ enthält eine endliche Teilfamilie $(a_{i_1},b_{i_1}),\ldots,(a_{i_n},b_{i_n})$, die $[\,a,b\,]$ überdeckt.*

(CD) Der Satz von Cantor: *Jede durchschnittsleere Familie abgeschlossener Intervalle $[\,a_i,b_i\,]$ $(a_i\neq b_i\,,\ i\in I)$ enthält mindestens zwei durchschnittsleere Intervalle.*

(SM) Der Satz vom Maximum: *Jede über $[\,a,b\,]$ stetige Funktion f besitzt einen Wertebereich mit Maximum.*

(ZS) Der Zwischenwertsatz: *Jede über $[\,a,b\,]$ stetige Funktion nimmt über $[\,a,b\,]$ jeden Wert zwischen $f(a)$ und $f(b)$ an.*

(AS) Der Abbildungssatz: *Stetige Funktionen überführen abgeschlossene Intervalle in abgeschlossene Intervalle.*

BEWEIS.

(AO) $\Longleftrightarrow$ **(HB)**:

(a) Gelte **(AO)**. Wir bilden

$$X:=\{\,x\,|\,[\,a,x\,]\text{ wird (schon) endlich überdeckt}\,\}\,.$$

Dann gibt es mindestens ein x echt zwischen a und b, das (noch) zu X gehört, man wähle ein $(a_k,b_k)\ni a$, und es gilt $\Omega(X):=\Omega\leq b$. Wählen wir nun ein Intervall $(a_\ell,b_\ell)\ni\Omega$, so liegt in diesem (a_ℓ,b_ℓ) links von Ω mindestens noch ein $x\in X$. Folglich muss Ω gleich b sein, da sonst auch rechts von Ω noch ein $x\in X$ läge.

Somit überdecken schon endlich viele der (a_i,b_i) das abgeschlossene Intervall $[\,a,b\,]$.

(b) Gelte nun **(HB)**. Enthielte $\mathfrak{K}$ dann eine Lücke $A|B$, so könnten wir Elemente $a'<a\in A$ und $b'>b\in B$ wählen, derart, dass die Menge aller (a',a_i) mit $a_i\in A\cap[\,a,b\,]$ und aller (b_i,b') mit $b_i\in[\,a,b\,]\cap B$ eine offene Überdeckung von $[\,a,b\,]$ lieferte, die ihrerseits aber keine endliche Teilüberdeckung von $[\,a,b\,]$ enthielte, mit Widerspruch zu **(HB)**.

Also hat $\mathfrak{K}$ keine Lücke, so dass nach oben beschränkte Teilmengen stets nach oben begrenzt sind.

(AO) $\Longleftrightarrow$ **(CD)**:

(a) Gelte **(AO)**. Gäbe es dann kein

$$[\,a_i, b_i\,] \cap [\,a_j, b_j\,] \;=\; \emptyset\,,$$

so läge jedes a_i vor jedem b_j. Das bedeutete aber

$$sup\{\,a_i\,\} \;\leq\; \inf\{\,b_i\,\}\;\; (i \in I)$$

und damit einen Widerspruch zur Annahme, da $sup\{\,a_i\,\}$ dann im Durchschnitt aller betrachteten Intervalle läge.

(b) Gelte hiernach **(CD)**. Wäre dann A nach oben beschränkt, nicht aber nach oben begrenzt, so bildete die Menge aller $[\,a_i, b_i\,]$ mit „$a_i \in A$ und b_i ist obere Schranke" eine Familie von Intervallen mit leerem Durchschnitt. Folglich gäbe es auch zwei durchschnittsleere unter diesen Intervallen mit Widerspruch zur Konstruktion.

(AO) $\Longleftrightarrow$ **(SM)**:

(a) Gelte **(AO)**. Ist dann $f(a)$ oder $f(b)$ Maximum des Wertebereichs $W := f[\,a, b\,]$, so ist nichts zu zeigen.

Sonst aber betrachten wir die Menge X aller $x \in [\,a, b\,]$ mit der Eigenschaft, dass $[\,a, x\,]$ beschränkt ist. Sie ist nicht leer, wegen $a \in X$ und nach oben beschränkt, etwa durch b, also auch begrenzt, sprich durch $\Omega \leq b$. Da f stetig ist, folgt dann unmittelbar $\Omega = b$ und damit, dass f über $[\,a, b\,]$ beschränkt ist, also $W := f([\,a, b\,])$ nach oben begrenzt ist, sprich durch G.

Sei hiernach U die Menge aller $u \in [\,a, b\,]$ mit $\mathrm{Sup\,f}([\,\mathrm{a, u}\,]) < \mathrm{Sup\,f}([\,\mathrm{a, b}\,])$ und S die obere Grenze von U. Dann muss $S < b$ sein, da man sonst ein offenes Intervall $I \subseteq [\,a, b\,]$ um S wählen könnte, über dem die Funktionswerte von f noch alle unterhalb eines $g < G$ lägen, mit Widerspruch.

Und es muss $f(S) = G$ erfüllt sein, da $f(S) < G$ aus analogen Gründen zu dem Widerspruch führen würde, dass S nicht obere Grenze von U wäre.

Also nimmt f das Supremum des Wertebereichs an.

(b) Gelte hiernach **(SM)**. Gäbe es eine *Lücke* $A|B$, so könnten wir ein stetiges f definieren vermöge

$$f(x) := \begin{cases} x & \text{falls } x \in A \\ a & \text{sonst} \end{cases}$$

mit einem festen $a \in A$. Da f kein Maximum annimmt, wäre dann aber **(SM)** nicht erfüllt.

(**AO**) $\Longleftrightarrow$ (**ZS**):

(a) Sei $f(a) < z < f(b)$. Wir bilden $X := \{\, x \mid f([\, a, x\,]) < z \,\}$ und betrachten das Supremum $\Omega(X) =: \Omega$. Dann gilt $f(\Omega) = z$, da *per constructionem* aufgrund der Stetigkeit sowohl $f(\Omega) < z$ als auch $f(\Omega) > z$ zum Widerspruch führen.

(b) Gäbe es eine *Lücke* $A|B$, so könnten wir ein stetiges f definieren vermöge

$$f(x) := \begin{cases} a & \text{falls } x \in A \\ b & \text{sonst} \end{cases}$$

mit festem $a \in A$ und $b \in B$, das **(ZS)** offenbar nicht erfüllt. □

Ist $\mathfrak{K}$ eine Kette mit abzählbarer dichter Teilmenge C, so dürfen wir (natürlich) etwas mehr erwarten. Als Satz sei hier formuliert:

3. 2. 4 Proposition. *Enthält $\mathfrak{K}$ sogar eine abzählbare in K dichte Teilmenge C, so sind zusätzlich äquivalent zu* **(AO)***:*

(MA) Die Monotonieaussage: *Jede nach oben beschränkte streng monoton steigende Folge (a_n) ist konvergent.*

(BW) Der Satz von Bolzano-Weierstraß: *Jede beschränkte unendliche Teilmenge von K besitzt mindestens einen Häufungspunkt.*

BEWEIS.

(**AO**) $\Longleftrightarrow$ (**MA**).

(a) Gelte **(AO)** . Wie man sofort sieht, konvergiert die Folge (a_n) $(n \in \mathbf{N})$ gegen die obere Grenze der Menge der Folgenglieder.

(b) Gelte hiernach **(MA)** und sei C abgezählt. Ist dann A eine nach oben beschränkte Teilmenge, so können wir sukzessive Elemente $c_1, \ldots, c_n, \ldots \in C$ derart wählen, dass c_n jeweils das aufgrund der Abzählung von C erste Element aus C unterhalb aller oberen Schranken von A ist, das $c > c_i$ $(1 \leq i \leq n-1)$ erfüllt. Auf diese Weise erhalten wir eine monoton wachsende Folge (c_n), die offenbar die gleichen oberen Schranken hat wie A. Dann ist aber der *Limes* von (c_n) obere Grenze zu A.

$(\mathbf{AO}) \Longleftrightarrow (\mathbf{BW})$.

(a) Gelte **(AO)**. Sei B eine unendliche beschränkte Menge im Intervall $[\,a, b\,]$. Dann gilt: Rechts von a liegen unendlich viele Punkte aus B, also ist die Menge X der Punkte x mit der Eigenschaft

rechts von x liegen unendlich viele Punkte aus B

nicht leer und nach oben begrenzt.

Sei nun $\Omega := Sup\,(X)$. Dann ist Ω Häufungspunkt zu B. Denn wählen wir irgendeine Umgebung $(u, v) \ni \Omega$ von Ω, so liegen rechts von v nur endlich viele, aber rechts von u unendlich viele Elemente aus B, und das bedeutet, dass mindestens ein Punkt aus B in (u, v) liegt.

(b) Gelte hiernach **(BW)** und sei $A|B$ eine Lücke in $\mathfrak{K}$. Dann existiert zu jedem $a \in A$ noch ein a', a'' in A mit $a < a' < a''$. Also können wir eine Umgebung $U(a)$ zu a so wählen, dass rechts von $U(a)$ noch ein Element aus A liegt.

Folglich könnten wir sukzessive mit Hilfe der Abzählindizes Elemente $a_{i_1} < a_{i_2} < \ldots < a_\kappa$ mit paarweise disjunkten Umgebungen wählen, derart dass jedes $a \in A$ unterhalb eines a_{i_n} läge, so dass wir zu einer beschränkten unendlichen Teilmenge gelangten, die mit Widerspruch zur Voraussetzung keinen Häufungspunkt enthielte. □

Bis hierher hatten wir es mit angeordneten Mengen zu tun. Mit Blick auf die Differential-Integralrechnung, der wir uns ja in späteren Kapiteln zuwenden werden, hier noch ein Abschnitt über

3.3 Das AOG und die Infinitesimalrechnung

3. 3. 1 Definition. Ein Körper $\mathfrak{K}$ heißt angeordnet bezüglich einer Ordnungsrelation $<$, wenn gilt:

$$a < b \Longrightarrow\ a + x < b + x \quad \text{und} \quad 0 \leq a, b \Longrightarrow 0 \leq ab\,.$$

3. 3. 2 Definition. Sei $\mathfrak{K}$ ein angeordneter Körper und f eine Funktion $K \longrightarrow K$. Dann heißt f differenzierbar an der Stelle x_0, wenn gilt:

$$\exists\, a\ :\quad \frac{f(x_n) - f(x_o)}{x_n - x_0} \to a =: f'(x_o)\,.$$

3. 3. 3 Proposition. *Ist $\mathfrak{K}$ sogar ein angeordneter Körper, so sind neben den soeben behandelten Äquivalenzen drei weitere wichtige Äquivalenzen zu erwähnen, nämlich:*

(SR) Der Satz von Rolle *Ist f stetig über $[\,a,b\,]$ mit $f(a)=f(b)$ und differenzierbar in (a,b), so gibt es eine Stelle ξ in (a,b) an der f' verschwindet.*

(MS) Der Mittelwertsatz *Sei f stetig über $[\,a,b\,]$ und differenzierbar in (a,b). Dann gibt es ein ξ in (a,b) mit*

$$f'(\xi)=\frac{f(b)-f(a)}{b-a}$$

(AS) Der Ableitungssatz:

$$f'=0 \Longrightarrow f=const\,.$$

BEWEIS. Wir bemerken vorweg, dass $(K,<)$ im vorliegenden Fall dicht ist, da zwischen je zwei Elementen a,b noch das weitere Element $(a+b):2$ liegt. Hiernach können wir zeigen:

$(\mathbf{AO})\Longrightarrow(\mathbf{SR})$.

Denn erfüllt f die Voraussetzungen des **(SR)**, so ist f konstant oder aber es nimmt nach **(AO)** der Wertebereich von f an einer Stelle ξ aus (a,b) sein Maximum oder sein Minimum an. Hier verschwindet dann aber f', denn man nähere sich dem Wert dem Wert ξ das eine Mal von links, das andere Mal von rechts.

$(\mathbf{SR})\Longrightarrow(\mathbf{MS})$:

Wir betrachten

$$\phi(x):=f(x)-\frac{f(b)-f(a)}{b-a}\cdot(x-a)\,.$$

und beachten den Satz von Rolle.

$(\mathbf{MS})\Longrightarrow(\mathbf{AS})$:

Für beliebige x und x_0 aus $[\,a,b\,]$ gilt

$$\frac{f(x)-f(x_0)}{x-x_0} = f'(\xi) = 0\,.$$

$(\mathbf{AS}) \Longrightarrow (\mathbf{AO})$:

Denn, gäbe es eine Lücke $A|B$, so könnten wir eine Treppenfunktion f konstruieren mit $f' = 0$, mit Widerspruch zu **(AO).** □

ÜBUNG: Man zeige: Ist $\mathfrak{K}$ ein angeordneter Körper, so ist zum Axiom von der oberen Grenze ebenfalls äquivalent

(IS) Der Intervallschachtelungssatz: Sind (a_n), (b_n) zwei Folgen mit $[\,a_n,b_n\,] \subseteq [\,a_{n+1},b_{n+1}\,]$ und gilt zudem $(a_n - b_n) \to 0$, so enthält $\cap[\,a_n,b_n\,]$ $(n \in \mathbf{N})$ genau einen Wert.

Anmerkung: Die Frage stellt sich natürlich, ob denn überhaupt angeordnete Körper existieren, die nicht stetig sind. Die Antwort ist trivial: Man betrachte $\mathfrak{Q}$.

Interessanter ist jedoch

3.4 Der Körper der rationalen Funktionen über $\mathfrak{R}$.

bzw. ganz allgemein: der Körper der rationalen Funktionen über einem angeordneten Körper $\mathfrak{K}$.

Definieren wir nämlich $f(x) < g(x)$, gdw. der höchste Koeffizient der Differenz $g(x) - f(x)$ positiv ist, so liefert dies eine lineare Ordnung im Polynombereich $\mathfrak{K}\,[x]$, die sich dann kanonisch ausdehnen lässt auf Den Körper $\mathfrak{K}\,(x)$ vermöge:

$$\frac{f}{g} < \frac{u}{v} \Longleftrightarrow f \cdot v < g \cdot u\,.$$

Doch ist die so definierte Anordnung nicht nur nicht stetig, sondern nicht einmal archimedisch.

Projekt: Man studiere die Herleitungen zum Axiom von der oberen Grenze in $\mathfrak{R}\,(x)$.

Man beachte hierbei insbesondere, dass die Elemente aus R, aufgefasst als Funktionen, auch Elemente aus $\mathfrak{R}(x)$ sind und dass es in $\mathfrak{R}(x)$ Werte gibt, die größer sind als 0, aber kleiner als jedes positive Element ε aus $\mathfrak{R}$, weshalb man diese Werte auch zu Recht als unendlich klein bezeichnet. Insbesondere gilt mit $1/x =: \varepsilon$

$$0 < n \cdot \varepsilon < r \ \ (\forall r \in \mathbf{R}) .$$

So kann man bei der Bestimmung der Ableitung an der Stelle x_0 sagen, dass sich dort der Differenzenquotient nur um einen unendlich kleinen Wert von $f'(x_0)$ unterscheidet. Z. B. erhalten wir für $f(x) = x^2$

$$\frac{(x_0 + h)^2 - (x_0)^2}{h} = \frac{2x_0 h + h^2}{h} = 2x_0 + h$$

mit unendlich kleinem h.

3.5 Das AOG und die rationalen Zahlen

Und warum reichen uns, müssen uns reichen, die rationalen Zahlen, ja die ganzen Zahlen, um die Rakete vom Computer gesteuert zum Mond zu schießen – und zurück zu holen?

Es ist der Umstand, dass die irrationalen Zahlen gewissermaßen den „Kitt" liefern – der die rationalen Zahlen „bindet". Ob man auch ein Modell der Art bilden dürfte, dass die irrationalen Zahlen auf die rationalen Zahlen einwirken, wie Gravitationspunkte auf Massenpunkte, möchte der Autor außen vor lassen. Tatsächlich arbeiten wir ja nicht mit beliebigen stetigen Funktionen über $\mathbf{Q}$, sie erfüllen ja nicht notwendig jene AO-äquivalenten Bedingungen, die wir formuliert haben. Nein, wir arbeiten – und das ist ein Unterschied – mit jenen Funktionen über $\mathbf{Q}$, die sich ergänzen lassen zu stetigen Funktionen auf $\mathbf{R}$. Dies sichert dann, dass im Reellen „exakte Werte" existieren, die es nur noch hinreichend anzunähern gilt. Mittels rationaler Zahlen kommen wir ja beliebig nahe an eine vorgegebene reelle Zahl heran, so genau, dass weitere Genauigkeit rein inhaltlich gesehen keine Verbesserungen brächte.

3.6 Das AOG und die Ω-Analysis

Kommen wir noch einmal zurück auf den Körper $\mathbf{R}(x)$ bezüglich der oben definierten Anordnung.

In der angewandten reellen Analysis geht es um nichts anderes als um Näherungen, gute Näherungen, und schon das Taylorpolynom zeigt, dass wir uns im Anwendungsbereich zurückziehen können auf rationale Funktionen.

Betrachten wir nun solche Funktionen auf $\Omega(\mathbf{R})$, so bietet sich die Methode der numerisch vernachlässigten unendlich kleinen Zahlen, der Epsilons an.

Denn, es ist ja $r \cdot h < s$ für jedes Paar $r, s \in \mathbf{R}$ und $r + h < s$ für jedes $r < s$. Der Gewinn ist methodischer und psychologischer Art.

Naturwissenschaftler dürfen hiernach formulieren:
wird nun s „unendlich klein", so ...

Vor allem aber der Lehrer hat eine Interpretationsmöglichkeit an der Hand für den Fall, dass ein Schüler formuliert:

„wenn aber nun dieses h unendlich klein wird ..."

WETTEN DASS die deutschen Oberlehrer an dieser Stelle fast ausnahmslos in Schwierigkeiten gerieten, doch das ist nicht den deutschen Oberlehrern, das ist den deutschen Professoren anzulasten.

Den einen wie den anderen sei an dieser Stelle zur Lektüre empfohlen:

David Hilbert: **Natur und Mathematisches Erkennen**

Ein brillanter Beitrag zur „Höheren Didaktik" – wie der Autor sie versteht.

3.7 In memoriam Karl Dörge

In diesem Abschnitt möchte der Autor seines Lehrers Karl Dörge gedenken. In dessen „Grünem Buch"[14] zur Differential- und Integralrechnung in einer Veränderlichen, basierend auf seiner Vorlesung zu diesem Stoff, verfasst gemeinsam mit seinem Schüler Klaus Wagner, findet sich ein Theorem zur Theorie der total geordneten Mengen, das im Falle stetiger Funktionen unmittelbar den zentralen Satz vom Maximum stetiger Funktionen liefert – und das den Autor als Studenten geradezu „fasziniert" hat.

Hierbei halten wir uns zunächst an den O-Ton Dörge

3. 7. 1 Definition. Wir sagen von zwei Kurven $\mathfrak{C}_1, \mathfrak{C}_2$, dass $\mathfrak{C}_1$ die Kurve $\mathfrak{C}_2$ übertrifft, wenn es eine Höhe von $\mathfrak{C}_1$ gibt, die größer als eine jede Höhe von $\mathfrak{C}_2$ ist.

Die gegenteilige Aussage lautet:

Zu einer jeden Höhe von $\mathfrak{C}_1$ gibt es immer eine mindestens gleich große Höhe von $\mathfrak{C}_2$. Dies nennen wir $\mathfrak{C}_2$ erreicht $\mathfrak{C}_1$.

Zur Erläuterung dieser Bezeichnungen betrachten wir die folgenden Kurven. $\mathfrak{C}_1$ sei die Kurve: $f(x) = \sin x, \left(0, \frac{\pi}{2}\right)$, $\mathfrak{C}_2$ die Kurve $f(x) = \cos x, (-\pi, 0)$. Dafür gilt dann: $\mathfrak{C}_2$ übertrifft $\mathfrak{C}_1$, erst recht $\mathfrak{C}_2$ erreicht $\mathfrak{C}_1$, aber $\mathfrak{C}_1$ erreicht nicht $\mathfrak{C}_2$.

3. 7. 2 Lemma. *Man habe über* $\langle x_0, x_1\rangle, \langle x_1, x_2\rangle, \langle x_2, x_3\rangle$ *je eine Kurve* $\mathfrak{C}_1$, $\mathfrak{C}_2$ *und* $\mathfrak{C}_3$.[1)]

Voraussetzungen

1. $\mathfrak{C}_1 + \mathfrak{C}_2$ übertrifft $\mathfrak{C}_1$ und 2. $\mathfrak{C}_1 + \mathfrak{C}_2$ erreicht $\mathfrak{C}_3$[2)]

Behauptung: $\mathfrak{C}_2$ übertrifft $\mathfrak{C}_1$ und erreicht $\mathfrak{C}_3$

Denn nach Voraussetzung (1) übertrifft mindestens eine Höhe von $\mathfrak{C}_2 + \mathfrak{C}_3$ das $\mathfrak{C}_1$. Ist dies eine Höhe von $\mathfrak{C}_3$, die also das $\mathfrak{C}_1$ übertrifft, so erreicht nach Voraussetzung (2) unser $\mathfrak{C}_2$ gewiss $\mathfrak{C}_3$.

In dem übrig bleibenden Falle, wo also eine Höhe von $\mathfrak{C}_3$ das $\mathfrak{C}_1$ übertrifft, muss nach Voraussetzung unser $\mathfrak{C}_2$ das $\mathfrak{C}_3$ erreichen und, da $\mathfrak{C}_3$ das $\mathfrak{C}_1$ übertrifft, gewiss auch $\mathfrak{C}_1$ übertreffen.

In beiden Fällen hat also $\mathfrak{C}_1$ die in der Behauptung formulierten Eigenschaften. –

Hat man eine Kurve $\mathfrak{C}$ über $\langle a, b\rangle$, ferner $\langle a', b'\rangle \leq \langle a, b\rangle$, so bezeichnen wir den Teil von $\mathfrak{C}$, der über $\langle a', b'\rangle$ liegt, mit $\mathfrak{C}\langle a', b'\rangle$.

Wir sagen $\mathfrak{C}$ verhält sich bei ξ maximal, wenn für jedes x_1 aus (a, ξ) und jedes x_2 aus (ξ, b) gilt: $\mathfrak{C}\langle x_1, x_2\rangle$ übertrifft $\mathfrak{C}\langle a, x_1\rangle$ und erreicht $\mathfrak{C}\langle x_2, b\rangle$. Wir sagen $\mathfrak{C}$ verhält sich bei $\xi = a$ maximal, wenn für jedes x' aus (a, b) gilt: $\mathfrak{C}\langle a, x'\rangle$

[1)] In Anlehnung an den späteren Beweis wollen wir annehmen, dass $\mathfrak{C}_1$, $\mathfrak{C}_2$ und $\mathfrak{C}_3$ durch Zerschneidung einer einzigen über $\langle x_0, x_2\rangle$ gegebenen Kurve $\mathfrak{C}$ in den beiden über x_1, x_2 liegenden Kurvenpunkten aus $\mathfrak{C}$ entstehen.

[2)] In der vorstehenden Zeichnung ist so getan, als ob unsere drei Kurven durch Zerschneidung einer stetig gezeichneten Kurve entstehen. Wir bemerken zu diesem Hilfssatz ausdrücklich, dass er aber für beliebiges $\mathfrak{C}$ formuliert und bewiesen ist. In Wahrheit ist er allgemeine ein Satz über beliebige Zahlenmengen, der für nach oben beschränkte Zahlenmengen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$, wenn wir etwa unter a, b, c ihre oberen Grenzen verstehen, auch wie folgt formuliert werden kann: Aus 1. $\max(b, c) > a$ und 2. $\max(a, b) \geq c$ folgt $b > a$ und $b \geq c$.

erreicht $\mathfrak{C}\langle x', b\rangle$. Wir sagen schließlich, $\mathfrak{C}$ verhält sich bei $\xi = b$ maximal, wenn für jedes x' aus (a, b) gilt $\mathfrak{C}\langle x', b\rangle$ übertrifft $\mathfrak{C}\langle a, x'\rangle$.

Wir sagen, $\mathfrak{C}$ verhält sich bei ξ' minimal, wenn sich das an der x-Achse gespiegelte $f(x)$ bei ξ' maximal verhält.[3)]

Nunmehr gilt [der]:

3. 7. 3 Satz über das Extremalverhalten beliebiger Kurven. *Hat man eine Kurve $\mathfrak{C}$ über $\langle a, b\rangle$, so gibt es (genau)[4)] eine Stelle ξ in $\langle a, b\rangle$, bei der sich $\mathfrak{C}$ maximal verhält.*

Entsprechend gibt es genau eine Stelle ξ' in $\langle a, b\rangle$, bei der sich $\mathfrak{C}$ minimal verhält.

...Wir nennen ein x' aus (a, b) (um eine kurze Bezeichnung zu haben) ein γ, wenn $\mathfrak{C}\langle a, x'\rangle$ von $\mathfrak{C}\langle x', b\rangle$ übertroffen wird.

Gibt es dann kein γ, d.h. erreicht $\mathfrak{C}\langle a, x'\rangle$ immer das $\mathfrak{C}\langle x', b\rangle$, so hat ... $\mathfrak{C}$ bei $\xi = a$ maximales Verhalten.

Wir können daher annehmen, dass es mindestens ein γ gibt.

Nun sei ξ die obere Grenze der Menge unserer γ. Wir zeigen $\mathfrak{C}$ verhält sich bei ξ maximal. Wir bemerken zuvor, dass wenn x' ein γ ist, jede links davon liegende Zahl aus (a, b) erst recht ... ein γ ist. Nun wählen wir in (a, ξ) ein beliebiges x_1. Nach Definition von ξ wird x_1 von der Menge unserer γ überschritten. x_1 ist also ein γ. D. h.

$$(1) \quad \mathfrak{C}\langle x_1, b\rangle \text{ übertrifft } \mathfrak{C}\langle a, x_1\rangle .$$

Ist $\xi = b$, so hat ... $\mathfrak{C}$ bei b maximales Verhalten.

Wir können also $\xi < b$ annehmen. Dann wählen wir in dem (ξ, b) ein beliebiges x_2. Natürlich ist x_2 kein γ. D. h.

$$(2) \quad \mathfrak{C}\langle a, x_2\rangle \text{ erreicht } \mathfrak{C}\langle x_2, b\rangle .$$

Also folgt aus (1) und (2) nach dem Hilfssatz 3.7.2 $\mathfrak{C}\langle x_1, x_2\rangle$ übertrifft $\mathfrak{C}\langle a, x_1\rangle$ und erreicht $\mathfrak{C}\langle x_2, b\rangle$.[5)]

[3)] Schöner ist es, auch das Minimalverhalten unter Zuhilfenahme der Definition 3.7.1 für sich ausführlich einzuführen, wobei dann natürlich überall nur „größer" sinngemäß durch „kleiner" zu ersetzen ist. Die obige Definition erspart uns jedoch einige Worte.

[4)] Den Beweis für „genau ein" schieben wir an dieser Stelle noch auf.

[5)] Man überzeugt sich leicht, dass unser ξ auch die einzige Stelle in $\langle a, b\rangle$ ist, bei der sich $\mathfrak{C}$ maximal verhält. Denn man habe ein $x_0 \neq \xi$ aus $\langle a, b\rangle$ und ein m aus $(x_0, \xi$. Der Mittelpunkt von $x_0\xi$ sei m. Es liege x_0 links von ξ. Dann übertrifft $\mathfrak{C}\langle m, b\rangle$ gewiss $\mathfrak{C}\langle a, m\rangle$, d. h. $\mathfrak{C}\langle a, m\rangle$ erreicht nicht $\mathfrak{C}\langle m, b\rangle$. Also verhält sich $\mathfrak{C}$ bei x_0 nicht maximal. Andererseits liege x_0 rechts von ξ. Dann erreicht $\mathfrak{C}\langle a, m\rangle$ gewiss $\mathfrak{C}\langle m, b\rangle$, d. h. $\mathfrak{C}\langle m, b\rangle$ übertrifft nicht $\mathfrak{C}\langle a, m\rangle$. Also verhält sich $\mathfrak{C}$ auch bei $x_0 > \xi$ nie maximal.

3. 7. 4 Der Existenzsatz vom Maximum und Minimum stetiger Funktionen.

Hat man in dem abgeschlossenen Intervall $\langle a, b\rangle$ eine stetige Funktion $f(x)$, so gibt es immer eine (erste, d.h. kleinste) Stelle ξ in $\langle a, b\rangle$, so dass $f(\xi)$ Maximum von $f(x)$ist.

Entsprechendes gilt für das Minimum.

Wir brauchen den Satz nur für das Maximum zu beweisen, da ein Minimum von $f(x)$ ein Maximum von $-f(x)$ ist. Nun betrachten wir unser durch den Satz 3.7.3 nachgewiesenes ξ. Wir zeigen, dass $F(\xi)$ die Bedingung des Maximums erfüllt.

Denn es sei x_0 ein von ξ verschiedener Punkt aus $\langle a, b\rangle$. Es sei eine Zahl $\eta > 0$ gegeben. Nach Definition 3.7.1 gibt es ein $\mathfrak{I}(\xi)$, worüber dauernd $f(x) < f(\xi) + \eta$ gilt. Aus dem Maximalverhalten von $f(x)$ in diesem $\mathfrak{I}(\xi)$ bzw. $\mathfrak{I}_r(a)$, $\mathfrak{I}_l(b)$, so dass $f(x) \geq f(x_0)$ für dieses x gilt. Die beiden letzten Ungleichungen liefern $f(\xi) \geq f(x_0) - \eta$. Dies gilt für jedes $\eta > 0$. Also folgt $f(\xi) \geq f(x_0$ für jedes x_0 aus $\langle a, b\rangle$. D. h.$f(\xi)$ ist Maximum.

Für jedes x_0 aus $\langle a, b\rangle$ links von ξ gilt sogar: $f(\xi) > f(x_0)$.

Denn jedes unserer $\mathfrak{C}\langle x_1, b\rangle$ übertraf ja sogar das $\mathfrak{C}\langle a, x_1\rangle$.

Also ist ξ die erste Stelle in $\langle a, b\rangle$, in der $f(x)$ sein Maximum annimmt. –

Soweit das Original. Tatsächlich gilt der soeben bewiesene Satz auch losgelöst von den reellen Zahlen, denn man operiere statt mit einem η mit einem $g(x) = c > f(\xi)$. Dann resultiert der Satz für das Minimum nach dem Dualitätsprinzip.

Endlich gilt der Kehrsatz:

3. 7. 5 Proposition. *Ist $\mathfrak{T}$ linear und dicht geordnet und gilt der Satz über das Extremalverhalten beliebiger Funktionen über den Intervallen $\langle a, b\rangle$, so erfüllt $\mathfrak{T}$ das AOG.*

Denn wäre $A)(B$ eine Lücke im Intervall $\langle a, b\rangle$, so besäße die Funktion f mit $f(x) = x$ für $x \in A$ und $f(x) = c < a$ für $x \in B$ kein ξ der gewünschten Art.

Und schließlich: Besitzt jede über $\langle a, b\rangle$ stetige Funktion ein Maximum (ein Minimum), so verhält sich jede beliebige Funktion über $\langle a, b\rangle$ an mindestens einer Stelle ξ maximal (minimal), da die Maximum- (Minimum-) Bedingung äquivalent ist zum AOG.

Resümee:

3. 7. 6 Proposition. *Sei $\mathfrak{T} = (\mathfrak{T}, <)$ eine Kette. Dann sind äquivalent:*

(a) *$\mathfrak{T}$ ist stetig geordnet.*

(b) *Jedes Intervall $\langle a, b\rangle$ aus $\mathfrak{T}$ erfüllt die Bedingung des Extremalverhaltens für beliebige Funktionen.*

(c) *Jedes Intervall $\langle a, b\rangle$ aus $\mathfrak{T}$ erfüllt die Maximum/Minimum-Bedingung für stetige Funktionen.*

Somit reiht sich der Satz über das Extremalverhalten beliebiger Funktionen ein in die Serie von Äquivalenzen zum AOG.

Kapitel 4

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.

4.1 Posets und Verbände

Wir wiederholen:

4. 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

$$\forall a, b\ \exists\, c =: sup(a, b) : (a, b \leq c) \quad \& \quad (a, b \leq x \Longrightarrow c \leq x)\,,$$

so heißt $(M, \leq)$ ein *sup-Halbverband.*

Dual ist der *inf-Halbverband* erklärt.

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.

4. 1. 2 Lemma. *Ist* $(M, \leq)$ *ein* sup*-Halbverband, so haben wir:*

$$\begin{aligned} &\text{(I)} && a \vee a &&= a \\ &\text{(K)} && a \vee b &&= b \vee a \\ &\text{(A)} && a \vee (b \vee c) &&= (a \vee b) \vee c\,. \end{aligned}$$

DENN: $\sup(a, b) = \sup(x, y)$ ist äquivalent zu $a, b \leq u \iff x, y \leq u$. □

4. 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 $a, b \leq a \cdot b \;\&\; a \cdot x = x = b \cdot x \Longrightarrow (a \cdot b) \cdot x = x$. □

Nach 4.1.2 und 4.1.3 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:

4. 1. 4 Proposition. *Die oben erklärten Operatoren* $\mathfrak{H}$ *und* $\mathfrak{P}$ *erfüllen:*

$$\begin{aligned} \mathfrak{P}(\mathfrak{H}(M, \leq)) &\cong (M, \leq) \\ \text{und} \qquad \mathfrak{H}(\mathfrak{P}(H, \cdot)) &\cong (H, \cdot)\,. \end{aligned}$$

Hiernach kommen wir zur Definition des *Verbandes,* einer Struktur, die schon von DEDEKIND unter dem Namen *Dualgruppe* eingeführt wurde, vgl. [11].

4. 1. 5 Definition. Sei $\mathfrak{V} := (V, \vee, \wedge)$ eine Algebra vom Typ (2,2). Dann heißt $\mathfrak{V}$ ein *Verband*, wenn gilt:

$$\begin{array}{llll}
(\mathrm{I}\vee) & a \vee a = a & (\mathrm{I}\wedge) & a \wedge a = a \\
(\mathrm{K}\vee) & a \vee b = b \vee a & (\mathrm{K}\wedge) & a \wedge b = b \wedge a \\
(\mathrm{A}\vee) & a \vee (b \vee c) = (a \vee b) \vee c & (\mathrm{A}\wedge) & a \wedge (b \wedge c) = (a \wedge b) \wedge c \\
(\mathrm{V}\vee) & a \vee (b \wedge a) = a & (\mathrm{V}\wedge) & a \wedge (b \vee a) = a \ .
\end{array}$$

Wie man leicht erkennt, ist der Verband selbstdual erklärt, d. h. 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

$$\begin{array}{rcll}
a \wedge a & = & a \wedge (a \vee (b \wedge a)) & (\mathrm{V}\vee) \\
& = & a \wedge ((b \wedge a) \vee a) & (\mathrm{K}\vee) \\
& = & a & (\mathrm{V}\wedge)\,.
\end{array}$$

Weiter folgt mittels (K$\vee$), (K$\wedge$), (V$\wedge$), (V$\vee$) die Äquivalenz:

$$a \wedge b = a \iff a \vee b = b\,. \tag{4.11}$$

Damit erhalten wir zusammenfassend

4. 1. 6 Proposition. *Ist $(V, \vee, \wedge)$ ein Verband, so liefert die Festsetzung*

$$\begin{array}{rcl}
a \leq b & :\Longleftrightarrow & a \wedge b = a \\
& (\Longleftrightarrow & a \vee b = b)
\end{array}$$

eine Partialordnung auf V , die nach (4.11) den Regeln der Isotonie genügt:

$$\begin{array}{rcl}
b \leq c & \Longrightarrow & a \wedge b \leq a \wedge c \\
& \& & a \vee b \leq a \vee c\,.
\end{array} \tag{ISO}$$

4.2 Modulare und 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.

4. 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:

4. 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 (D′∧), dann folgt $(\mathrm{D}_{\wedge})$ und wir erhalten mittels (V∨)

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

Als ein halbverbandstheoretisches Äquivalent der Distributivität – unter vielen anderen – erhalten wir

4. 2. 3 Proposition. *Ein Verband $\mathfrak{V}$ ist genau dann distributiv, wenn er die nachfolgende Zerlegungsbedingung erfüllt:*

(Z) $$x \leq a \vee b \Longrightarrow x = x_a \vee x_b \ \ (\exists\ x_a \leq a, x_b \leq b)$$

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 erfüllt ist. Also gilt (Z) $\Longrightarrow$ (D).

Sei hiernach (D) erfüllt. Dann folgt (Z) unmittelbar *via*

$$x = x \wedge (a \vee b) = (x \wedge a) \vee (x \wedge b) =: x_a \vee x_b \ \ (x_a \leq a, x_b \leq b) \qquad \square$$

4. 2. 4 Definition. Ein Verband heißt *modular*, wenn er der selbstdualen Implikation genügt:

(M) $$a \geq c \implies a \wedge (b \vee c) = (a \wedge b) \vee c\,.$$

(M) lässt sich auch als Gleichung schreiben. Denn, man ersetze a durch $a \vee c$. Dann liest sich (M) als

$$(a \vee c) \wedge (b \vee c) = ((a \vee c) \wedge b) \vee c\,.$$

Ferner beachte man, dass es in der obigen Implikation genügt, die Inklusion der linken Seite in der rechten zu fordern. Denn, es gilt ja stets $a \geq a \wedge b$ und nach (ISO) $b \vee c \geq (a \wedge b) \vee c$.

Insbesondere sind also *per definitionem* alle distributiven Verbände (erst recht) modular.

Ein klassisches Beispiel für einen modularen Verband ist etwa der Verband der Untergruppen einer abelschen Gruppe.

BEWEIS. Sei $\mathfrak{G}$ eine abelsche Gruppe. Wir schreiben ihre zweistellige Operation additiv. Dann gehört ein $x \in G$ genau dann zum Erzeugnis der beiden

Untergruppen $\mathfrak{A}, \mathfrak{B}$, wenn es sich in der Form $a+b$ mit $a \in A, b \in B$ schreiben lässt, und dies liefert im Falle $A \supseteq C$:

$$\begin{array}{rcl} x \in A \cap (B+C) & \Longrightarrow & x = y+z \ (y \in B, z \in C \subseteq A) \\ & \Longrightarrow & y = x-z \in A \cap B \\ & & \qquad (\text{wegen } y \in B \ \& \ x, z \in A) \\ & \Longrightarrow & x = (x-z)+z \\ & \Longrightarrow & x \in (A \cap B)+C \end{array}$$

also $A \cap (B+C) \subseteq (A \cap B)+C$, was zusammen mit $A \cap (B+C) \supseteq (A \cap B)+C$ die Behauptung liefert. □

Der Beweis des soeben bewiesenen Satzes liefert unmittelbar als Korollare:

4. 2. 5 Korollar. *Der Verband der Unterräume eines jeden linearen Raumes ist modular.*

4. 2. 6 Korollar. *Der Verband der Ideale eines jeden Ringes ist modular.*

4. 2. 7 Definition. Ein Verband $(V, \vee, \wedge)$ mit 0 als Minimum und 1 als Maximum heißt *komplementär*, wenn zu jedem x ein x' existiert mit

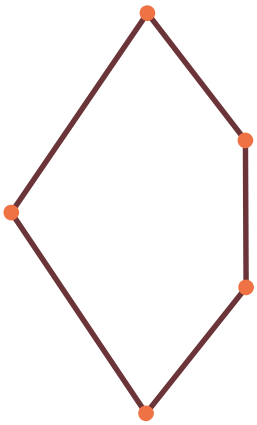
$$\text{(COM)} \qquad x \vee x' = 1 \quad \& \quad x \wedge x' = 0.$$

Ist diese Bedingung bezogen auf jedes *Hauptideal* $(\, x\,]$ erfüllt, so nennt man $\mathfrak{V}$ *abschnittskomplementär.*

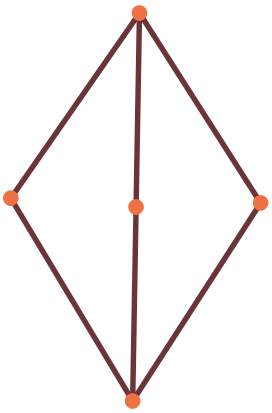
4. 2. 8 Definition. Ist $\mathfrak{V}$ distributiv und komplementär, so heißt $\mathfrak{V}$ ein *Boolescher Verband*, auch eine *Boolesche Algebra.*

Das klassische Beispiel für den Booleschen Verband ist der Potenzmengenverband. Klassisches Beispiel für den komplementären modularen Verband ist der Verband aller linearen Teilräume eines Vektorraumes. Kern-Beispiele liefern das *Pentagon* und der *Diamant,* siehe unten. Sie werden fundamental in die Theorie der modularen bzw. distributiven Verbände eingehen. Diese beiden Klassen sollen als nächstes „geometrisch" charakterisiert werden. Hierzu erinnern wir vorweg noch einmal an das Hasse-Diagramm:

Ist $(P, \leq)$ eine endliche Partialordnung, so lässt sich $(P, \leq)$ darstellen durch ein Diagramm. Denn, man ordne jedem $a \in M$ einen Punkt der *cartesischen*



DAS PENTAGON



DER DIAMANT

Ebene, sprich des $\mathbf{R}^2$, derart zu, dass sich alle $x \geq a$ „von unten nach oben" erreichen lassen.

Eine Methode, Klassen von Verbänden zu charakterisieren, ist der Weg über *„verbotene" Unterverbände.* Extrem trivial ist etwa die Charakterisierung der Ketten durch die Eigenschaft, keine *Raute* als Unterverband zu enthalten.

Interessanter wird es bei der Klasse der modularen bzw. distributiven Verbände, die sich über das Pentagon bzw. den Diamanten, s. o., charakterisieren lassen. Hier gilt zunächst genauer:

4. 2. 9 Dedekind. *Ein Verband ist modular genau dann, wenn er keinen Unterverband enthält, der isomorph ist zum Pentagon, kurz, wenn er kein Pentagon enthält.*

BEWEIS. Ist $\mathfrak{V}$ nicht modular, so existieren Elemente a, b, c mit $a \geq c$ mit

$$A := a \wedge (b \vee c) \;\; > \;\; (a \wedge b) \vee c =: C\,,$$

und es kann das Element $b =: B$ das Element C nicht übertreffen und das Element A nicht unterschreiten. Denn sonst wäre im ersten Fall $b \geq c$ und im zweiten Fall $b \leq a$ und damit in jedem Fall $a \wedge (b \vee c) = (a \wedge b) \vee c$ erfüllt.

Somit sind die Elemente A, B, C paarweise verschieden, und es gilt zudem $B \wedge A = b \wedge a \geq B \wedge C \geq b \wedge a = B \wedge A$, also $B \wedge A = B \wedge C$ und dual $B \vee A = B \vee C$.

Enthält der Verband umgekehrt ein Pentagon, so ist die Verletzung der Modularität evident. □

Der letzte Satz weist über die Charakterisierung durch das Pentagon hinaus. Denn im Pentagon gibt es zwei Ketten unterschiedlicher *Länge* Dies regt an zur Einführung einer *Dimension* für modulare Verbände. Zu diesem Zweck zunächst

4. 2. 10 Der Kettensatz. *Sei $\mathfrak{V}$ ein modularer Verband und sei die Kette $a < a_1 \ldots < a_n = b$ maximal in dem Intervall $[\,a\,,\,b\,]$. Dann ist $(\,a_1, \ldots, a_n)$ auch längenmaximal in $[\,a\,,\,b\,]$.*

BEWEIS. Wir verfahren induktiv.

Natürlich gilt unsere Behauptung für den Fall, dass a unmittelbar über b liegt, also für den Fall, dass unsere a-Kette die Länge 1 hat.

Sei nun der Satz schon bewiesen für alle maximalen Ketten einer Länge zwischen 1 und $n-1$. Wir gehen aus von einer maximalen a-Kette wie oben und nehmen an, es sei $a < b_1 < b_2 < \ldots < b_n < b_{n+1} = b$ eine formal längere Kette.

Gilt dann etwa $a_k \leq b_m$, so können wir nach Induktionsvoraussetzung eine maximale Kette $a_k < c_1 < c_2 < \ldots < c_\ell < c_{\ell+1} = b_m$ einschieben und ebenfalls nach Induktionsvoraussetzung kalkulieren, dass es von a nach b *via* $a_1, \ldots, a_k, c_1, \ldots, c_{\ell+1} = b_m, \ldots, b_n$ nicht „weiter" ist als entlang $a_1, \ldots a_{n-1}$, woraus fast unmittelbar folgt, dass die b-Kette von a nach b höchstens so viele Elemente enthalten kann wie die a-Kette.

Gibt es aber kein Paar $a_k \leq b_m$ von der soeben angenommenen Art, so bilden wir die Kette

$$a_1 \vee b_1 \leq a_1 \vee b_2 \leq a_1 \vee b_3 \leq \ldots \leq a_1 \vee b_n \leq a_1 \vee b_{n+1}\,.$$

Dann gibt es nach Induktionsvoraussetzung mindestens zwei verschiedene Elemente $b_i\,,\, b_j$ mit $a_1 \vee b_i = a_1 \vee b_j$ und wegen der Maximalität unserer a-Kette auch mit $a_1 \wedge b_i = a_1 \wedge b_j = a$, also ein Pentagon in $\mathfrak{V}$, mit Widerspruch zur Modularität. □

Weiter haben wir:

4. 2. 11 Proposition. *Sei $\mathfrak{V}$ ein modularer Verband und seien a, b zwei Elemente aus V. Dann sind die Intervalle $[\,a \wedge b, b\,]$ und $[\,a, a \vee b\,]$ isomorph.*

BEWEIS. Definiere

$$\begin{aligned} f_a(x) &:= a \vee x \qquad (x \in [\, a \wedge b\,,\, b\,]) \\ f_b(y) &:= b \wedge y \qquad (y \in [\, a\,,\, a \vee b\,])\,. \end{aligned}$$

Dann gilt $u \leq v \Longrightarrow f_a(u) \leq f_a(v)$ und wegen der Modularität

$$f_a(f_b(y)) = f_a(b \wedge y) = a \vee (b \wedge y) = (a \vee b) \wedge y = y$$

und es folgt dual

$$f_b(f_a(x)) = f_b(a \vee x) = b \wedge (a \vee x) = (b \wedge a) \vee x = x\,.$$

Somit ist f_a *surjektiv*, *injektiv* und *isoton*. □

Gilt $a < b$ und $[\, a, b\,] = \{a, b\}$, so nennen wir a und b *benachbart,* auch a einen *unteren Nachbarn* von b bzw. b einen *oberen Nachbarn* von a, und wir schreiben in diesem Fall $a \succ b$. Als Korollar resultiert in dieser Sprechweise aus 4.2.11

4. 2. 12 Der Nachbarsatz. *Ist $\mathfrak{V}$ ein modularer Verband und p oberer Nachbar von $p \wedge q$, so ist $p \vee q$ oberer Nachbar von q.*

4. 2. 13 Definition. Ein Verband heißt *längenendlich*, wenn jede *absteigende Kette* $k_1 > k_2 > \ldots > k_n \ldots$ endlich ist.

Ist $\mathfrak{V}$ längenendlich, so besitzt $\mathfrak{V}$ *a fortiori* ein Minimum 0, da minimale Elemente in jedem Verband übereinstimmen, und ist $\mathfrak{V}$ noch zusätzlich modular, so können wir jedem Element a aus V eindeutig eine natürliche Zahl $\dim(a)$ als Dimension zuordnen, nämlich die eindeutig bestimmte gemeinsame Länge aller *längenmaximalen Ketten* von 0 nach a.

Beachte, nach dem ZORNschen LEMMA bzw. dem Satz von HAUSDORFF existiert eine maximale Kette und diese ist endlich und damit auch längenmaximal. Ist insbesondere unser Verband ein Verband von Teilräumen eines *endlich erzeugten linearen Raumes,* so entspricht die soeben definierte Dimension der für lineare Räume erklärten Dimension (LinAl 1).

4. 2. 14 Definition. Sei $\mathfrak{V}$ ein längenendlicher modularer Verband und a ein Element aus V. Dann verstehen unter der Dimension von a in $\mathfrak{V}$ die soeben erklärte Zahl $\dim(a)$.

Für diese Dimension gilt nach den beiden letzten Sätzen zusätzlich analog zu den Verhältnissen in der Linearen Algebra:

4. 2. 15 Die Dimensionsformel. *Ist $\mathfrak{V}$ ein längenendlicher modularer Verband, so gilt für alle Paare a, b die Formel:*

$$\text{(DF)} \qquad \dim(a) + \dim(b) \;=\; \dim(a \wedge b) + \dim(a \vee b)\,.$$

BEWEIS. Man beachte, dass die Intervalle $[\,a\wedge b\,,\,b\,]$ und $[\,a\,,\,a\vee b\,]$ isomorph sind und gehe das eine Mal von $a \wedge b$ über a, das andere Mal von $a \wedge b$ über b nach $a \vee b$. Dann ergibt sich die Behauptung unmittelbar. □

4. 2. 16 Lemma. *Sei $\mathfrak{V}$ ein modularer Verband. Dann leitet man leicht her:*

$$(x \wedge (y \vee z)) \vee (y \wedge z) = (x \vee (y \wedge z)) \wedge (y \vee z)\,,$$

und es erfüllen die Elemente

$$A = (a \wedge (b \vee c)) \vee (b \wedge c)\,,\ \ldots\ ,\ C = (c \wedge (a \vee b)) \vee (a \wedge b)$$

die Gleichung

$$A \vee B = B \vee C = C \vee A = (a \vee c) \wedge (b \vee c) \wedge (a \vee b) =: 1_{A,B,C}$$

sowie aus Gründen der Dualität

$$A \wedge B = B \wedge C = C \wedge A = (a \wedge c) \vee (b \wedge c) \vee (a \wedge b) =: 0_{A,B,C}.$$

BEWEIS.
$$\begin{aligned} A \vee B &= (a \wedge (b \vee c)) \vee (b \wedge c) \vee (b \wedge (c \vee a)) \vee (c \wedge a) \\ &= (a \wedge (b \vee c)) \vee (b \wedge (c \vee a) \\ &= ((a \wedge (b \vee c)) \vee b) \wedge (a \vee c) && \text{(M)} \\ &= (a \vee b) \wedge (b \vee c) \wedge (a \vee c) && \text{(M)}\,. \end{aligned}$$

□

Hiernach lässt sich herleiten:

4. 2. 17 Birkhoff. *Ein Verband $\mathfrak{V}$ ist distributiv genau dann, wenn er keinen Unterverband enthält, der isomorph ist zum Pentagon oder zum Diamanten.*

BEWEIS. Wir dürfen ausgehen von einem Verband, der modular, aber nicht distributiv ist. Seien hierin nun A, B, C definiert wie oben. Sind dann zwei dieser Elemente gleich, so folgt o.B.d.A. $A \leq B$. Das führt weiter zu:

$$\begin{aligned} a \wedge (b \vee c) &= \Big(a \wedge (b \vee c)\Big) \wedge \Big((b \wedge (a \vee c)) \vee (a \wedge c)\Big) \\ &= \Big(a \wedge (b \vee c) \wedge b \wedge (a \vee c)\Big) \vee (a \wedge c) \qquad \text{(M)} \\ &= (a \wedge b) \vee (a \wedge c)\,. \end{aligned}$$

Somit gelten aus Gründen der Symmetrie im Falle $a \wedge (b \vee c) \not\leq (a \wedge b) \vee (a \vee c)$ die Ungleichungen $A \neq B$ und $A \neq C$.

Es kann aber wegen 4.2.16 auch nicht $B \leq C$ (oder $C \leq B$) erfüllt sein, da im Falle $<$ die Modularität gestört wäre und im Falle $=$ die Regel 4.2.16. Folglich haben wir im Falle $a \wedge (b \vee c) \not\leq (a \wedge b) \vee (a \vee c)$ aus Gründen der Dualität fünf Elemente, $0_{A,B,C}, A, B, C, 1_{A,B,C}$, die ihrerseits einen Unterverband vom Typ des Diamanten bilden. Umgekehrt sind Verbände „mit" Pentagon oder Diamant evidenterweise nicht distributiv. □

Die beiden letzten Propositionen beinhalten noch zusätzlich:

4. 2. 18 Korollar. *Ein Verband $\mathfrak{V}$ ist genau dann distributiv, wenn gilt:*

$$\text{(DIS)} \qquad (a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a)\,.$$

DENN: diese Gleichung schließt sowohl das Pentagon als auch den Diamanten als Unterverband aus, folglich liefert (DIS) die Distributivität.

Auf der anderen Seite ermittelt man (DIS) geradeaus mittels (D$\wedge$). □

(DIS) besagt anschaulich, dass die zum Beweis des Satzes von Birkhoff betrachteten Elemente $0_{A,B,C}$ und $1_{A,B,C}$ zusammenfallen, etwaige Diamanten also zu einem Punkt degenerieren.

4. 2. 19 Proposition. *Ein Verband $\mathfrak{V}$ ist genau dann distributiv, wenn er der Implikation genügt:*

$$\text{(COM)} \qquad \begin{array}{c} a \wedge x = a \wedge y \\ \quad \& \quad \\ a \vee x = a \vee y \end{array} \implies x = y\,.$$

BEWEIS. Ist $(V, \wedge, \vee)$ nicht distributiv, so enthält $\mathfrak{V}$ ein Pentagon oder einen Diamanten, und die obige Implikation ist gestört. Ist $\mathfrak{V}$ aber distributiv, so folgt aus der Prämisse:

$$\begin{aligned} x &= x \wedge (a \vee y) \\ &= (x \wedge a) \vee (x \wedge y) \\ &= (y \wedge a) \vee (y \wedge x) \\ &= y \wedge (a \vee x) \\ &= y \wedge (a \vee y) \\ &= y\,. \end{aligned}$$ □

4.3 Zum Darstellungsproblem

Das Darstellungsproblem im allgemeinen wurde schon unter Posets erörtert.

In diesem Abschnitt wollen wir uns Darstellungsproblemen der Verbandstheorie zuwenden. Zunächst zum Halbverband.

4. 3. 1 Definition. Sei $\mathfrak{H}$ ein $\vee$-Halbverband. Dann heißt eine Teilmenge I aus H ein *Halbverbands-Ideal,* wenn gilt:

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

$I \subseteq H$ ist also ein Ideal gdw. zum einen mit je zwei Elementen a, b auch deren Vereinigung zu I gehört und zum anderen mit jedem $y \in I$ auch alle $x \leq y$ in I liegen.

Wie man leicht bestätigt, ist H selbst ein Ideal und mit jeder Familie von Idealen auch deren Durchschnitt wieder ein Ideal, so dass jede Teilmenge A aus H ein engstes Ideal erzeugt, nämlich den Durchschnitt aller A umfassenden Ideale, bezeichnet – etwa – mit $[\,A\,]$.

Dieses *extern* erklärte *Erzeugnis* erweist sich *intern* leicht als die Menge aller x unterhalb eines geeigneten $a_1 \vee \ldots \vee a_n$ mit $a_i \in A$ $(1 \leq i \leq n)$.

Sind a, b zwei verschiedene Elemente des Halbverbandes $\mathfrak{H}$, so existiert offenbar stets ein a und b trennendes Ideal. Das bedeutet, dass sich der Darstellungssatz für Posets überträgt auf Halbverbände.

Wenden wir uns hiernach den Verbänden zu. Unter welchen Bedingungen lassen sie sich als *Mengenverbände* auffassen?

Da jeder Mengenverband distributiv ist, können wir natürlich nur bei distributiven Verbänden auf eine solche Darstellung hoffen. Hier allerdings gelangen wir leicht ans Ziel. Gilt nämlich etwa $u \not\leq v$, so gibt es nach ZORN unter den *„u schneidenden, aber v meidenden"* Idealen ein maximales, etwa M. Dieses M erfüllt dann – wie wir unten zeigen werden – $a, b \notin M \Longrightarrow a \wedge b \notin M$, also $a \wedge b \in M \Longrightarrow a \in M \vee b \in M$ und ist demnach ein *Primideal.*

DENN: Da $\mathfrak{V}$ distributiv ist, würde im Falle $a \wedge b \in M$ einerseits die Menge aller x mit $a \wedge x \in M$ ein echtes Oberideal A zu M und andererseits die Menge aller y mit $y \wedge x \in M \ \ (\forall x \in A)$ ein echtes, also v enthaltendes *Oberideal* B zu M bilden. Und hieraus würde $v \in A \wedge B = M$ resultieren, mit Widerspruch zur Voraussetzung.

Folglich können wir jeden distributiven Verband unter Erhalt der Operationen $\wedge$ und $\vee$ nach Primidealen zerlegen, d. h. es gilt

4. 3. 2 Birkhoff. *Jeder distributive Verband ist ein Mengenverband.*

Sei hiernach $\mathfrak{V}$ ein Boolescher Verband und seien x, x' zwei Komplemente. Dann enthält jedes von V verschiedene Primideal eines dieser beiden Elemente, wegen $x \wedge x' = 0$, aber auch nur eines dieser beiden Elemente wegen $x \vee x' = 1$. Und das bedeutet:

4. 3. 3 Stone. *Jeder Boolesche Verband ist ein Mengenkörper, d. h. ein komplementärer Mengenverband.*

4.4 Vollständige Verbände

4. 4. 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.

4. 4. 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:

$$\text{(DV)} \qquad s = \bigwedge a_i \ (i \in I) \implies x \vee s = \bigwedge (x \vee a_i) \ (i \in I) \ ,$$

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:

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

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

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 $x^2 + y^2 \leq 1 - k^{-2}$ $(k \in N)$, so gilt im Verband aller abgeschlossenen Teilmengen der Ebene $C \cap \bigvee C_k = C \neq \emptyset = \bigvee (C \cap C_k)$.

4.5 Der Boolesche Verband

Der Begriff des Booleschen Verbandes wurde unter 4.2.8 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 Booeleschen Verbandes als Ring. Hierzu vorweg eine Reduktion des Axiomensystems.

4. 5. 1 Proposition. *Eine Algebra* $\mathfrak{B} := (B, \wedge, \vee, ')$ *ist schon dann ein Boolescher Verband, wenn sie den Gleichungen genügt:*

$$\text{(B11)} \qquad a \wedge b = b \wedge a$$

$$\text{(B12)} \qquad a \vee b = b \vee a$$

$$\text{(B21)} \qquad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

$$\text{(B22)} \qquad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

$$\text{(B31)} \qquad a \wedge (b \vee b') = a$$

$$\text{(B32)} \qquad a \vee (b \wedge b') = a$$

BEWEIS. Wir beweisen zunächst die beiden Gleichungen:

$$\text{(4.28)} \qquad a \wedge a' = b \wedge b'$$

$$\text{(4.29)} \qquad a \vee a' = b \vee b'.$$

Wegen der $\wedge/\vee$ Dualität reicht es natürlich die Gleichung (5.7) 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:

$$\text{(4.30)} \qquad a \wedge 0 = a$$

$$\text{(4.31)} \qquad a \vee 1 = 1$$

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 Assoziativgesetz kommen, vorweg noch die beiden Verschmelzungsgesetze

$$\begin{aligned} &(\mathrm{V}\wedge) && a \wedge (b \vee a) &&= a \\ &(\mathrm{V}\vee) && a \wedge (b \vee a) &&= a\,, \end{aligned}$$

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 der hierzu $\wedge/\vee$-dualen Herleitung.

Hiernach lässt sich das 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:

$$\begin{aligned} & ((a \wedge b) \wedge c) \vee (a \wedge (b \wedge c)) \\ = \; & ((a \wedge b) \vee (a \wedge (b \wedge c))) \wedge (c \vee (a \wedge (b \wedge c))) \\ = \; & (a \wedge (b \vee (b \wedge c))) \wedge ((c \vee a) \wedge (c \vee (b \wedge c)) \\ = \; & (a \wedge b) \wedge ((c \vee a) \wedge c) \\ = \; & (a \wedge b) \wedge c \\ = \; & f(a, b, c) \\ = \; & f(c, b, a) \\ = \; & a \wedge (b \wedge c)\,, \end{aligned}$$

also in Formeln

$$(\mathrm{A}\wedge) \qquad a \wedge (b \wedge c) \;=\; (a \wedge b) \wedge c\,,$$
$$(\mathrm{A}\vee) \qquad a \vee (b \vee c) \;=\; (a \vee b) \vee c\,.$$

Wir betonen noch einmal die Eindeutigkeit des Komplements, vgl. (COM), also $a'' = a$. Diese Regel liefert uns in Kombination mit den Distributivgesetzen

4. 5. 2 Die Regeln von de Morgan.

$$(\mathrm{V}\wedge) \qquad (a \wedge b)' \;=\; a' \vee b'$$
$$(\mathrm{V}\vee) \qquad (a \vee b)' \;=\; a' \wedge b'$$

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 Regeln (5.9), (5.10) 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:

4. 5. 3 Proposition. *Setzen wir in einem Booleschen Verband* $(V, \wedge, \vee, ')$

$$(4.38) \qquad a \oplus b \;:=\; (a \wedge b') \vee (b \wedge a')$$
$$(4.39) \qquad a \odot b \;:=\; a \wedge b\,,$$

so bildet V *bezüglich dieser beiden Operationen einen* idempotenten *Ring* $\mathfrak{R}(V)$*, und es bildet umgekehrt jeder idempotente Ring* $(R, +, \cdot, 1)$ *bezüglich*

$$(4.40) \qquad a \wedge b \;:=\; a \cdot b$$
$$(4.41) \qquad a \vee b \;:=\; a + ab + b$$
$$(4.42) \qquad a' \;:=\; a + 1$$

einen Booleschen Verband $\mathfrak{V}(R)$*. Darüber hinaus erfüllen die beiden hier vorgestellten Operatoren die* Galoisbedingung:

$$(4.43) \qquad \mathfrak{V}(\mathfrak{R}(V) = \mathfrak{V} \quad \& \quad \mathfrak{R}(\mathfrak{V}(R) = \mathfrak{R}$$

BEWEIS. Der Leser ermittelt geradeaus:

$$\text{(R11)} \qquad a \odot b = b \odot a$$

$$\text{(R12)} \qquad (a \odot b) \odot c = a \odot (b \odot c)$$

$$\text{(R13)} \qquad a \odot a = a$$

$$\text{(R14)} \qquad a \odot 1 = a$$

$$\text{(R21)} \qquad a \oplus b = b \oplus a$$

$$\text{(R22)} \qquad a \oplus a = 0$$

$$\text{(R22)} \qquad a \oplus 0 = a$$

Komplizierter sind die beiden restlichen Herleitungen. Zunächst verifizieren wir das Assoziativgesetz

$$\text{(R23)} \qquad a \oplus (b \oplus c) = (a \oplus b) \oplus c$$

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

$$\text{(R23)} \qquad a \odot (b \oplus c) = a \odot b \oplus a \odot c$$

$$\begin{aligned} \text{vermöge} \qquad a \odot (b \oplus c) &= a \wedge ((b \wedge c') \vee (c \wedge b')) \\ &= (a \wedge b \wedge c') \vee (a \wedge c \wedge b') \\ &= 0 \vee (a \wedge b \wedge c') \vee 0 \vee (a \wedge c \wedge b') \end{aligned}$$

$$\begin{aligned}
&= \Big(a \wedge b \wedge a'\Big) \vee \Big(a \wedge b \wedge c'\Big) \vee \Big(a \wedge c \wedge a'\Big) \vee \Big(a \wedge c \wedge b'\Big) \\
&= \Big((a \wedge b) \wedge (a' \vee c')\Big) \vee \Big((a \wedge c) \wedge (a' \vee b')\Big) \\
&= \Big((a \wedge b) \wedge (a \wedge c)'\Big) \vee \Big((a \wedge c) \wedge (a \wedge b)'\Big) \\
&= (a \wedge b) \oplus (a \wedge c) \\
&= (a \odot b) \oplus (a \odot c)\,.
\end{aligned}$$

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

$$ab \;=\; ba \tag{4.53}$$

resultiert. Der Rest darf dem Leser als Übung überlassen bleiben.

Zu verifizieren bleibt (4.43). Betrachten wir also die Operatoren $\mathfrak{V}$ und $\mathfrak{R}$. Hier haben wir zunächst $ab = a \wedge b = a \odot b$ und $a' = a + 1$, denn man beachte $a' \oplus a = 0 \rightsquigarrow a' = a + 1$. Und dies impliziert weiter:

$$\begin{aligned}
a + b &= ab + a + ab + ab + ab + ab + ba + b \\
&= a(b + 1) + a(b + 1) \cdot b(a + 1) + b(a + 1) \\
&= (a \wedge b') \vee (b \wedge a') \\
&= a \oplus b
\end{aligned}$$

□

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.

Deshalb sei betont, dass mit einem Booleschen Ring im folgenden stets ein idempotenter Ring mit 1 gemeint sein wird.

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.

4.6 Verbände mit eindeutigen Komplementen

In den Beschreibungen Boolescher Algebren könnte man ertrinken.

Wir wollen hier nur auf einige Charakterisierungen *via* eindeutiger Komplemente eingehen. Dazu ist jeweils zu zeigen, dass aus den Voraussetzungen die Distributivität des unterliegenden Verbandes folgt.

Zusätzlich sind die nachfolgenden Sätze interessant, insofern sie deutlich machen, welche Bedingungen ein nicht Boolescher Verband mit eindeutigen Komplementen in jedem Fall erfüllen muss.

Lange hat man geglaubt, dass jeder Verband $\mathfrak{V}$ mit eindeutigen Komplementen zwangsläufig distributiv, also Boolesch sei. In der Sprache der Logik, ein wenig salopp, dass eine Logik mit tertium non datur die 2-wertige Logik „ausschöpfe", genauer – beschreibe.

Doch dann konnte Dilworth 1945 in [13] zeigen:

4. 6. 1 Dilworth. *Jeder Verband lässt sich einbetten in einen Verband mit eindeutigen Komplementen.*

Der Beweis dieses Satzes ist außerordentlich aufwendig und nahm in seiner ersten Fassung 30 Seiten in Anspruch, allerdings ist dieser Beweis andererseits von elementarer Natur.

Die nachfolgenden Fakten werden deutlich machen, warum sich der oben erwähnte Irrglaube – oder sagen wir fairer diese Fehleinschätzung – so lange hat halten können und sie werden deutlich machen, warum der Satz von Dilworth so unzugänglich ist..

Insbesondere zeigt es sich, dass ein Verband mit eindeutigen Komplementen schon dann distributiv ist, wenn er *atomar* ist, d.h. jedes nicht minimale Element mindestens ein *Atom* enthält, ja isomorph ist zum Potenzmengenverband der Menge seiner Atome. Ferner werden wir sehen, dass ein Verband mit eindeutigen Komplementen schon dann distributiv ist, wenn er von endlicher *Breite* ist, d.h. die Länge seiner Antiketten nach oben beschränkt ist, und endlich, dass jeder modulare Verband mit eindeutigen Komplementen sogar distributiv ist.

Wir stellen die drei Beweise nacheinander vor. Noch einmal sei daran erinnert, dass es sich insbesondere jeweils um einen Beitrag zur Booleschen Algebra handelt.

4. 6. 2 Birkhoff und Ward. *Jeder atomare Verband $\mathfrak{V}$ mit eindeutigen Komplementen ist distributiv, ja mehr noch: lässt sich auffassen als Potenzmengenverband der Menge seiner Atome.*

BEWEIS. (1) Sei $x > y$. Dann existiert ein Atom p mit $p \leq x$ & $p \wedge y = 0$. Denn $x > y \Longrightarrow x \vee y' = 1$. Also kann $y' \wedge x$ nicht gleich 0 sein, da sonst y und $x \neq y$ zugleich Komplemente zu y wären. Folglich gilt $y' \wedge x > 0$. Daher existiert ein Atom $p \leq y' \wedge x$, also mit $p \leq x$ & $p \leq y'$, insbesondere also mit $p \leq x$ & $p \wedge y = 0$.

(2) Enthalten x und y die gleichen Atome, so sind sie gleich.

Klar, mit x und y enthält auch $x \wedge y$ die gemeinsamen Atome von x und y. Wir hätten also $x \wedge y < x$, und es enthielten $x \wedge y$ und y die gleichen Atome, mit Widerspruch zu (1).

(3) Das Komplement eines jeden Atoms ist ein Co-Atom.

Sei p ein Atom und $p' < x \leq 1$. Dann ist $p \vee x = 1$ und $p \wedge x = 0$ V $p \wedge x = p$. $p \wedge x = p$ bedeutet aber $p \leq x$, also $x = 1$, und $p \wedge x = 0$ liefert $x = p'$. Also ist p' ein Co-Atom.

(4) Sind p und q verschiedene Atome, so gilt $p \leq q'$.

Denn, im Falle $q \not\leq p'$ würde nach (3) gelten $p' \vee q = 1$ & $p' \wedge q = 0$, also $q = p'' = p$.

(5) Ist p ein Atom, so gilt $p \wedge x = 0 \Longleftrightarrow x \leq p'$.

Im Falle $p \wedge x = 0$ folgt $p \not\leq x$, also ist jedes prime q unterhalb von x verschieden von p. Folglich liegt nach (4) jedes prime q unter x auch unterhalb von $x \wedge p'$. Daher enthalten x und $x \wedge p'$ die gleichen Atome und sind somit nach (2) gleich. Das bedeutet dann $x \leq p'$.

(6) p ist genau dann ein Atom, wenn $p \leq x \vee y \Longrightarrow p \leq x$ V $p \leq y$ erfüllt ist.

Zunächst gilt $p \leq x$ oder nach (5) $x \leq p'$ und analog $p \leq y$ V $y \leq p'$. Es kann aber nicht $x, y \leq p'$ gelten, da dies $x \vee y \leq p'$ und damit $p \leq x \vee y \leq p'$ bedeuten würde.

Hiernach folgt mit (1) bis (6) geradeaus, dass die Abbildung $x \to \{p \,|\, p \leq x\}$ einen Isomorphismus von $\mathfrak{A}$ auf den Potenzmengenverband der Menge seiner Atome, betrachtet bezüglich $\cap, \cup, ^-$ darstellt. □

4. 6. 3 Proposition. *Jeder Verband $\mathfrak{V}$ mit eindeutigen Komplementen von endlicher Breite ist distributiv.*

BEWEIS. Wir zeigen, dass unter den gegebenen Umständen die *absteigende Kettenbedingung* gilt, $\mathfrak{A}$ also atomar ist.

Sei $x_1 > x_2 > x_3 > ...$ eine absteigende Kette. Dann ist wegen $x_i \vee {x_{i+1}}' = 1$ jedes $x_i \wedge {x_{i+1}}' \neq 0$, da ${x_{i+1}}'$ sonst zwei verschiedene Komplemente hätte. Wir definieren $y_i := x_i \wedge {x_{i+1}}'$. Dann folgt im Falle $j > i$ die Abschätzung $y_j \leq x_j \leq x_{i+1}$ und daher $x_i \wedge y_j \leq x_{i+1} \wedge {x_{i+1}}' = 0$.

Es würden also die y_i eine unendliche Antikette bilden, mit Widerspruch. □

4. 6. 4 J. von Neumann. *Jeder modulare Verband $\mathfrak{V}$ mit eindeutigen Komplementen ist distributiv.*

BEWEIS. Zunächst erhalten wir $a \wedge b = 0 \Longrightarrow a \leq b'$. Denn es gilt

$$\begin{array}{rll} & ((a \vee (a \vee b)') \vee b & = 1 \\ \& & ((a \vee (a \vee b)') \wedge b & = ((a \vee (a \vee b)') \wedge (a \vee b) \wedge b \\ & & = (a \vee ((a \vee b)' \wedge (a \vee b))) \wedge b \\ & & = (a \vee 0) \wedge b \\ & & = a \wedge b \\ & & = 0 \end{array}$$

und daher $b' = a \vee (a \vee b)' \geq a$.

Wir nehmen nun an, $\mathfrak{V}$ enthielte einen Diamanten mit u als Minimum, v als Maximum und den Elementen x, y, z als Atomen.

Dann folgt im Falle $u = 0$ zunächst $y \leq x' \;\&\; z \leq x'$ und damit der Widerspruch $x \leq v = y \vee z \leq x'$.

Daher muss $u \neq 0$ sein. Wir setzen $x^* := u' \wedge x$, $y^* := u' \wedge y$, $z^* := u' \wedge z$. Dann folgt

$$x^* \wedge y^* = y^* \wedge z^* = z^* \wedge x^* = 0 \,. \tag{4.54}$$

Hiernach betrachten wir $u \vee v'$ und erhalten

$$\begin{array}{rl} (u \vee v') \wedge (x^* \vee y^*) & = (u \vee v') \wedge v \wedge (x^* \vee y^*) \\ & = (u \vee (v' \wedge v)) \wedge (x^* \vee y^*) \\ & = u \wedge (x^* \vee y^*) \\ & \leq u \wedge u' \\ & = 0 \\ & \& \end{array}$$

$$\begin{aligned}(u \vee v') \vee (x^* \vee y^*) &= (u \vee v') \vee (u' \wedge x) \vee (u' \wedge y)\\ &= v' \vee u \vee (u' \wedge x) \vee u \vee (u' \wedge y)\\ &= v' \vee x \vee y \qquad\qquad (\mathrm{M})\\ &= 1 \qquad\quad (\text{beachte } x \vee y = v)\end{aligned}$$

Damit ist $x^* \vee y^*$ Komplement zu $u \vee v'$, und das bedeutet aus Gründen der Symmetrie

$$x^* \vee y^* = y^* \vee z^* = z^* \vee x^*. \tag{4.55}$$

Das führt uns dann zusammen mit (4.54) auf die Situation $u = 0$, siehe oben, zurück. □

4.7 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: $a \leq b \Longrightarrow xay \leq xby$. Ist dies erfüllt, so resultiert:

$$a \leq b \Longleftrightarrow a^{-1}ab^{-1} \leq a^{-1}bb^{-1} \Longleftrightarrow b^{-1} \leq a^{-1}. \tag{4.56}$$

Hieraus folgen weiter

$$x(a \wedge b)y = xay \wedge xby, \tag{4.57}$$

$$x(a \vee b)y = xay \vee xby, \tag{4.58}$$

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

$$(1 \wedge a)(1 \vee a) = 1 = (1 \vee a)(1 \wedge a) \tag{4.59}$$

vermöge

$$\begin{aligned}a \leq (1 \vee a) \wedge (a \vee a^2) &= (1 \vee a)(1 \wedge a)\\ &= (1 \wedge a) \vee (a \wedge a^2) \leq a.\end{aligned}$$

$$(a \wedge b)^{-1} = 1 = a^{-1} \vee b^{-1} \tag{4.60}$$

(4.61) $$(a \vee b)^{-1} = 1 = a^{-1} \wedge b^{-1}$$

wegen
$$\begin{array}{rcl} x \leq (a \vee b)^{-1} & \iff & x^{-1} \geq a \vee b \\ & \iff & x^{-1} \geq a \;\&\; x^{-1} \leq b \\ & \iff & x \leq a^{-1} \;\&\; x \leq b^{-1} \\ & \iff & x \leq a^{-1} \wedge b^{-1} \end{array}$$

und der hierzu dualen Herleitung.

(4.62) $$x = ab \;\&\; a \wedge b^{-1} = 1 \implies 1 \vee x = a \;\&\; 1 \wedge x = b\,,$$

denn die Prämisse führt wegen $a^{-1} \vee b = (a \wedge b^{-1})^{-1}$ zu

$$\begin{array}{rcl} 1 \vee x = 1 \vee ab = aa^{-1} \vee ab & = & a(a^{-1} \vee b) = a \\ \& \quad 1 \wedge x = 1 \wedge ab = b^{-1}b \wedge ab & = & (b^{-1} \wedge a)b = b\,. \end{array}$$

Als nächstes folgt:

(4.63) $$(1 \vee a) \wedge (1 \wedge a)^{-1} = 1,$$

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

Nun sind wir in der Lage, die Distributivität nachzuweisen:

(4.64) $$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

DENN:
$$\begin{array}{rcl} a \wedge (b \vee c) & = & (b \vee c)((b \vee c)^{-1}a \wedge 1) \\ & = & (b \vee c)((b^{-1} \wedge c^{-1})a \wedge 1) \\ & = & (b \vee c)(b^{-1}a \wedge c^{-1}a \wedge 1) \\ & = & (a \wedge bc^{-1}a \wedge b) \vee (cb^{-1}a \wedge a \wedge c) \\ & \leq & (a \wedge b) \vee (a \wedge c)\,. \end{array}$$ □

Zur Erinnerung: mit (4.64) gilt, wie schon gezeigt, auch

(4.65) $$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

Hiernach betrachten wir den *Kegel* P von $(G, \cdot, \vee, \wedge)$, das ist die Menge aller positiven Elemente, also $P := \{x \mid x \geq 1\}$. Wir erhalten sofort, dass P abgeschlossen ist bezüglich $\cdot, \vee, \wedge$, und man verifiziert leicht für die Operationen $*$ and $:$, definiert über

$$\begin{aligned} a * b := (a \wedge b)^{-1} \cdot b &= 1 \vee a^{-1}b \in P, \\ \text{und} \quad b : a := b \cdot (a \wedge b)^{-1} &= 1 \vee ba^{-1} \in P, \end{aligned}$$

$$\text{(A1)} \qquad a * ab = b$$

$$\text{(A2)} \qquad ba : a = b$$

$$\text{(A3)} \qquad a(a * b) = b(b * a)$$

$$\text{(A4)} \qquad (b : a)a = b(b * a)$$

$$\text{(A5)} \qquad ab * c = b * (a * c).$$

Auf der anderen Seite lässt sich zeigen, siehe [**?**], dass jede Algebra $(P, \cdot, *. :)$, die den Gesetzen (A1) bis (A5) genügt, als ein ℓ-Gruppen-Kegel betrachtet werden kann mit

$$\begin{aligned} a(a * b) = a \vee b = (b : a)a \\ \text{und} \quad b : (a * b) = a \vee b = (a : b) * a. \end{aligned}$$

Das soll in diesem Kapitel genügen.

Kapitel 5

Boolesches

5.1 Boolesche Strukturen

Der Begriff des Booleschen Verbandes wurde unter 4.2.8 erklärt. Über Boolesche Algebren existiert eine Flut an Literatur, mehr als verständlich, wenn man bedenkt, dass hier *Ringe, Gruppen, topologische Räume* und *Verbände* zusammenspielen. Unter anderem haben wir in [6] Boolesche Probleme in großer Breite bis hin zu den Schaltwerken betrachtet. Deshalb wollen wir uns hier auf einen engen Kern beschränken, wobei sich Überlappungen nicht ganz vermeiden lassen.

Beginne wollen wir mit der Auffassung des Booeleschen Verbandes als Ring. Hierzu vorweg eine Reduktion des Axiomensystems.

5. 1. 1 Proposition. *Eine Algebra* $\mathfrak{B} := (B, \wedge, \vee, ')$ *ist schon dann ein Boolescher Verband, wenn sie den Gleichungen genügt:*

(B11) $$a \wedge b = b \wedge a$$

(B12) $$a \vee b = b \vee a$$

(B21) $$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

(B22) $$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

(B31) $$a \wedge (b \vee b') = a$$

(B32) $$a \vee (b \wedge b') = a$$

BEWEIS. Wir beweisen zunächst die beiden Gleichungen:

$$a \wedge a' = b \wedge b' \tag{5.7}$$
$$a \vee a' = b \vee b'. \tag{5.8}$$

Wegen der $\wedge/\vee$ Dualität reicht es natürlich die Gleichung (5.7) 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:

$$a \wedge 0 = a \tag{5.9}$$
$$a \vee 1 = 1 \tag{5.10}$$

via

$$\begin{aligned} a \wedge 0 &= (a \wedge 0) \vee 0 \\ &= 0 \vee (a \wedge 0) \\ &= (a \wedge a') \vee (a \vee 0) \\ &= a \wedge (a' \vee 0) \\ &= a \wedge a' \\ &= 0 \end{aligned}$$

und die beiden *Verschmelzungsgesetze*

$$a \wedge (b \vee a) = a \tag{5.11}$$
$$a \wedge (b \vee a) = a \tag{5.12}$$

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 das Assoziativgesetz 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:

$$\begin{aligned} & ((a \wedge b) \wedge c) \vee (a \wedge (b \wedge c)) \\ = \; & ((a \wedge b) \vee (a \wedge (b \wedge c))) \wedge (c \vee (a \wedge (b \wedge c))) \\ = \; & (a \wedge (b \vee (b \wedge c))) \wedge ((c \vee a) \wedge (c \vee (b \wedge c) \\ = \; & (a \wedge b) \wedge ((c \vee a) \wedge c) \\ = \; & (a \wedge b) \wedge c \\ = \; & f(a, b, c) \\ = \; & f(c, b, a) \\ = \; & a \wedge (b \wedge c)\,, \end{aligned}$$

also in Formeln

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

Wir betonen noch einmal die Eindeutigkeit des Komplements, vgl. (COM), also $a'' = a$. Diese Regel liefert uns in Kombination mit den Distributivgesetzen

5. 1. 2 Die Regeln von de Morgan.

$$\begin{aligned} &(\mathrm{V}\wedge) && (a \wedge b)' &&= a' \vee b' \\ &(\mathrm{V}\vee) && (a \vee b)' &&= a' \wedge b' \end{aligned}$$

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 Regeln (5.9), (5.10) 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:

5. 1. 3 Proposition. *Setzen wir in einem Booleschen Verband* $(V, \wedge, \vee, ')$

$$a \oplus b := (a \wedge b') \vee (b \wedge a') \tag{5.17}$$

$$a \odot b := a \wedge b, \tag{5.18}$$

so bildet V *bezüglich dieser beiden Operationen einen* idempotenten *Ring* $\mathfrak{R}(V)$*, und es bildet umgekehrt jeder idempotente Ring* $(R, +, \cdot, 1)$ *bezüglich*

$$a \wedge b := a \cdot b \tag{5.19}$$

$$a \vee b := a + ab + b \tag{5.20}$$

$$a' := a + 1 \tag{5.21}$$

einen Booleschen Verband $\mathfrak{V}(R)$*. Darüber hinaus erfüllen die beiden hier vorgestellten Operatoren die* Galoisbedingung:

$$\mathfrak{V}(\mathfrak{R}(V) = \mathfrak{V} \quad \& \quad \mathfrak{R}(\mathfrak{V}(R) = \mathfrak{R} \tag{5.22}$$

BEWEIS. Der Leser ermittelt geradeaus:

$$a \odot b = b \odot a \tag{R11}$$

$$(a \odot b) \odot c = a \odot (b \odot c) \tag{R12}$$

$$a \odot a = a \tag{R13}$$

$$a \odot 1 = a \tag{R14}$$

$$a \oplus b = b \oplus a \tag{R21}$$

$$a \oplus a = 0 \tag{R22}$$

$$a \oplus 0 = a \tag{R22}$$

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
$$\begin{aligned}
a \odot (b \oplus c) &= a \wedge ((b \wedge c') \vee (c \wedge b')) \\
&= (a \wedge b \wedge c') \vee (a \wedge c \wedge b') \\
&= \vee(a \wedge b \wedge c') \vee 0 \vee (a \wedge c \wedge b') \\
&= \Big(a \wedge b \wedge a'\Big) \vee \Big(a \wedge b \wedge c'\Big) \vee \Big(a \wedge c \wedge a'\Big) \vee \Big(a \wedge c \wedge b'\Big) \\
&= \Big((a \wedge b) \wedge (a' \vee c')\Big) \vee \Big((a \wedge c) \wedge (a' \vee b')\Big) \\
&= \Big((a \wedge b) \wedge (a \wedge c)'\Big) \vee \Big((a \wedge c) \wedge (a \wedge b)'\Big) \\
&= (a \wedge b) \oplus (a \wedge c) \\
&= (a \odot b) \oplus (a \odot c)\,.
\end{aligned}$$

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

$$ab = ba \tag{5.32}$$

resultiert. Der Rest darf dem Leser als Übung überlassen bleiben.

Zu verifizieren bleibt (4.43). Betrachten wir also die Operatoren $\mathfrak{V}$ und $\mathfrak{R}$. Hier haben wir zunächst $ab = a \wedge b = a \odot b$ und $a' = a + 1$, denn man beachte $a' \oplus a = 0 \rightsquigarrow a' = a + 1$. Und dies impliziert weiter:

$$\begin{aligned} a + b &= ab + a + ab + ab + ab + ab + ba + b \\ &= a(b+1) + a(b+1) \cdot b(a+1) + b(a+1) \\ &= (a \wedge b') \vee (b \wedge a') \\ &= a \oplus b\,. \end{aligned}$$

□

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.

Deshalb sei betont, dass mit einem Booleschen Ring im folgenden stets ein idempotenter Ring mit 1 gemeint sein wird.

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.

5.2 Boolesche Polynome

Wir kehren zurück zur Booleschen Algebra und wenden uns nun einem Aspekt zu, der von außerordentlicher wissenschaftsdidaktischer Bedeutung ist. Da wir den Booleschen Verband bereits als Ring erkannt haben, ist klar, was wir unter einem *booleschen Polynom* verstehen. Ein Beispiel wäre etwa das Polynom $f(x_1, x_2, x_3) := (x_1 \vee (x_2' \wedge x_3))' + x_1 x_3$. Durch Umschreiben würden wir zu einem Ring-Polynom gelangen. Doch auch intuitiv ist der Begriff des booleschen Polynoms natürlich klar. Damit ist dann auch die boolesche Gleichung begrifflich geklärt. Gemeint ist natürlich mit

$$p(x_1, \ldots, x_m) = q(x_1, \ldots, x_n)\,,$$

dass die linke und die rechte Seite bei jeder *Belegung* mit Elementen einer booleschen Algebra, insbesondere also bei jeder $0,1$-Belegung den gleichen Wert liefern.

Die Frage, ob ein Verfahren existiert, das in endlich vielen Schritten klärt, ob zwei Polynome in dem Sinne äquivalent sind, dass sie stets den gleichen Wert liefern, nennt man das *Wortproblem* – hier der booleschen Algebra. Boolesch äquivalent wären beispielsweise $x \wedge x$ und $x \vee x$ oder auch $x \oplus x$ und $y \oplus y$ oder auch x^2 und x. Im Falle $x \oplus x = y \oplus y$ Haben wir den Sonderfall, dass auf der linken Seite lediglich die Variable x auf der rechten lediglich die Variable y auftritt. Dies ist aber nur dem Anschein nach eine Abweichung. Denn wir können ja stets eine neue Variable z hinzunehmen, indem wir ein vorgegebenes Polynom mit $z \vee z'$ multiplizieren. Das führte im obigen Fall etwa zu

$$p(x,y) := (y \vee y')(x \oplus x) = (x \vee x')(y \oplus y) =: q(x,y)\,.$$

Das Überraschende ist nun, dass es einen schlichten *Algorithmus* gibt, mit dessen Hilfe wir die Gleichwertigkeit zweier Polynome schematisch – weil algorithmisch – herleiten können.

MAN BEACHTE: $p(x_1,\ldots,x_n) = q(y_1,\ldots y_m)$ ist genau dann gegeben, wenn $p \oplus q = 0$ erfüllt ist. Es ist $p \oplus q$ ein boolesches Polynom, dass wir zunächst einmal durch Auflösen aller $'$-Klammern, also durch Anwendung von de Morgan überführen können in ein Polynom, in dem nur die Variablen – nicht aber Klammern – „gestrichen" auftreten. Hiernach symbolisieren wir in Gedanken $\wedge$ durch $\cdot$ und $\wedge$ durch $\times$. Dann wird sofort klar, dass Auflösung aller $\times$-Klammern gemäß der wohl vertrauten Schulalgebra zu einem $\times$-Ausdruck von Produkten führt, unser $p \oplus q$ sich also darstellen lässt als eine Vereinigung von Schnitten. Ein solcher Ausdruck liefert aber genau dann stets den Wert 0, wenn jede Komponente stets den Wert 0 liefert, und das ist genau dann der Fall, wenn in jedem der vorkommenden Schnitte wenigstens eine Variable sowohl gestrichen als auch ungestrichen auftritt.

Diese Einsicht liefert ein Doppeltes:

Zum einen haben wir ein Verfahren an der Hand, in endlich vielen Schritten die Gleichwertigkeit zweier Polynome zu überprüfen, zum anderen ist aber noch etwas mehr – und zwar etwas Entscheidendes – hinzugekommen, nämlich:

Vereinbaren wir die Redeweise, es verschwinde ein boolesches Polynom identisch, wenn es über allen booleschen Algebren $\mathfrak{B}$ den Wert 0 annimmt, so gilt:

5. 2. 1 Das Reduktionstheorem. *Ein boolesches Polynom verschwindet identisch gdw. es über* $\mathfrak{Z}_2$ *verschwindet.*

Insbesondere liefert der soeben formulierte Satz zusätzlich ein sehr praktisches *Entscheidungsverfahren.* Wir notieren in den *Zeilen einer Tafel* alle $0, 1$-Kombinationen der Länge n und vergleichen die *Ergebnis-Spalten.*

5. 2. 2 Beispiel. Sei $f := a \wedge (b \vee c')$ und $g := (a \wedge b) \vee c'$. Dann notieren wir:

a	b	c	f	g
O	O	O	O	I
O	O	I	O	O
O	I	O	O	I
O	I	I	O	O
I	O	O	I	I
I	O	I	I	O
I	I	O	I	I
I	I	I	I	I

woraus $f \neq g$ resultiert. Hätten wir hingegen zweimal die gleiche Ergebnisspalte erhalten, so hätte dies trotz der Einengung auf Nullen und Einsen die allgemeine Identität der beiden Polynome bedeutet.

Das soeben betrachtete *Tafel-Verfahren* liefert als ein weiteres zunächst überraschendes Ergebnis:

5. 2. 3 Proposition. *Ist f irgendeine n-stellige* $\mathsf{0}, \mathsf{I}$*-Funktion, so lässt sich f als boolesche Funktion darstellen.*

BEWEIS. Wir be(tr)achten diejenigen Tafelzeilen, in denen f dem eingetragenen $\mathsf{0}, \mathsf{I}$-n-tupel $m_{i,1}, \ldots m_{i,n}$ den Wert I zuordnet, und ersetzen in $x_1 \wedge x_2 \wedge \ldots \wedge x_n$ diejenigen Variablen x_k $(1 \leq k \leq n)$ durch ${x_k}'$, deren $m_{i,k} = 0$ ist.

Dann liefert die *Disjunktion* dieser *Konjunktionen* unsere Behauptung. □

Dies sei erläutert an den obigen Beispielen: Im Falle f bilden wir zunächst

$$(a \wedge b' \wedge c') \ , \ (a \wedge b' \wedge c) \ , \ (a \wedge b \wedge c') \ , \ (a \wedge b \wedge c)$$

und hiernach

$$F := (a \wedge b' \wedge c') \vee (a \wedge b' \wedge c) \vee (a \wedge b \wedge c') \vee (a \wedge b \wedge c)$$

und im Falle g bilden wir zunächst

$$(a \wedge b' \wedge c') \ , \ (a' \wedge b \wedge c') \ , \ (a \wedge b \wedge c') \ , \ (a \wedge b \wedge c') \ , \ (a \wedge b \wedge c)$$

und hiernach

$$G := (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (a \wedge b \wedge c') \vee (a \wedge b \wedge c) \, .$$

Das bedeutet insbesondere, dass die 16 möglichen verschiedenen Operationen auf der Menge $\{0, 1\}$ sich ausnahmslos darstellen lassen als *boolesche Normalform.*

FRAGE: Benötigen wir wirklich alle drei Operationen $\wedge, \vee, '$? Hier wird sofort klar, dass wir auf $\vee$ verzichten können, da nach de Morgan $a \vee b = (a' \wedge b')'$ erfüllt ist. Doch es gilt noch mehr. Und zwar lassen sich alle Operationen mittels der Operation NAND darstellen, die wir hier mittels ∇ symbolisieren wollen und die definiert ist über $a \nabla b := (a \wedge b)'$. Wir sehen sofort $a' = a \nabla a$ und damit $a \wedge b = (a \nabla b) \nabla (a \nabla b)$. Dies ist, wie in [6] aufgezeigt, von Bedeutung für den Entwurf von Schaltungen.

Wie wir sahen, lässt sich die Zahl der definierenden Gleichungen der booleschen Algebra reduzieren. So konnten wir u. a . das Assoziativgesetz „umgehen". Die Frage stellt sich nach einem möglichst knappem Axiomensystem, exakter nach einem Axiomensystem von möglichst wenig Gleichungen.

Wie wir bereits wissen, lässt sich der Verband mit einer einzigen Gleichung beschreiben, der distributive Verband hingegen nicht. Doch wie steht es mit der booleschen Algebra? Hier haben wir wieder mehr Glück. Tatsächlich lässt sich die boolesche Algebra mit einer einzigen Gleichung beschreiben. Das sei hier jedoch nicht ausgeführt, sondern dem Leser überlassen. Er studiere die Gleichung:

(BR) $$((x+y)+z)+((x+z)+h(t,u,v,w))=y$$

mit

$$h(t,u,v,w) := ((tt+t(u(vw)+w(uv)))+t)+(u(v+w)+(uv+wu))$$

ODER ABER

ER GLAUBE !

Kapitel 6

McKenzie's celebrated Theorem

In diesem Abschnitt soll ein Theorem vorgestellt werden, der in einmaliger Weise demonstriert, dass auch heute noch tief liegende zentrale Resultate mit elementaren Methoden und schlichten Ideen erschlossen werden können, sofern nur diese schlichten Ideen und elementaren Methoden mit genialem Blick fruchtbar gekoppelt werden.

Die Rede ist von einem Satz von R. McKenzie, der besagt, dass sich der Verband mit einer einzigen Gleichung beschreiben lässt.

Betrachten wir etwa das Gruppoid $(G, *)$ mit der definierenden Gleichung $a * b = b$, so sehen wir sofort, dass das Wortproblem degeneriert zu einem „Schau-nach-rechts-problem".

Betrachten wir etwa die kommutative Halbgruppe $(H, \cdot)$, so ist diese definiert durch die beiden Gleichungen

$$\begin{aligned} a \cdot (b \cdot c) &= (a \cdot b) \cdot c \\ a \cdot b &= b \cdot a \end{aligned}$$

Leicht lässt sich hier erkennen, dass eine Beschreibung der abelschen Halbgruppe mittels einer einzigen Gleichung nicht möglich ist. Denn eine solche Gleichung hätte die Form

$$f(x_1, x_2, \ldots, x_n) = y\,.$$

Dabei muss die Variable rechts außen verschieden sein von y, da die Gleichung sonst auch von der Rechts-zero-Halbgruppe erfüllt würde. Wäre nun das Kommutativgesetz herleitbar, so könnten wir jede Variable nach rechts

bringen. Das lieferte dann $(g(x_1, \ldots, x_n)) \cdot y = y \cdot (g(x_1, \ldots, x_n))$ für ein geeignetes g. Also besäße jede a ein *privates Eins-Element.*

Das aber kann nicht sein, man betrachte **N** ohne 0 bezüglich der Addition.

Anders verhält es sich etwa mit der Gruppe, sie lässt sich in der Tat durch eine einzige Gleichung charakterisieren – wie A. Tarski in [36] als erster für den kommutativen Fall und G. Higman und B. H. Neumann in [**?**] für den allgemeinen Fall gezeigt haben.

Doch nun zum Verband. Hier gilt – überraschenderweise

6. 0. 4 McKenzie. The theory of lattices is one-based – but – no further variety of lattices is one-based, too.

Der Beweis läuft über vier Phasen, wobei wir als interessante Zwischenresultate erhalten:

(a) Ein Absorptionssystem,

(b) Ein Injektionssystem,

(c) Eine Fundamentalgleichung,

(d) Die 2-Basigkeit aller echten Untervarietäten.

6.1 Ein Absorptionssystem

Der erste Schritt auf dem Wege zum Beweis wird die Entwicklung eines charakteristischen Axiomensystems sein, das aus lauter *Absorptionsgleichungen,* d.h. aus Gleichungen der Form

$$f(x, x_1, \ldots, x_n) = x$$

besteht, wobei f eine *rationale Verbandsfunktion* darstellt. Dabei nehmen wir den Begriff der rationalen Verbandsfunktion naiv hin, der Leser möge sich Verbandsrechenausdrücke in $x, x_1, \ldots, x_n$ vorstellen. Ein Weg könnt sein, klassische rationale Polynome durch Austausch von $\cdot$ gegen $\wedge$ und von $+$ gegen $\vee$ zu betrachten. Beispiele wären:

$$\begin{aligned} f(x, y) &:= x \wedge y \\ g(x, y) &:= x \vee (x \wedge y) \\ h(x, y, z) &:= (x \vee ((x \wedge y) \wedge (x \vee z)) \end{aligned}$$

Man erkennt, dass aufgrund des Verbandsrechnens g und h Absorptionsfunktionen darstellen, f hingegen nicht.

Unmittelbar evident ist, dass mit

$$\begin{aligned} f(x, x_1, \ldots, x_n) &= x \\ g(x, y_1, \ldots, y_m) &= x \end{aligned}$$

auch

$$f(g(x, y_1, \ldots, y_m), x_1, \ldots, x_n) = x$$

erfüllt ist. Es ist ja lediglich in f die Variable x an allen Stellen durch $g(x, y_1, \ldots, y_m)$ ersetzt.

Die Bedeutung von Absorptionsgleichungen für die 1-basige Grundlegung des Verbandes lässt sich leicht einsehen:

Unmöglich kann man den Verband mit einer (einzigen) Gleichung beschreiben, die die Absorptionseigenschaft nicht besitzt. Denn jede *Nichtabsorptionsgleichung* in einem Verband gilt auch in $\mathbf{Z}$, wenn man die Operationen $\wedge$ und $\vee$ vermöge

$$\begin{aligned} a \wedge b &:= 0 \\ a \vee b &:= 0 \end{aligned}$$

erklärt, insofern jede Belegung auf der linken wie auf der rechten Seite einer Nichtabsorptionsgleichung zum Ergebnis 0 führt.

Keineswegs aber bildet $\mathbf{Z}$ bezüglich $\wedge$ und $\vee$ im oben definierten Sinn einen Verband. Denn es gilt beispielsweise $1 \vee 1 = 0 \neq 1$.

Da nun einerseits eine für den Verband charakteristische Gleichung zwangsläufig eine Absorptionsgleichung ist und sich andererseits Absorptionsgleichungen zu neuen Absorptionsgleichungen schachteln lassen, liegt der Ansatz nahe, zunächst ein Absorptionssystem zu entwickeln, um hiernach durch Schachtelung zu einer Fundamentalgleichung zu gelangen. Als ein selbstduales Absorptionssystem erweist sich hier nach McKenzie:

6. 1. 1 Proposition. $(V, \wedge, \vee)$ *ist genau dann ein Verband, wenn die folgenden 4 – offenbar in jedem Verband gültigen – Absorptionsgleichungen gelten:*

(A11) $$x \wedge ((y \vee x) \vee z) = x$$

$$x \vee ((y \wedge x) \wedge z) = x \tag{A12}$$

$$((y \vee x) \wedge (z \vee x)) \wedge x = x \tag{A21}$$

$$((y \wedge x) \vee (z \wedge x)) \vee x = x\,. \tag{A22}$$

Wir beobachten zunächst, dass (A11) und (A12) sowie (A21) und (A22) durch Umpolung auseinander hervorgehen, also zueinander dual sind. Sodann zeigen wir:

$$x \vee y = y \vee x \tag{V1}$$

$$x \vee (y \vee z) = (x \vee y) \vee z \tag{V2}$$

$$x \vee (x \wedge y) = x \tag{V3}$$

Hierzu beachten wir zunächst, dass aus (A11) bis (A22) unmittelbar bezüglich $\wedge$ und $\vee$ jeweils die Existenz einer *privaten Rechts-* und *einer privaten Links-eins* resultiert, d. h. es gibt zu jedem x ein (u_x, v_x, r_x, s_x) mit

$$u_x \vee x = x \tag{6.8}$$

$$x \vee v_x = x \tag{6.9}$$

$$r_x \wedge x = x \tag{6.10}$$

$$x \wedge s_x = x \tag{6.11}$$

Denn man definiere mit beliebigen y, z

$$u_x := (y \wedge x) \vee (z \wedge x) \tag{6.12}$$

$$v_x := (y \wedge x) \wedge z \tag{6.13}$$

$$r_x := (y \vee x) \wedge (z \vee x) \tag{6.14}$$

$$s_x := (y \vee x) \vee z\,. \tag{6.15}$$

Dann folgen, was der Leser überprüfen möge, die beiden Gleichungen:

$$x \vee (x \wedge z) = x \vee ((r_x \wedge x) \wedge z) \overset{(A12)}{=} x \tag{6.16}$$

$$x \vee (y \wedge x) = x \vee ((y \wedge x) \wedge s_{y \wedge x}) = x \tag{6.17}$$

und somit (durch Umpolung) auch die beiden Gleichungen:

$$x \wedge (x \vee z) = x \tag{6.18}$$

$$x \wedge (y \vee x) = x \tag{6.19}$$

Insbesondere haben wir mit (6.16) die Gleichung (V3) gewonnen. Als nächstes folgt die Gleichung (V1) vermöge:

$$\begin{aligned} x \vee y &\overset{(6.17)}{=} (x \vee y) \vee ((y \vee x) \wedge (x \vee y)) \\ &\overset{(A22)}{=} (x \vee y) \vee ((y \vee x) \wedge (((y \wedge (x \vee y)) \\ &\quad \vee (x \wedge (x \vee y))) \vee (x \vee y))) \\ &= (x \vee y) \vee ((y \vee x) \wedge ((y \vee x) \vee (x \vee y))) \\ &= (x \vee y) \vee (y \vee x) \\ &= ((x \wedge (y \vee x)) \vee (y \wedge (y \vee x))) \vee (y \vee x) \\ &= y \vee x \end{aligned}$$

und dies liefert aus Gründen der Dualität weiter:

$$x \wedge y = y \wedge x\,. \tag{6.20}$$

Schließlich gewinnen wir

$$x \vee (y \vee z) = (x \vee y) \vee z \tag{6.21}$$

denn, mittels (A22) bzw. (A11) und (0.4) folgt

$$\begin{aligned} &(x \vee y) \vee z \\ &\overset{(A22)}{=} ((y \wedge ((x \vee y) \vee z)) \vee (z \wedge ((x \vee y) \vee z))) \vee ((x \vee y) \vee z) \\ &= (y \vee z) \vee ((x \vee y) \vee z) \end{aligned} \tag{6.22}$$

und wenden wir diese Gleichung wiederholt an, so erhalten wir:

$$\begin{aligned} (x \vee y) \vee z &= (z \vee (x \vee y)) \vee (y \vee z) \\ &= ((x \vee y) \vee (y \vee z)) \vee ((z \vee (x \vee y)) \vee (y \vee z)) \\ &= ((x \vee y) \vee (y \vee z)) \vee (z \vee (x \vee y)) \\ &= (z \vee (x \vee y)) \vee ((y \vee z) \vee (x \vee y)) \\ &= (y \vee z) \vee (x \vee y)\,, \end{aligned}$$

Es ist aber – wegen der Kommutativität – die letzte Zeile symmetrisch in x, z, weshalb sich auch der Wert von $(x \vee y) \vee z$ nicht ändert, wenn wir x und z miteinander vertauschen. Daher gilt

$$(x \vee y) \vee z = (z \vee y) \vee x = x \vee (y \vee z)\,. \tag{6.23}$$

6.2 Ein Injektionssystem

Nach der Absorptions-Charakterisierung im letzten Paragraphen geben wir in diesem Abschnitt eine Injektionscharakterisierung.

Wir zeigen:

6. 2. 1 Proposition. *$(V, \wedge, \vee)$ ist genau dann ein Verband, wenn die nachfolgenden 2- bzw. 3-stelligen Funktionen f_1 bis f_{10} von den $x_v (1 \leq \nu \leq 12)$ unabhängig und f_1 bis f_8 injektiv sind, d. h., $a \neq b \Longrightarrow f_\nu(a, x_\nu) \neq f_\nu(b, x_\nu)$ erfüllen.*

$$
\begin{aligned}
f_1\ (x, x_1) &:= (x_1 \wedge x) \vee (x \wedge x) \\
f_2\ (x, x_2) &:= ((x \vee x) \wedge x_2) \vee (x \wedge x) \\
f_3\ (x, x_3) &:= ((x \vee x) \wedge (x \vee x)) \vee (x_3 \wedge x) \\
f_4\ (x, x_4) &:= ((x \vee x) \wedge (x \vee x)) \vee ((x \vee x) \wedge x_4) \\
f_5\ (x, x_5) &:= (x_5 \vee x) \wedge (x \vee x) \\
f_6\ (x, x_6) &:= ((x \wedge x) \vee x_6) \wedge (x \vee x) \\
f_7\ (x, x_7) &:= ((x \wedge x) \vee (x \wedge x)) \wedge (x_7 \vee x) \\
f_8\ (x, x_8) &:= ((x \wedge x) \vee (x \wedge x)) \wedge ((x \wedge x) \vee x_8) \\
f_9\ (x, x_9, x_{11}) &:= ((x_9 \wedge x) \vee (x_{11} \wedge x)) \vee x \\
f_{10}(x, x_{10}, x_{12}) &:= ((x_{10} \vee x) \wedge (x_{12} \vee x)) \wedge x
\end{aligned}
$$

BEWEIS. Offenbar sind f_1 bis f_{10} Absorptionsfunktionen, der Leser möge dies bestätigen, und somit injektiv und von $x_1, \ldots, x_{12}$ unabhängig. Damit ist die Bedingung des Satzes notwendig. Sie ist aber auch hinreichend:

Da für $1 \leq \nu \leq 8$ der Funktionswert der f_ν von x_ν nicht abhängt, gilt:

$$
\begin{aligned}
f_1(x, x_1) &= f_1(x, x \vee x) \\
&= f_2(x, x) \\
&= f_2(x, x_2) \\
&= f_2(x, x \vee x) \\
&= f_3(x, x) \\
&= f_3(x, x_2) \\
&= f_3(x, x \vee x) \\
&= f_4(x, x)
\end{aligned}
$$

$$\begin{aligned} &= f_4(x, x \vee x) \\ &= f_1(x \vee x, x \vee x) \\ &= f_1(x \vee x, x_1) \end{aligned}$$

also $$f_1(x, x_1) = f_1(x \vee x, x_1)$$

und damit wegen der Injektivität von $f(x, x_1)$ und aus Gründen der Dualität die Gleichungen

$$x \vee x = x \tag{6.24}$$

$$x \wedge x = x \tag{6.25}$$

Somit ergeben sich mittels

$$\begin{aligned} f_\nu(x, x) &= x \quad (1 \leq \nu \leq 8) \\ \& \quad f_\nu(x, x, x) &= x \quad (9 \leq \nu \leq 10) \end{aligned}$$

die paarweise dualen Absorptionsgleichungen:

$$(x_1 \wedge x) \vee x = x \wedge (x_5 \vee x) \wedge x = x \tag{6.26}$$

$$(x \wedge x_2) \vee x = x \wedge (x \vee x_6) \wedge x = x \tag{6.27}$$

$$x \vee (x_3 \wedge x) = x \wedge x \wedge (x_7 \vee x) = x \tag{6.28}$$

$$x \vee (x \wedge x_4) = x \wedge x \wedge (x \vee x_8) = x \tag{6.29}$$

&

$$((x_9 \wedge x) \vee (x_{11} \wedge x)) \vee x = x \tag{6.30}$$

$$((x_{10} \vee x) \wedge (x_{12} \vee x)) \wedge x = x \tag{6.31}$$

Mittels dieser Gleichungen wurden aber in Satz 1 die Verbandsgleichungen hergeleitet, womit unsere Behauptung bewiesen ist. □

6.3 Eine Fundamentalgleichung

6. 3. 1 Lemma. *Sind f und g Funktionen von M und ist $f \circ g \circ f$ eine Permutation von M, also eine bijektive Selbstabbildung von M, so sind auch f und g Permutationen von M.*

BEWEIS. Zunächst ist f injektiv wegen

$$\begin{aligned} f(a_1) = f(a_2) &\implies f(g(f(a_1))) = f \circ g(f(a_2)) \\ &\implies f \circ g \circ f(a_1) = f \circ g \circ f(a_2)\ , \\ &\implies a_1 = a_2\ , \quad \text{da} \quad f \circ g \circ f \ \text{ bijektiv ist}\ . \end{aligned}$$

Es ist f aber auch surjektiv, denn ist a aus M, so existiert wegen der Surjektivität von $f \circ g \circ f$ ein u in M mit $f \circ g \circ f(u) = a$, also mit $f(g(f(u))) = a$, so dass mit $b := g(f(u)) \in M$ die Gleichheit $f(b) = a$ erfüllt ist. Folglich ist f eine Permutation. Dann ist aber auch

$$g = f^{-1} \circ f \circ g \circ f \circ f^{-1}$$

eine Permutation von M. □

Als unmittelbare Folge des letzten Lemmas erhalten wir natürlich, dass mit

$$f_1 \circ f_2 \circ \ldots \circ f_{n-1} \circ f_n \circ f_{n-1} \circ \ldots \circ f_2 \circ f_1$$

auch die $f_1, \ldots, f_n$ Permutationen sind.

Hiernach gelingt die Konstruktion der angekündigten Fundamentalgleichung. Dabei gehen wir aus von den Funktionen $f_1, \ldots, f_{10}$ und bilden die Terme

$$\begin{gathered} f_1\ (x\,,\, y_1) \\ \vdots \\ f_{10}\,(x\,,\, y_{10}\,,\, y_{12}) \end{gathered}$$

Natürlich stellen etwa $f_1(x, x_1)$ und $f(x, y_1)$ die gleiche Funktion dar, lassen wir diese beiden Terme aber in eine Gleichung eingehen, etwa in

$$f_1(x, x_1) \vee f_1(x, y_1) = x$$

so kann man die Variablen x_1, y_1 unterschiedlich belegen, was bedeutet, dass sich der Spielraum durch „Trennung" der Variablen erweitert. Dies ist im Falle der McKenzie-Konstruktion entscheidend. Wir wählen im folgenden als Symbol für den Funktionsterm $f_\nu\,(x, x_1, \ldots, x_n)$ das Zeichen $f_{\nu x}$. Dann wäre beispielsweise f_{1x} ein Symbol für $f_1(x, x_1)$, f_{1y} eines für $f_1(x, y_1)$. Wir vereinbaren weiter $f_{\nu x} \circ f_{\kappa y}$ als Symbol desjenigen Terms, der entsteht, wenn man in $f_{\nu x}$ die Variable x durch den Term $f_\kappa(x, y_1, \ldots, y_n)$ ersetzt.

Dann ist

$$f_{1y} \circ f_{2y} \ldots \circ f_{9y} \circ f_{10y} \circ f_{9x} \ldots \circ f_{2x} \circ f_{1x}$$

erklärt und wir können die Gleichung

$$\mathbf{F}: \qquad f_{1y} \circ \ldots \circ f_{9y} \circ f_{10x} \circ f_{9x} \ldots \circ f_{1x} = x$$

bilden.

Dabei ist die linke Seite eine Funktion in $x, x_1, \ldots, x_{12}, y_1, \ldots, y_{12}$, die rechte hingegen eine Funktion in x. Hieraus ergibt sich unmittelbar, dass die linke Seite nicht abhängt von den indizierten Variablen $x_1, \ldots, x_{12}, y_1, \ldots, y_{12}$. Es ergibt sich aber noch mehr. Belegen wir nämlich die Variablen $x_1, \ldots, x_{12}$ und $y_1, \ldots, y_{12}$ paarweise mit den gleichen Konstanten $a_1, \ldots, a_{12}$ eines Verbandes $(V, \wedge, \vee)$ so gehen die $f_{\nu x}$ bzw. $f_{\nu y}$ über in Funktionsterme $f_\nu(x, a_\nu) =: f_{\nu a}$ so dass die linke Seite unserer Gleichung übergeht in

$$f_{1a} \circ \ldots \circ f_{9a} \circ f_{10a} \circ f_{9a} \circ \ldots \circ f_{1a} = \text{ id}$$

und damit, da id, also auch die linke Seite eine Permutation darstellt, dass alle $f_{\nu a}$ Permutationen sind. Insbesondere heißt dies:

$$f_\nu(u, a_\nu) = f_\nu(v, a_\nu) \Longrightarrow u = v \quad (1 \leq \nu \leq 8)$$

(2) Sind für ein festes ν^* die Belegungen der indizierten Variablen voneinander verschieden, für die übrigen jedoch gleich, so folgt:

$$\begin{aligned} & f_{1a} \circ \ldots \circ f_{\nu^* a} \circ \ldots \circ f_{9a} \circ f_{10a} \circ f_{9a} \circ \ldots \circ f_{1a} \\ = \; & f_{1a} \circ \ldots \circ f_{\nu^* b} \circ \ldots \circ f_{9a} \circ f_{10a} \circ f_{9a} \circ \ldots \circ f_{1a} \end{aligned}$$

was *via* Rechts- und Linkskürzung zu $f_{\nu^* a} = f_{\nu^* b}$ führt. Dies besagt in Worten aber nichts anderes, als dass die Funktionen f_ν $(1 \leq \nu \leq 10)$ von den indizierten Variablen unabhängig sind und somit zunächst $x \wedge x = x = x \vee x$ folgt, woraus dann weiter die Gleichungen (A11), (A12), (A21), (A22) resultieren.

Damit ist aus F die Voraussetzung von Proposition 6.1.1 hergeleitet, weshalb die Fundamentalgleichung **F** die Klasse der Verbände charakterisiert.

6.4 Genau zwei Verbands-Varietäten sind 1-basig

Es stellt sich natürlich die Frage, ob sich neben der Klasse aller Verbände, auch spezielle Verbandsklassen wie die der modularen oder der distributiven

Verbände durch eine einzige Gleichung charakterisieren lassen. Auch diese Frage wurde von McKenzie beantwortet und zwar negativ.

Wir erkennen zunächst, dass eine Funktion in 2 Variablen, die in irgendeiner Verbandsklasse „absorbiert" schon in jedem Verband absorbiert.

Denn, sei $f(x_1, x_2, ..., x_n) =: f$ ein Polynom in n Variablen, die in diesem Polynom jeweils exakt einmal auftreten. Sei weiter $\overline{f}$ ein Polynom, das aus f dadurch hervorgeht, dass man die vorgegebenen Variablen eventuell durch neue, nicht notwendig paarweise verschiedene Variablen ersetzt. Dann sagen wir $\overline{f}$ – also auch f – habe die Länge n.

Sei hiernach $f(x, y)$ ein Polynom der Länge $n \geq 5$. Dann lässt sich $f(x, y)$ in zwei Polynome f_1, f_2 kürzerer Länge zerlegen. Wir wählen dasjenige größerer Länge, o.B.d.A. f_1. Hiernach verfahren wire mit f_1 wie zuvor mit f und setzen das Verfahren fort bis wir zwangsläufig bei einem f_k der Länge 3 oder 4 ankommen. Dies liefert dann aber in jedem Verband $x, y, x \wedge y$ oder $x \vee y$ in jedem Falle also ein Unterpolynom von $f(x, y)$ von kürzerer Länge als der Länge von f_k.

Das bedeutet: jedes Absorptions-Polynom einer Länge ≤ 5 einer speziellen Verbandsklasse lässt sich in jedem Verband herleiten, und lässt sich jedes Absorptions-Polynom von der Länge $k \geq 5$ schon in jedem Verband herleiten, so auch jedes Absorptions-Polynom der Länge $k + 1$.

Hieraus folgt dann weiter, dass auch jede Funktion in mehr als zwei Variablen höchstens dann in einer speziellen Verbandsklasse absorbiert, wenn sie in jedem Verband absorbiert. Denn gelte in einer speziellen Verbandsklasse

$$f(x, x_1, \ldots, x_n) = x$$

Dann resultieren in dieser speziellen Verbandsklasse für

$$d := x_1 \wedge x_2 \ldots \wedge x_n \quad \& \quad v := x_1 \vee x_2 \ldots \vee x_n$$

die Gleichungen

$$x = f(x, d, \ldots, d) \quad \& \quad f(x, v, \ldots, v) = x\,.$$

Diese Gleichungen sind aber solche in 2 Variablen und gelten somit in jedem Verband, woraus nach den Regeln des Verbandsrechnens resultiert:

$$x = f(x, d, \ldots, d) \leq f(x, x_1, \ldots, x_n) \leq f(x, v, \ldots, v) = x$$

also auch

$$f(x, x_1, \ldots, x_n) = x\,.$$

Bleibt der Fall einer Funktion in einer Variablen zu betrachten. Sie ist zwangsläufig in jedem Verband gleich x und liefert uns zwei Möglichkeiten einer Absorptionsgleichung, nämlich

$$f(x) = x \quad \text{und} \quad f(x) = y$$

Die erste Gleichung ist in jedem Verband erfüllt, die zweite erzwingt das V nur ein Element besitzt.

Damit erhalten wir, dass genau zwei Verbandsklassen durch eine Fundamentalgleichung charakterisiert werden, nämlich die Klasse aller und die Klasse der 1-elementigen Verbände.

Kapitel 7

Verbandsordnungen auf R.

7.1 Wilson's Theorem

Man zeigt leicht, dass es nur eine verträgliche Anordnung von $(\mathbf{Q}, +, \cdot)$ gibt.

Nimmt man aber eine transzendente Zahl hinzu, etwa π, so haben wir unendlich viele Möglichkeiten, den von π über $\mathfrak{Q}$ erzeugten Körper verträglich anzuordnen. Man beachte, in jedem noch so kleinen echten Intervall liegt mindestens eine transzendente Zahl t, die wir *per definitionem* durch eine Unbestimmte ersetzen könne, ohne die Struktur von $\mathbf{Q}(t)$ zu „stören".

Also könnten wir auch π unterhalb von 1 „ansiedeln", eine Trauma für den klassischen Mathematiker, doch kein Problem für den Ordnungstheoretiker, es würde ja keine wunderbare Brotvermehrung bedeuten, da etwa 2 Brote nun weniger wären als 1.

Ferner könnten wir, da es überabzählbar viele transzendente Zahlen gibt, eine Erweiterung von $\mathfrak{Q}$ mit abzählbarer Basis auf unendlich viele Weisen anordnen.

Und somit kommt die Frage auf, ob sich durch Fortsetzung oder andere geeignete Methoden ganz $\mathbf{R}$ verträglich „umzusortieren" lässt. Nun ist, wie man leicht zeigt, die Anordnung eines Körpers bestimmt durch seine positiven Elemente, und das sind in $\mathbf{R}$ die Quadrate x^2. Sie und nur sie sind bei allen Anordnungen des Körpers $\mathfrak{R}$ positiv. Also gibt es eine und nur eine Möglichkeit $\mathbf{R}$ verträglich anzuordnen.

Allerdings bleibt die Frage offen, ob es möglicherweise eine – und damit dann wahrscheinlich ein Fülle von verträglichen Verbandsordnungen von $\mathbf{R}$ gibt.

Diese Frage formulierten 1956 Birkhoff und Pierce als Problem. Ihr ist der nachfolgende Beitrag gewidmet.

Dabei handelt es sich um den Teil einer Publikation von Robert Ross Wilson, in dem er zeigt, dass $\mathfrak{R}$ 2^c, i.W. 2 hoch kontinuum viele paarweise verschiedene verträgliche Verbandsordnungem zulässt.

Es versteht sich, dass dies auf dem Wege sukzessiver Erweiterungen erfolgt. Herangezogen werden hierzu lediglich vergleichsweise elementare Mittel, so dass man auch diesen Beitrag als fundamental, obwohl elememta(l)r bezeichen darf.

Wir übernehmen das Original in Englisch, gewiss kein Problem für den Leser.

Auch diese Arbeit war mehrfach Gegenstand der Seminare des Autors bzw. Thema einer Hausarbeit.

Pacific Journal of Mathematics
Vol. 63, No. 2, 197

LATTICE ORDERINGS ON THE REAL FIELD

ROBERT ROSS WILSON

Since every total order is a lattice order, and the real field R is a totally ordered field, it is a lattice-ordered field. In 1956 Birkhoff and Pierce raised the question of whether R can be made into a lattice-ordered field in any other way. In this paper we answer their question affirmatively by showing that there are, in fact, 2^c such orderings, where c is the cardinal of R.

Introduction. We answer the question of the existence of such orderings, raised by Birkhoff and Pierce in [2, p. 68], in Theorem 1, and find the number of orders in Corollary 1.2. We denote the rational field by $\mathbf{Q}$, the positive cone of $\mathbf{R}$ (i.e., the set of reals ≥ 0) in the usual order by $\mathbf{R}^+$, and the positive cone of $\mathbf{Q}$ by $\mathbf{Q}^+$.

Theorem 1. *Let L be any subfield of $\mathbf{R}$ except $\mathbf{Q}$. Let K be any proper subfield of L, such that L is algebraic over K. Then there is a relation $\leq$ on L, with positive cone PL, such that $\langle L, \leq \rangle$ is a lattice-ordered field which is not totally ordered. Moreover:*

(1) *The order $\leq$ restricted to K is the usual total order ($K \cap P_L = K \cap R^+$)*

(2) *K is the largest totally ordered subfield of L under $\leq$.*

(3) *The order $\leq$ is a distributive lattice order.*

(4) *The order $\leq$ is* **R-compatible** *($P_L \subseteq R^+$).*

(5) *$L \cap \mathbf{R}^+$ is* **quotient-represented** *by P_L, in the sense that for each $l \in \mathbf{R}^+$, there exist $p, q \in P_L$ with $q \neq 0$, such that $l = p/q$.* We will give the proof in Section 2, where we state the main lemma (see 2.2). We will use the assertion (2) in counting the number of such orders, and we will need the technical feature (5) in the construction process.

Corollary 1.1. *Let L be a subfield of $\mathbf{R}$ containing κ distinct subfields K such that L is algebraic over K. Then L admits at least κ distinct lattice orders.*

Proof. By (2), these distinct subfields give distinct orders.

COROLLARY 1.2. **R** *admits exactly* 2^c *and the algebraic numbers A admit exactly* $2^{\aleph_0}$ *lattice orders.*

*Proof.***R** is known to be algebraic over 2^c distinct subfields and **A** over $2^{\aleph_0}$

In fact, **R** may be replaced by any uncountable subfield in Corollary 1.2. Similarly, A may be replaced by any other countable subfield which is algebraic over $2^{\aleph_0}$ subfields. We observe that incompatibility excludes from consideration many orders on proper subfields L. For example, for every incompatible order on $\mathbf{Q}(\sqrt{2})$ the non-trivial field automorphism produces another order which is not **R**-compatible. Even though it can be shown that incompatibility follows from quotient-representability, which plays an important role in the construction process, we require incompatibility during the inductive step to show that quotient-representability extends. Thus we cannot dispense with **R**-compatibility and, indeed, must prove it independently.

When P_M is the positive cone for an order $\leq$ on some subfield M of **R**, we will refer order expressions to P_M by (wrt P_M) meaning with respect to P_M.

I am especially indebted to K. Baker for many valuable suggestions and to the reviewer for extensive clarifying remarks.

2. Main lemma and proof of Theorem 1. Our method of proof employs judiciously chosen algebraic bases to extend orders. Thus, if K is ordered by $\leq$ with positive cone P_K, if $M$is an extension field of K, and if B is a basis for Mover$K$, we write $P_K(B)$ for the set of finite sums of the form $\sum k_i b_i$ with $k_i \in P_K$ and $b_i \in B$. For $B = \{b_1, ..., b_m\}$ we write $P_K(b_1, ..., b_m)$.

REMARK 2.1. If P_K is the positive cone for a lattice order on K and B is a basis for M over K, then it is immediate that $P_K(B)$ is closed under addition and that $P_K(B)$ induces a lattice order $\leq$ on Mconsidered as a group (since ordering, like addition, is computed 'coordinatewise'). Moreover, if the order on the 'coordinate' field is total, then $\leq$ is distributive.

To prove Theorem 1, we start with $P_K = K \cap \mathbf{R}^+$ and consider the collection $\mathfrak{m} = \{\langle M, B\}\rangle$ where M is an intermediate field and where $B = B_M$ is a basis for M over K such that $B \subset L \cap \mathbf{R}^+$ and such that:

(a) $P_K(B)$ is closed under multiplication (for which it will be sufficient to show that $b \cdot c \in P_K(B)$ for all b and c in B) :

(b)$P_K(B)$ is $\mathbf{P}^+$-compatible;

(c) $P_K(B)$ quotient-represents $M \cap \mathbf{R}^+$; and

(d) $1 \in B$.

By (a) and (c) above and Remark 2.1 we see that the order $\leq$ on $M$with positive cone $P_K(B)$ makes $(M, \leq)$ into a lattice-ordered field satisfying (3) and (5). Our original choice of P_K as $K \cap \mathbf{R}^+$ and (d) give (1) while the fact that distinct elements of B are incomparable with respect to $\leq$ gives us (2). Finally, (4) is just (b).

Thus, Theorem 1 will be proven if we show that (L, B_L) belongs to $\mathfrak{m}$. In fact, we will employ induction, in the form of Zorn's lemma (though we may also view it as a transfinite induction using successive simple extensions) to choose a maximal (M_0, B_{M_0}) from $\mathfrak{m}$ and we will see that $M_0 = L$. For the inductive step we will require the following lemma.

Main Lemma 2.2. *Let $M$and M' be subfields of $\mathbf{R}$ with M' a finite algebraic extension of M. Suppose that P_M is the positive cone of a lattice order $\leq$ on M which quotient-represents $M \cap \mathbf{R}^+$. Then there exists an $\alpha \in M'$ such that*

(i) $M' = M[\alpha]$,

(ii) *α satisfies $\alpha^n = a_{n-1}\alpha^{n-1} + ... + a_0$ with $a_i \in P_M$ (where n is the degree of M' over M),*

(iii) *$P_M(1, \alpha, ..., \alpha^{n-1})$ is $\mathbf{R}$-compatible, and*

(iv) *$P_M(1, \alpha, ..., \alpha^{n-1})$ quotient-represents $M' \cap \mathbf{R}^+$.*

The proof will be given in the next section.

For the inductive step we suppose $\langle M, B\rangle$ is a member of $\mathfrak{m}$ so that B is a basis for M over K satisfying (a), (b), (c) and (d). We suppose that $M \neq L$, so that there exists a proper simple extension M' of M with $M' \subset L$. We choose $\alpha \in M'$ using the Main Lemma and consider $B' = \{b\alpha^i \mid b \in B, 0 \leq i \leq n-1\}$. Now $B' \supset B$ and is a basis for M' over K satisfying (a), (b), (c) and (d). Thus $\langle M', B'\rangle \in \mathfrak{m}$. Clearly, any maximal member M_0 of $\mathfrak{m}$ must be L.

3. Proof of [the] Main Lemma In outline, the proof proceeds as follows:

Step 1. We find a β such that $M[\beta], \beta > 1$(wrt $\mathbf{R}^+$), and β satisfies $\beta^n = b_{n-1}\beta^{n-1} + ... + b_0$ with $b_i \in M \cap \mathbf{R}^+$. That is, (ii) holds except that

$M \cap \mathbf{R}^+$ replaces P_M, (This step depends only on the usual topology of $\mathbf{R}$ and $\mathbf{C}$ and the usual order structure of $\mathbf{R}$.)

Step 2. We use quotient-representability to replace β by $\alpha \in M'$ so that (i) $M' = M[\alpha], \alpha > 1($ wrt $R+)$, and α satisfies (ii). We write P'_M for $P_M(1, \alpha^n, ..., \alpha^{n-1})$. It is clear that $P'_M \subset M \cap \mathbf{R}^+$ (i.e., that P'_M satisfies (iii)).

For use in the remaining steps we define

$$Q'_M := \{p/q | p, q, \in P'_M, q \neq 0\}$$

which is the positive cone of an incompatible partial order on M'.

Step 3. To show [that] P'_M quotient-represents $M' \cap \mathbf{R}^+ \subset \mathbf{Q}'_M$ it is clearly sufficient to show $\mathbf{Q}^+ \subset \mathbf{Q}'_M$. To this end, we show that $\mathbf{Q}^{\subset} Q'_M$ and, after defining the concept of $\mathbf{Q}$-approximability, we show how $\mathbf{Q}$-approximability of M' implies I $M' \cap \mathbf{R}^+ \subset \mathbf{Q}'_M$.

Step 4. We show that a is $\mathbf{Q}$-approximable, that every element of $M$is $\mathbf{Q}$-approximable and that the $\mathbf{Q}$-approximable elements of M' constitute a subring and therefore must be $M[a] = M'$ itself.

Details of Step 1. We let γ be such that $M' = M'[\gamma]$ and its minimal polynomial is $h(x)$. We suppose $\gamma = \gamma_1, \gamma_2, ..., \gamma_n$ are all the (necessarily distinct) roots of h in $\mathbf{C}$. We show below how to construct a non-singular linear fractional transform T with rational coefficients so that $\beta = T(\gamma) > 1($ wrt $\mathbf{R}^+)$ and for $2 \leq i \leq n$ the $\beta_1 = T(\gamma_i >$ are "sufficiently close" to $1/n$. Since the coefficients are continuous in the roots, a comparison with $(x + 1/n)^{n-1}$ shows that $(x\beta_2) \cdot ... \cdot (x\beta_n) = x^{n-1} + c_{n-2}x^{n-2} + ... + c_0$ satisfies $1 = c_{n-1} > c_{n_2} > ... > c_0 > 0$. (See [3, L. 6.2, p. 40] for details, including [the]proof that "sufficiently close" means "within $\varepsilon = 1/n$". Therefore $g(x) = (x - \beta) \cdot (x - \beta_2) \cdot ... \cdot (x - \beta_n) = x^n - b_{n-1}xn - 1 - ... - b_0$ where $b_i = c_i\beta - c_i > c_i c_{i-1} > 0$ for $1 \leq i \leq n1$ and $c_0 = \beta c_0 > 0$. We note that $g(x)$ is the minimal polynomial of β over M and is computed by clearing the denominators of $h(T^{-1}(x))$ and scaling.

To construct T we let $\varepsilon = 1/n^2$ as above and choose rationals t and s such that $0 < t(1/\varepsilon + 1/2) < \min |\beta - \beta_i|$ for $i \geq 2$ and $0 < \beta/ - s << 1/2$. Then T is the composition of the following maps: $x \to x/t; x \to x - s; x \to 1/x; x \to x - 1/n$ (After the first two the image of γ is in the interval $(0, 1/2)$

and the rest of the roots are outside a circle of radius $1/\varepsilon$ centered at 0, and after the last $\beta = t/(\gamma - ts) - 1/n > 1$ and the other β_i are within ε of $1/n$.)

Details of Step 2. Using quotient-representability, we choose $d \in P_M$ so that $db_i \in P_M$ for $0 \leq i \leq n1$ and so that $d > 1(\text{ wrt } \mathbf{R}^+)$. (The latter Condition may be achieved by positive integer scaling without affecting the former conditions.) Then $\alpha = d\beta$ has $f(x) = d^g(x/d) = x^n a_{n-1}x^{n-1} - ... - a_0$ as its minimal polynomial over M and $a_i = d^{n-1}b_i \in P_M$ for $0 \geq i \geq n1$. That is, α satisfies (ii). Clearly $M[\alpha] = M[\beta] = M[\gamma] = M'$.

Details of Step 3. Let $r \in \mathbf{Q}^+$ and $p \in P'_M$. We may scale p by positive integers, as above, and by reciprocals of such using [1, Thm. 3, p. 293] with the result rp in P'_M. Since we may write $r = rp/p$ for any non-zero p, we see that $r \in \mathbf{Q}'_M$. We say that $m \in M'$ is $\mathbf{Q}$-approximable if for each positive rational t there is a rational s such that $m < s < m+t(\text{ wrt } \mathbf{Q}'_M)$. (Of course, $mt < st < m(\text{ wrt } \mathbf{Q}'_M)$ also.)

Now if $m > 0(\text{ wrt } \mathbf{R}^+)$ and m is $\mathbf{Q}$-approximable, we choose a positive rational t so that $mt > 0(\text{ wrt } \mathbf{R}^+)$ and rational s so that $m < s < m + t(\text{ wrt } \mathbf{Q}'_M)$. By $\mathbf{R}$-compatibility

$$s - t > m - t > 0(\text{ wrt } \mathbf{R}),$$

and since $\mathbf{Q} \subset \mathbf{Q}'_M, s - t \in \mathbf{Q}'_M$. Thus $m = ((m + ss) - s) + (s - t) \in \mathbf{Q}'_M$ by the additive closure of Q'_M.

Details of Step 4. To show M is $\mathbf{Q}$-approximable, we arbitrarily choose m in M and t positive in $\mathbf{Q}$. By density of $\mathbf{Q}$ in $\mathbf{R}$, there is a rational s such that $m < s < m + t(\text{ wrt } \mathbf{R}^+)$ and by quotient-representability of $M \cap \mathbf{R}^+$ by P_M these inequalities hold wrt $\mathbf{Q}_M$. But $\mathbf{Q}_M \subset \mathbf{Q}'_M$ so $m < s < m+t(\text{ wrt } \mathbf{Q}'_M)$, which is $\mathbf{Q}$-approximability.

To verify that a is $\mathbf{Q}$-approximable, we again choose an arbitrary positive t in $\mathbf{Q}$. Since $f(x) = 0$ and f is separable, the derivative $f'(\alpha)$ is non-zero. Because $a > l(\text{ wrt } \mathbf{R}^+)$ this implies there is a rational $s > l(\text{ wrt } \mathbf{R}^+$ such that $0 < f(s) < \alpha+t(\text{ wrt } \mathbf{Q}'_M)$. For such s we show $\alpha < s < \alpha+t(\text{ wrt } \mathbf{Q}'_M)$ and hence that α is $\mathbf{Q}$-approximable:

First, since $s, f(s)$, and t are in M and M is quotient-representable, we see that $s > 1$ and $0 < f(s) < t(\text{ wrt } \mathbf{Q}_M)$ and hence (wrt Q'_M). Next we note that Q'_M is closed under division and $s\alpha f(s)/(f(s)/(s\alpha)$, so, to show $s\alpha > 0(\text{ wrt } \mathbf{Q}'_M)$, we need only show $f(s)/(s - a) \in \mathbf{Q}'_M$. Now $f(s) =$

$f(s)-f(\alpha) = (s^n-\alpha^n)-a_{n-1}(a^{n-1}-\alpha^{n-1}-...-1(s-\alpha)$. Thus $f(s)/(s-\alpha) = s^{n-1} + d_{n-2}s^{n-2} + ... + d_0$, where the $d_i = \alpha^{n-i-1} - \alpha_{n-1}\alpha^{n-i-2} - ... - \alpha_{i+1}$ are "scaled truncations" of $f(\alpha)$. In fact, $d_i = (f(\alpha) + a_i\alpha_i + ...a_0)/\alpha^{i+1} = (a_i\alpha_i + ... + a_0)/\alpha^{i+1} \in \mathbf{Q}'_M$ Since $s^i > 1 > 0(\text{ wrt } \mathbf{Q}'_M), f(s)/(s-\alpha) > 1 > 0(\text{ wrt } \mathbf{Q}'_M)$. Thus $0 < s-\alpha < f(s) < t(\text{ wrt } \mathbf{Q}'_M)$ so that $\alpha < s < a+t(\text{ wrt } \mathbf{Q}'_M)$.

To finish Step 4 and thus the proof of the Main Lemma, we need to show the set of **Q**-approximable elements of M is a subring. The proof of closure under subtraction is straightforward, after recalling that we can approximate below also. The proof of closure under multiplication, though resembling the proof of the product rule for derivatives, takes some care. At several points when dealing with the rationals used as "epsilons and deltas" by the approximating process it is necessary to switch from $\mathbf{R}^+$ to Q'_M using $\mathbf{Q}^+ \subset Q'_M$ or from Q'_M to $\mathbf{R}^+$ using **R**-compatibility.

4. Alternate theorem, examples and questions. By a slight modification in the proof of Theorem 1 we can prove Theorem 1*, which differs from Theorem 1 in that (1) and (2) are replaced by their complete opposites (1*) and (2*) and in that (0*), which has no counterpart in Theorem 1, is added. (0*) There are no totally ordered subfields of L under $\leq$.

(1*) The order $\leq$ restricted to K is the trivial partial order. (In particular, $1 \not> 0$.)

(2*) K is the largest trivially ordered subfield of L under $\leq$.

Before we prove Theorem 1*, we note that Corollaries 1.1 and 1.2 also hold for this type of order. In the proof of Theorem 1* we indicate by * the changes from the proof of Theorem 1. We again start with $P_K = K \cap \mathbf{R}^+$ and seek $B^* = L \cap \mathbf{R}^+$ satisfying (a), (b) and (c) as before, but

(d*) $1 \notin P_K(B^*)$

instead of (d). Now (3), (4) and (5) follow as before and (d*) implies (1*). To see this, we suppose (1*) false and pick $k \in K \cap P_K(B^*)$ with $k \neq 0$. Then $0 < kk^{-1}(\text{ wrt } \mathbf{R}^+)$ by **R**-compatibility and so $k^{-1} \in K \cap \mathbf{R}^+$. Thus $0 < k^{-1}k = 1(\text{ wrt } K\cap \Rightarrow^+)$, contradicting (d*).

The fact that every $b \in B*$ satisfies $0 < b(\text{ wrt } P_K(B*))$ gives (2*) while (1*) shows that **Q** must be trivially ordered and this gives (0*). The Main Lemma is unaltered and applies as before during the inductive step to show

that (a), (b), (c) and (d*) are preserved by finite extensions. Thus, in order to achieve (d*), we start the induction so that the first nontrivial finite extension has basis $B^* = \{\alpha, \alpha^2, ..., \alpha^n\}$ rather than $\{1, \alpha, ..., \alpha^{n-1}\}$. Then we note that, in the proof of the Main Lemma, the b_i in step 1 and hence the a_i in step 2 are all nonzero. Thus $1 = (\alpha^n a_{n-1}\alpha^{n-1}...a_1\alpha)/\alpha_0 \notin P_K(B*)$, which is (d*).

The following examples illustrate how bases are constructed using the Main Lemma. Of course, all of them satisfy (a), (b), and (c) and either (d) or (d*).

EXAMPLE 4.1. We let $M = Q$, $M' = Q(\gamma)$ where $\gamma^2 = 2$ and $\gamma > 0$(wrt $\mathbf{R}^+$) and choose $t = 1, s = 1$. This gives β satisfying $\beta^2 = 2\beta + 1$ and choosing $d = 1$ gives $\alpha = \beta$. Thus $B = \{1, \alpha\}$ satisfies (d) and $B^* = \{\alpha, \alpha^2\}$ satisfies (d*). Note that γ is neither in $P_Q(B)$ nor in $P_Q(B^*)$.

EXAMPLE 4.2. We let $M = Q(\alpha)$, $M' = Q(\gamma')$ where $\gamma'^2 = \gamma$ and $\gamma^2 > 0$(wrt $\mathbf{R}^+$), and choose $t = 1/2, s = 2$. This gives β' satisfying $\beta'^2 = (\alpha - 1)\beta' + (3\alpha - 1)/4$. The coefficients, while positive wrt $\mathbf{R}^+$ are not positive in either order of 4.1. If $P_M = P_Q(1, \alpha)$, then $\alpha - 1 = (\alpha + 1)/\alpha$ and $3\alpha - 1 = (5\alpha+3)/\alpha$. Thus we choose $d = \alpha$ and get α' satisfying $\alpha'^2 = (\alpha+1)\alpha' + (5\alpha^2 + 3\alpha)/4$. This gives $B = \{1, \alpha, \alpha', \alpha\alpha'\}$. On the other hand, if $P_M = P_Q(\alpha, \alpha^2)$, then $\alpha - 1 = (\alpha^2+\alpha), 3\alpha - 1 = (5\alpha^2+3\alpha)/\alpha^2$ and we choose $d = \alpha^2$. This gives α^* satisfying $\alpha^{*2} = (\alpha^2 + \alpha)\alpha^* + (5\alpha^4 + 3\alpha^3)/4$ and $B^* = \{\alpha, \alpha^2, \alpha\alpha^*, \alpha^2\alpha^*\}$

We note that Corollaries 1.1 and 1.2 fail to determine the cardinality of the class of lattice orders for those countable subfields L which are algebraic over only countably many subfields K. For instance, Corollary 1.1 only accords finitely many lattice orders to simple extensions L of $\mathbf{Q}$, but:

COROLLARY 4.3. *If L is a simple extension of $\mathbf{Q}$ then L admits at least $\aleph_0$ lattice orders.*

Proof. We recall from the proof of Theorem 1* that in $f(x) = x^n - a_{n-1}x^{n-1} - ... - a_0$, the minimal polynomial of α, the (rational) α^* are greater than 0 (i.e., α satisfies (ii)). Thus there are $\aleph_0$ distinct sufficiently small rationals r such that the minimal polynomial of $\alpha - r$ still satisfies (ii).

Questions 4.4.

(a) Do any countable subfields L of $\mathbf{R}$ which are algebraic over no more than $\aleph_0$ subfields have $2^{\aleph_0}$ orders?

(b) Are there any **R**-compatible lattice orders on subfields L of **R** which do not quotient-represent $L \cap \mathbf{R}^+$

(c) Besides the **R**-compatible orders constructed here and those on subfields related to **R**-compatible orders by automorphisms, what other lattice orders are there? In particular, are there any non-incompatible orders on **R** itself?

Kapitel 8

Allgemein Algebraisches

8.1 Algebraische Verbände

8. 1. 1 Definition. Sei $(V, \leq)$ ein vollständiger Verband. Dann heißt $a \in V$ *kompakt*, wenn gilt:

$$a \leq \bigvee b_i (i \in I) \Longrightarrow a \leq b_{i_1} \vee \ldots \vee b_{i_n} \quad (\exists\, b_{i_k} : i_k \in I, 1 \leq k \leq n)\,.$$

Offenbar ist mit je zwei kompakten Elementen a, b auch $a \vee b$ kompakt. Hingegen muss das Element $a \wedge b$ nicht notwendig kompakt sein.

8. 1. 2 Beispiel. Setze in $\mathbf{R}^2$ $(a, b) \subset (c, d)$ gdw. $b < d$ und betrachte die Menge M der Elemente

$$\Big\{(0,0), (0,\frac{1}{2}), (0,\frac{3}{4}), \ldots, (0,\frac{2^n-1}{2^n}), (0,1), (-1,2), (+1,2), (0,3)\Big\}\,.$$

Dann sind die Elemente $a := (-1, 2)$ und $b := (+1, 2)$ kompakt, doch ist der Durchschnitt $a \cap b = (0{,}1)$ nicht kompakt.

8. 1. 3 Definition. Sei $(V, \leq)$ ein vollständiger Verband. Dann heißt $(V, \leq)$ *algebraisch*, wenn jedes b aus V ein $\bigvee a_i$ $(i \in I)$ mit kompakten $a_i \in V$ ist.

Offenbar ist der soeben konstruierte Verband algebraisch. Als ein erster klassischer Vertreter des algebraischen Verbandes ist der Verband der Unterräume eines Vektorraums zu nennen. Als weitere klassische Vertreter seien erwähnt der Verband der Ideale eines (kommutativen) Ringes mit 1, der Verband der Untergruppen einer Gruppe und schließlich das elementarste und fundamentalste aller Beispiele, nämlich der Verband aller Teilmengen einer (nicht leeren) Menge M.

Dies legt es nahe, die Elemente algebraischer Verbände mit großen Buchstaben – im Sinne von Teilmengen – zu bezeichnen und die kleinen Buchstaben zu reservieren für ausgezeichnete Elemente, die später stehen werden für Elemente von Mengen bzw. für Repräsentanten von *endlich erzeugten Idealen.* Ist $\mathfrak{V}$ ein algebraischer Verband, so schreiben wir auch im Sinne der Idealtheorie $\subseteq$ statt $\leq$ und setzen

$$\sum A_i \ (i \in I) := \bigvee A_i \ (i \in I)$$

$$\text{und} \qquad \bigcap A_i \ (i \in I) := \bigwedge A_i \ (i \in I) \,.$$

Als klassischstes aller Modelle des algebraischen Verbandes wird sich der Verband der Ideale eines $\vee$-Halbverbandes erweisen. Weiter sei erinnert an den Verband der Ordnungsideale bzw. Ordnungsfilter. Dass die Menge der Ordnungsideale bzw. der Halbverbandsideale jeweils einen algebraischen Verband bildet, ist natürlich noch nachzuweisen. Aus diesem Grunde, nicht zuletzt auch wegen der symptomatischen Bedeutung, formulieren wir als Satz:

8. 1. 4 Proposition. *Sei $\mathfrak{H} = (H, \vee, 0, 1)$ ein Sup-Halbverband mit 0 als Minimum und 1 als Maximum. Dann bilden die Ideale aus $\mathfrak{H}$ einen algebraischen Verband $\mathfrak{V}$.*

BEWEIS. Zunächst bildet H selbst ein Ideal.

Weiter bildet mit jeder Familie von Idealen auch ihr Durchschnitt ein Ideal, wie man routinemäßig zeigt.

Somit lässt sich jeder Teilmenge A aus H als *Erzeugnis* $[\,A\,]$ der Durchschnitt aller Ideale zuordnen, die A umfassen. Dies ist dann wieder ein Ideal und insbesondere im Falle zweier Hauptideale $(a\,], (b\,]$ das Hauptideal $(a \vee b\,]$. Denn offenbar ist $(a \vee b\,]$ an der Bildung von $[\,(a\,] \cup (b\,]]$ beteiligt und andererseits in jedem anderen, die Hauptideale $(a\,]$ und $(b\,]$ umfassenden Ideal, enthalten. Damit ist die Vollständigkeit gesichert. Um zu zeigen, dass $\mathfrak{A}$ auch algebraisch ist, bauen wir als nächstes die Hülle $[\,A\,]$ von innen her auf.

Hier erkennen wir, dass natürlich alle endlichen Suprema $a_1 \vee \ldots \vee a_n$ in $[\,A\,]$ enthalten sein müssen und damit gemäß der Definition des Idealbegriffs auch alle $x \leq a_1 \vee \ldots \vee a_n$. Andererseits liefert dies schon eine interne Beschreibung von $[\,A\,]$, da diese Menge, wie der Leser sofort bestätigt, selbst schon ein Ideal bildet.

Hiernach ist der Rest des Beweises rasch geführt. Denn zunächst haben wir die Gleichung $\bigvee\limits_{i\in I} A_i = \left[\bigcup\limits_{i\in I} A_i\right]$ und damit weiter

$$\begin{aligned} x \leq \bigvee A_i &\implies x \leq a_1 \vee \ldots \vee a_n \quad (\exists\, a_k \in \textstyle\bigcup_{i_k\in I} A_{i_k}) \\ &\implies x \leq A_{i_1} \vee \ldots \vee A_{i_n} \end{aligned}$$

□

Wie nicht anders zu erwarten, gelten in algebraischen Verbänden ähnliche Sätze wie in den Idealverbänden von Halbverbänden. Dies hat seinen ganz natürlichen Grund in dem nun folgenden:

8. 1. 5 1. Darstellungssatz für algebraische Verbände. *Jeder algebraische Verband $\mathfrak{A}$ lässt sich auffassen als der Verband der Ideale eines Halbverbandes.*

BEWEIS. Mit je zwei kompakten Elementen a, b ist auch deren Supremum $a \vee b$ kompakt, so dass die Menge C aller kompakten Elemente aus $\mathfrak{A}$ einen Halbverband bildet und die in einem beliebig vorgegebenen Element A enthaltenen kompakten Elemente stets ein Ideal dieses Halbverbandes.

Ordnen wir also A als $\phi(A)$ jeweils die Menge $\{c \,|\, c \in C \;\&\; c \leq A\}$ zu, so ist ϕ natürlich eine Funktion, die einerseits injektiv ist, da zu verschiedenen Elementen aus $\mathfrak{A}$ *per definitionem* verschiedene Bilder gehören, und die andererseits alle Ideale ausschöpft, da den jeweiligen Suprema von Idealen aufgrund der Algebraizität exakt diese Ideale als ϕ-Bild zugeordnet sind.

Schließlich erkennen wir, dass die Abbildung ϕ zunächst $\bigcap$-treu und damit weiter auch $\sum$-treu ist. □

Der letzte Satz beinhaltet natürlich, dass sich Begriffe und Sätze, bezogen auf den Idealbereich eines Halbverbandes übertragen lassen auf algebraische Verbände.

Hiernach lässt sich beweisen

8. 1. 6 Der Einbettungssatz. *Sei $\mathfrak{V}$ eine Poset, ein Verband, ein modularer Verband, ein distributiver Verband. Dann lässt sich $\mathfrak{V}$ einbetten in einen algebraischen Verband, derart, dass die Elemente von $\mathfrak{V}$ übergehen in kompakte Elemente. Darüber hinaus ist mit $\mathfrak{V}$ auch die Erweiterung modular bzw. distributiv, und wir können $\mathfrak{V}$ im Falle einer Poset bezüglich der Inklusion $\supseteq$ sogar in eine Mengenalgebra einbetten.*

BEWEIS. Wir betrachten die Menge der Ideale. Wie schon erwähnt ist mit jeder Familie A_i $(i \in I)$ der jeweiligen Ideale auch deren Durchschnitt $\bigcap A_i$ ein Ideal, so dass die Gesamtheit der Ideale jeweils einen vollständigen Verband bildet. Wir erinnern an $A+B := [\, A \cup B\,]$ und sehen, dass die *Hauptideale* $(x\,]$ in der jeweils gegebenen Situation den Bedingungen

$$(a\,] \cap (b\,] = (a \wedge b\,] \quad \text{bzw.} \quad (a\,] + (b\,] = (a \vee b\,]$$

genügen.

Betrachten wir $\mathfrak{V}$ nun als Poset, so bilden die (Ordnungs-) Ideale einen Mengenverband, der sich erweitern lässt zu einem vollständigen Mengenverband, indem wir nicht nur die Ordnungsideale von $\mathfrak{V}$, sondern alle Teilmengen von V hinzuziehen.

Zu zeigen bleibt, dass der Idealverband modularer Verbände modular ist und der Idealverband distributiver Verbände distributiv.

Hierzu ist im Falle der Modularität die Implikation nachzuweisen:

$$A \supseteq C \Longrightarrow A \cap (B + C) \subseteq (A \cap B) + C\,.$$

Sei also $A \supseteq C$ erfüllt. Dann folgt:

$$\begin{aligned} x \in A \cap (B + C) &\implies x = a \wedge (b \vee c) \;\; (a \in A, b \in B, c \in C) \\ &\implies x \leq (a \vee c) \wedge (b \vee c) \\ &\implies x \leq ((a \vee c) \wedge b) \vee c) \\ &\implies x \in (A \cap B) + C \end{aligned}$$

und damit die Modularität des Idealverbandes.

Analog schließt man im Blick auf die Distributivität, allerdings haben wir hier wegen 4.2.3 sogar $A \vee B = \{x \,|\, x = a \vee b\}$, wodurch sich die Herleitung ein wenig erleichtert. □

Wir beenden diesen Paragraphen mit einem Darstellungssatz, der später herangezogen werden wird zur Beschreibung projektiver Geometrien. Doch zuvor erwähnen wir noch, ebenfalls im Blick auf das nächste Kapitel:

Ist $\mathfrak{P}$ eine Poset, so nennt man eine Teilmenge T von P nach *oben gerichtet*, wenn mit je zwei Elementen a, b aus T mindestens ein $c \geq a, b$ zu T gehört.

8. 1. 7 Proposition. *Sei $\mathfrak{V}$ ein $\bigvee$-algebraischer Verband und sei B eine nach oben gerichtete Teilmenge aus V. Dann gilt das Distributivgesetz:*

$$\ell := a \wedge \bigvee b_i \ \ (b_i \in B) = \bigvee (a \wedge b_i) \ \ (b_i \in B)\,.$$

DENN: Es genügt zu zeigen, dass $\ell \leq r$ erfüllt ist. Sei hierzu x kompakt und $x \leq \ell$ erfüllt. Dann gilt $x \leq a$ und $x \leq b_{i_1} \vee \ldots \vee b_{i_n}$, also wegen der Existenz eines $c \geq b_{i_1} \vee \ldots \vee b_{i_n}$ dann auch $x \leq r$. □

8.2 Algebren

Sei M eine nichtleere Menge. Dann versteht man unter einer *n-stelligen Operation* auf M jede *Abbildung* $f : M^n \longmapsto M$. Beispiele für Algebren sind also etwa die Gruppe $\big(G\,,\,\cdot\,,\,^{-1}\big)$, der Verband $(V, \vee, \wedge)$, aber auch der Vektorraum, man betrachte die *Skalaren-Multiplikationen* $\mathfrak{a} \mapsto s\mathfrak{a}$ als einstellige Operationen.

Ist $f_i \ \ (i \in I)$ eine *Familie* von Operationen $f_i : M^{n_i} \longmapsto M$, so heißt (M, f_i) eine *Algebra* vom *Typ* $(n_i \ \ (i \in I))$. Hiernach ist die Gruppe eine Algebra vom Typ $(2, 1)$, der Verband hingegen eine Algebra vom Typ $(2, 2)$ und jeder Vektorraum über $\mathbf{Q}$ etwa vom Typ $(2, 1, 1, \ldots)$

Die schlichteste aller Algebren ist natürlich (M, Id) mit $Id(a) = a$. In diesem Sinne ist jede Menge auch eine Algebra.

Symptomatisch(er) für das Verhalten von Algebren ist jedoch das Gruppoid, d. h. die Algebra vom Typ (2), über die also nichts weiter vereinbart ist als dass (genau) eine 2-stellige Operation erklärt sei.

Ist in einer Algebra für die Operation f etwa $f(a_1, \ldots, a_n) = a$ erfüllt, so schreiben wir auch $a_1\, f\, a_2\, f\, \ldots\, f\, a_n = a$. Insbesondere wählen wir für zweistellige Operationen Symbole der Art $+$, $-$, $\cdot$, $*$, $\wedge$, $\vee$, Δ, ∇ ..., wohingegen einstellige Operationen durch Symbole wie $-$, $^{-1}$, $'$,* ... symbolisiert werden.

Einstellige Operationen nennt man in Algebra und Geometrie auch *Operatoren,* in der Analysis hingegen *Funktionen.*

Operatoren bzw. Funktionen wären also u. a. in der Geometrie alle Abbildungen und damit insbesondere in der Geometrie die *Spiegelung* Σ_g an einer Geraden g oder in der Analysis etwa die *Logarithmus-Funktion* log, bzw.die *Exponentialfunktion* exp.

Sei erneut M eine nichtleere Menge. Dann verstehen wir unter einer *n-stelligen Relation* auf M jede Teilmenge von R^n. Insofern Relationen auf diese Weise als Mengen definiert sind, können wir mit Relationen verfahren wie mit Mengen, also u. a. den *Durchschnitt einer Familie* von Relationen bilden und somit auch das *Erzeugnis einer Familie* von Relationen, d. h. den Durchschnitt aller Relationen, die alle Relationen der vorgegebenen Familie umfassen etc. Unter den Relationen heben wir die *Identität* ι mit

$$(\iota) \qquad (x_1, \ldots, x_n) \in \iota \;:\Longleftrightarrow\; x_1 = x_2 = \ldots = x_n$$

und die *Allrelation* $R^n =: \omega$ hervor. Relationen werden üblicherweise mit kleinen griechischen Buchstaben benannt, also etwa mit $\rho\,, \sigma\,, \theta\;\ldots$ oder aber durch Symbole wie $|\,, \|\,, \perp\,, \equiv, \leq, \geq, \subset, \supseteq, \sim, \ldots$ notiert.

Für uns sind im weiteren lediglich zweistellige Relationen von Bedeutung und unter ihnen die so genannten *Kongruenzrelationen.* Ist ρ eine zweistellige Relation, so schreiben wir auch $a\,\rho\,b$ statt $(a, b) \in \rho\,.$

8. 2. 1 Definition. Eine 2-stellige Relation $\sim$ heißt eine *Äquivalenzrelation,* wenn sie *reflexiv, symmetrisch* und *transitiv* ist, d.h. die Gesetze erfüllt:

$$(\mathrm{R}) \qquad a \sim a$$

$$(\mathrm{S}) \qquad a \sim b \implies b \sim a$$

$$(\mathrm{T}) \qquad a \sim b \;\&\; b \sim c \implies a \sim c.$$

Äquivalenzrelationen induzieren *Klassenzerlegungen* $\{M_i\}\ (i \in I)$, kurz Zerlegungen von M mit $M = \bigcup M_i\ (i \in I)$ und $i \neq j \Longrightarrow M_i \cap M_j = \emptyset$, was der Leser leicht bestätigt.

Ist $\sim$ eine Äquivalenzrelation und $K(a)$ die Klasse von a bezüglich $\sim$, so bezeichnen wir $K(a)$ auch mit $a_\sim$ oder mit $\tilde{a}$ bzw. auch mit $\overline{a}$. Dabei wird in der Regel klar sein, worauf sich diese *Klassenbildung* bezieht. Ist eine Äquivalenzrelation mit θ bezeichnet, notieren wir $K(a)$ auch als $a\theta$.

Wie man leicht verifiziert, gehen gewisse Eigenschaften bei der Bildung des Durchschnitts mit. So ist der Durchschnitt einer Familie von Äquivalenzrelationen wieder eine Äquivalenzrelation. Demzufolge können wir zu einer Familie $\{\theta_i\}$ die erzeugte Äquivalenzrelation $\bigvee \theta_i := \bigcap \theta_j$ ($\theta_j \supseteq \theta_i$ (θ_i eine ÄR $(i \in I)$) bilden. Dieses Erzeugnis, das *per definitionem* von außen gebildet ist, lässt sich von innen her offenbar beschreiben vermöge der Äquivalenz

$$(\mathrm{OG}) \quad (a, b) \in \bigvee_{i \in I} \theta_i :\Longleftrightarrow \exists\, x_1\,, x_2\,, \ldots\,, x_n : a\ \theta_{i_1}\ x_1\ \theta_{i_2}\ x_2\ \theta_{i_3}\ \ldots\ \theta_{i_n}\ b\,.$$

Damit erhalten wir als ein erstes Resultat:

8. 2. 2 Proposition. *Der Verband der Äquivalenzrelationen einer Menge ist vollständig und sogar algebraisch.*

Von großer Bedeutung ist für 2-stellige Relationen neben den mengentheoretischen Operationen die *Verkettung.*

8. 2. 3 Definition. Seien ρ und σ 2-stellige Relationen. Dann definiert man das *Relationenprodukt* $\rho \circ \sigma$ vermöge

(RP) $$a \; \rho \circ \sigma \; b \quad :\Longleftrightarrow \quad \exists\, x : \, a \,\rho\, x \;\&\; x \,\sigma\, b \; .$$

Gilt insbesondere $\rho \circ \sigma = \sigma \circ \rho$, so heißen ρ und σ *vertauschbar.*

Wie der Leser weiter leicht bestätigt, ist das Relationenprodukt zweier vertauschbarer Relationen gleich ihrem Erzeugnis, man vertausche in (OG) sukzessive.

8. 2. 4 Definition. Ist A eine beliebige Menge und ist $f_i \;\; (i \in I)$ eine Familie endlichstelliger Operationen auf A, so nennt man $\mathfrak{A} := (A, f_i \;\; (i \in I))$ eine *Algebra* mit der Trägermenge A und den Operationen f_i.

8. 2. 5 Definition. Sei $\mathfrak{A} = (A, f_i) \;\; (i \in I)$ eine Algebra mit endlich-stelligen Operationen. Dann heiße eine Teilmenge T von A *abgeschlossen*, wenn sie für alle n-stelligen $f_i \;\; (n \in \mathbf{N})$ die Implikation erfüllt:

$$x_1, \ldots, x_n \in T \;\; \Longrightarrow \;\; f_i(x_1, \ldots, x_n) \in T.$$

Offenbar gelten die beiden nachfolgenden Items:

(i) Die Trägermenge A ist abgeschlossen.

(ii) Mit jeder Familie $A_i \;\; (i \in I)$ von abgeschlossenen Teilmengen ist auch deren Durchschnitt abgeschlossen.

Somit können wir zu jeder Teilmenge B die von B erzeugte engste abgeschlossene Teilmenge als Durchschnitt aller B umfassenden abgeschlossenen Teilmengen bilden. Sie wird auch als abgeschlossene Hülle von B bezeichnet und mittels $[\, B \,]$ symbolisiert.

Unter anderem erhalten wir so für jede Familie $A_i \;\; (i \in I)$ abgeschlossener Teilmengen mit $\bigvee\limits_{i \in I} A_i := [\, \bigcup A_i \,]$ eine natürliche obere Grenze derart, dass die

Menge der abgeschlossenen Teilmengen bezüglich $\bigcap$ und $\bigvee$ einen vollständigen Verband bildet.

Die von außen definierte Hülle $[\,B\,]$ lässt sich von innen her – nach bewährtem Muster – wie folgt gewinnen:

Man nehme zu B zunächst alle f_i-Werte für entsprechende n-tupel aus B hinzu und bilde auf diese Weise B_1. Hiernach verfahre man mit B_1 wie zuvor mit B und setze dieses Verfahren sukzessive fort. Dann ist $\bigcup\limits_{i\in I} B_i$ offenbar das Erzeugnis der Menge B und somit gleich $[\,B\,]$.

Insbesondere sehen wir, dass $[\,a\,]$ kompakt ist. Denn $[\,a\,]$ ist nach der soeben vorgestellten Konstruktion genau dann in dem Erzeugnis der abgeschlossenen Teilmengen $[\,B_i\,]$ enthalten, wenn $[\,a\,]$ schon in dem Erzeugnis endlich vieler dieser $[\,B_i\,]$ enthalten ist.

Somit bilden die abgeschlossenen Mengen einer Algebra einen algebraischen Verband. Es gilt aber auch

8. 2. 6 Ein Satz von Birkhoff und Frink. *Ist $\mathfrak{V}$ ein algebraischer Verband, so lässt sich $\mathfrak{V}$ auffassen als Verband der abgeschlossenen Mengen einer geeignet gewählten Algebra.*

BEWEIS. Definiere auf der Menge C der kompakten Elemente die Operationen $\vee_c$ mittels $a \vee_c b := a \vee b$ und f_c $(c \in C)$ vermöge

$$f_c(a) := \begin{cases} a & \text{falls } c \geq a \\ 0 & \text{falls } c \ngeq a\,. \end{cases}$$

Dann ist jedes Ideal I aus $(C, \vee)$ wegen $0 \in I$ *per definitionem* abgeschlossen, und ist umgekehrt eine Teilmenge A von C abgeschlossen, so liegt mit je zwei Elementen a, b auch $a \vee b = a \vee_c b$ in A und mit $a \leq c \in A$ auch $f_c(a) = a$.

Somit ist der Verband der abgeschlossenen Teilmengen aus $(C, \vee_c, f_c)$ identisch mit dem Verband der Ideale aus $(C, \vee)$ und folglich isomorph zu $\mathfrak{V}$. □

Der oben bewiesene Satz hat eine Entsprechung für Relative. Um dies zu skizzieren, geben wir zunächst

8. 2. 7 Definition. Sei $\mathfrak{A}$ ein Relativ. Dann heißt eine Teilmenge T von A abgeschlossen, wenn sie für alle $n+1$-stelligen ρ_i $(n \in \mathbf{N})$ die Implikation

erfüllt:

$$x_1, \ldots, x_n \in T \;\&\; (x_1, \ldots, x_n, x) \in \rho_i \Longrightarrow x \in T.$$

Hiernach dürfen wir den Beweis des Satzes von BIRKHOFF und FRINK für Relative dem Leser überlassen.

HINWEIS. Erkläre Relationen so, dass sie die Rolle der oben definierten f_c übernehmen können. Dies sichert, dass sich jeder algebraische Verband auffassen lässt als Verband der abgeschlossenen Teilmengen eines Relativs.

Andererseits erhalten wir wie oben, dass die abgeschlossenen Teilmengen eines Relativs stets einen algebraischen Verband bilden. Der Rest ist klar.

8.3 Kongruenzen

Wie schon oben erwähnt, darf man das Gruppoid als „Paukboden" der Allgemeinen Algebra betrachten. Was immer dort formuliert wird, gewinnt hier an Durchsicht ohne an eigentlicher Allgemeinheit zu verlieren. Dies wird ganz deutlich werden in dem nun folgenden Abschnitt.

8. 3. 1 Definition. Sei $\mathfrak{G} = (G, \circ)$ ein *Gruppoid* und $\sim$ eine Äquivalenzrelation auf G. Gilt dann

$$a \sim a' \;\&\; b \sim b' \;\Longrightarrow\; a \circ b \sim a' \circ b' \,, \tag{8.7}$$

so liefert die Festsetzung

$$K(a) \cdot K(b) \;:=\; K(a \circ b) \tag{8.8}$$

eine Operation auf der Menge der Klassen von $\sim$. Die Relation $\sim$ heißt in diesem Falle eine *Kongruenzrelation* und die *abgeleitete Algebra* der Klassen $K(a)$ die *Restklassenalgebra* von $\mathfrak{G}$ nach $\sim$, i. Z. $\mathfrak{G}/\!\sim$. Um auch symbolisch anzudeuten, dass es sich um eine Kongruenzrelation handelt, wählen wir in der Regel das Zeichen $\equiv$ (lies „cong"), eventuell mit Suffix.

Gilt lediglich $a \sim b \Longrightarrow s \circ a \sim s \circ b$, so nennen wir $\sim$ *linksverträglich*; auch eine *Linkskongruenz*.

Bezeichnen wir die Klassen $K(x)$ mit $\overline{x}$, so sieht man, dass *per definitionem* die Implikation

$$a \mapsto \overline{a} \;\&\; b \;\mapsto\; \overline{b} \quad\Longrightarrow\quad a \circ b \;\mapsto\; \overline{a} \cdot \overline{b} \tag{HI}$$

erfüllt ist. Ist ganz allgemein ein solcher Sachverhalt gegeben, so sprechen wir auch von einem *Homomorphismus.* Genauer:

8. 3. 2 Definition. Seien $\mathfrak{G} := (G, \circ)$ und $\mathfrak{H} := (H, \cdot)$ zwei Gruppoide. Dann bezeichnen wir als *Homomorphismus* von $\mathfrak{G}$ auf $\mathfrak{H}$ jede Abbildung h, die den Bedingungen genügt:

(HG) $$h(a \circ b) \;=\; h(a) \cdot h(b)\,.$$

Aus dieser Definition folgt unmittelbar, dass Gleichungen bei homomorphen Abbildungen „mitgehen" oder synonym, dass Homomorphismen Gleichungen mitnehmen bzw. *respektieren.*

DENN: Seien etwa $\mathfrak{R} = (R, \cdot, +)$ und $\mathfrak{S} = (R, \oplus, \odot)$ zwei Ringe und h ein Homomorphismus von $\mathfrak{R}$ auf $\mathfrak{S}$, so folgt gewissermaßen exemplarisch:

$$\begin{aligned} h\,(a) \odot (\,h(b) \oplus\; h\,(c)) \;&=\; h\,((a \cdot (b + c)\,) \\ &=\; h\,(a \cdot b + a \cdot c) \\ &=\; h\,(a) \odot h\,(b) \oplus h\,(a) \odot h\,(c)\,. \end{aligned}$$ □

Insbesondere gehen also bei Homomorphismen aufgrund der *Gleichungstreue idempotente Elemente* in Idempotente, *Einselemente* in Einselemente, *Inverse* in Inverse, *Nullen* in Nullen über etc.

Natürlich lässt sich der Begriff des Homomorphismus in kanonischer Weise auf beliebige Typen von Algebren übertragen, also auch etwa auf Gruppen, Ringe, Verbände oder Vektorräume.

Ihren Ursprung hat die Kongruenzrelation in der Zahlentheorie. „Wickelt" man nämlich – anschaulich gesprochen – die Gerade der ganzen Zahlen – o. B. d. A. im Uhrzeigersinn – derart um einen Kreis, dass die Zahl 0 und die Zahl m zusammenfallen, so liegen jeweils alle ganzen Zahlen, die zu der Zahl a den Abstand m haben, an der gleichen Stelle wie a, sind also in diesem Sinne kongruent mit a bzw. zueinander.

Wie man sofort sieht, lässt sich auf diesem *Ring* addieren, subtrahieren und multiplizieren wie auf der Geraden und, wie man weiter leicht bestätigt, gelten Gleichungen, die diesbezüglich in $\mathfrak{Z}$ gelten, auch in dem Ring $\mathfrak{Z}_m$.

Das bedeutet u. a., dass *infinite* Probleme möglicherweise zurückgeführt werden können auf *finite* Probleme.

So ist beispielsweise $p^2 = 2 \cdot q^2$ mit *teilerfremden* natürlichen Zahlen höchstens dann lösbar, wenn dies in jedem *Restklassenring* möglich ist. Es gilt aber in $\mathfrak{Z}_3$ die oben notierte Gleichung nur mit $\overline{p} = \overline{0} = \overline{q}$, also mit nicht teilerfremden natürlichen Zahlen p, q. Folglich ist die Zahl $\sqrt{2}$ *irrational*.

Sei hiernach ein Homomorphismus h des Gruppoids $\mathfrak{G}$ auf das Gruppoid $\mathfrak{H}$ gegeben. Dann stiftet h in natürlicher Weise eine Kongruenzrelation auf $\mathfrak{G}$ vermöge $a \equiv_h b \Longleftrightarrow h(a) = h(b)$, was sich fast unmittelbar ergibt.

Zusammen gefasst erhalten wir damit:

8. 3. 3 Theorem. *Ist $\mathfrak{G}$ ein Gruppoid, so erhalten wir bis auf Isomorphie alle homomorphen Bilder von $\mathfrak{G}$ als Restklassenstrukturen von $\mathfrak{G}$.*

Offenbar sind die bislang formulierten Sachverhalte unabhängig von der Struktur des Gruppoids. Denn alles bleibt gültig, wenn wir eine Algebra mit mehreren Operationen betrachten, und es dürfen diese Operationen beliebig n-stellig sein, also etwa auch einstellig wie $^{-1}$, wir brauchen ja lediglich die Forderung

$$a \equiv a' \;\&\; b \equiv b' \implies a \circ b \equiv a' \circ b' \tag{8.11}$$

umzuformulieren zu

$$a_i \equiv a_i' \Longrightarrow f(a_1, \ldots, a_i, \ldots, a_n) \equiv f(a_1, \ldots, a_i', \ldots, a_n)\,. \tag{8.12}$$

Aus diesen Überlegungen ergibt sich daher als Korollar:

8. 3. 4 Der Homomorphiesatz. *Ist $\mathfrak{A}$ eine Algebra, so erhalten wir – bis auf Isomorphie – alle homomorphen Bilder von $\mathfrak{A}$ als Restklassenstrukturen von $\mathfrak{A}$.*

8. 3. 5 Definition. Ein Homomorphismus von $\mathfrak{H}$ auf $\mathfrak{G}$ heißt ein *Endomorphismus,* wenn $H \supseteq G$ erfüllt ist, ein Homomorphismus heißt ein *Isomorphismus,* wenn die Abbildung h sogar bijektiv ist, ein Isomorphismus heißt ein *Automorphismus,* wenn $G = H$ erfüllt ist.

Neben dem Homomorphismus ist in der Allgemeinen Algebra das *Direkte Produkt* von fundamentaler Bedeutung. Sind $\mathfrak{A} = (A, \cdot)$ und $\mathfrak{B} = (B, \circ)$ zwei

Gruppoide, so lässt sich auf $A \times B$ in kanonischer Weise eine Multiplikation erklären *via*

$$\text{(CM)} \qquad (a_1 \mid b_1) \times (a_2 \mid b_2) \;:=\; (a_1 \cdot b_1 \mid a_2 \circ b_2)$$

Dies führt uns zum direkten Produkt $\mathfrak{G} \times \mathfrak{H} := (G \times H, \times)$.

Wiederum dient uns das Gruppoid als Prototyp, und es lässt sich ohne Probleme bei vorgegebenen Algebren $\mathfrak{A}_i \;\; (i \in I)$ gleichen Typs das direkte Produkt $\bigotimes \mathfrak{A}_i \;\; (i \in I)$ bilden.

Schließlich kommen wir zum Begriff der *Unteralgebra* , auch sie gehört zu den drei fundamentalen *Strukturoperatoren* der Allgemeinen Algebra.

8. 3. 6 Definition. Ist $\mathfrak{A}$ eine Algebra und ist $U \subseteq A$ *abgeschlossen* bezüglich der Operationen dieser Algebra, gilt also etwa im Falle des Gruppoids die Implikation $a, b \in U \Longrightarrow a \cdot b \in U$, so heißt (U, f_{iU}) eine Unteralgebra von $\mathfrak{A}$.

8. 3. 7 Beispiel. Als eine typische Konstruktion mittels der Operatoren S, P, H erwähnen wir hier die Konstruktion von $\mathbf{Q}$, ausgehend von $\mathbf{Z}$.

Die betrachteten Operationen sind *plus* und *mal.*

Wir starten von $\mathfrak{Z} = (\mathbf{Z}, +, \cdot)$, bilden das direkte Produkt $\mathfrak{Z} \times \mathfrak{Z}$, bilden hier die Unteralgebra der Paare $(a \,|\, b)$ mit $b \neq 0$ und betrachten sodann das homomorphe Bild zu $(a \,|\, b) \equiv (c \,|\, d) \Longleftrightarrow (ad = bc)$. Dies liefert uns $\mathbf{Q}$.

Wollen wir die Grundbegriffe der Allgemeinen Algebra und Ordnungstheorie didaktisch effizient bündeln, so bietet sich die Betrachtung des *Würfels* an. An seinem Modell lässt sich alles *in nuce* studieren, was für den angehenden Lehrer relevant sein dürfte.

Fassen wir vier parallele *Kanten* oder zwei parallele *Wände* als neue Objekte auf, so erhalten wir jeweils den vier- bzw. den 2-elementigen distributiven Verband als homomorphes Bild.

Auch sehen wir, dass es *genug* 2-elementige homomorphe Bilder gibt, d. h. zu jedem Paar a, b ein 2-elementiges homomorphes Bild, in dem a und b verschiedene Bilder erhalten.

Damit können wir – gewissermaßen exemplarisch – erklären, was man unter einer *subdirekten Zerlegung* einer Algebra versteht:

8. 3. 8 Definition. Sei $\mathfrak{A}$ eine Algebra und sei $\mathfrak{A}_i \ (i \in I)$ eine Familie von homomorphen Bildern von $\mathfrak{A}$.

Dann nennt man $\mathfrak{A}_i \ (i \in I)$ eine subdirekte Zerlegung von $\mathfrak{A}$ genau dann, wenn es zu jedem Paar a, b aus A ein $\mathfrak{A}_k \ (k \in I)$ gibt, in dem a und b verschiedene Bilder erhalten, kurz, wenn a und b durch $\mathfrak{A}_i \ (i \in I)$ getrennt werden.

Ist $\mathfrak{A}_i \ (i \in I)$ eine subdirekte Zerlegung von $\mathfrak{A}$, so können wir also jedes Element aus $\mathfrak{A}$ auffassen als eine Funktion von I nach $\bigcup A_i \ (i \in I)$ derart, dass das Bild von i jeweils in A_i liegt, und derart, dass den Operationsergebnissen an der i-ten Stelle jeweils die entsprechenden Operationsergebnisse aus $\mathfrak{A}_i$ zugeordnet werden.

8. 3. 9 Beispiel. Man betrachte $\mathfrak{Z} := (\mathbf{Z}, +, \cdot)$. Dann erkennt man leicht, dass $\mathfrak{Z}$ *subdirekt zerfällt* in $\mathfrak{Z}_m (m \in \mathbf{N})$.

8. 3. 10 Beispiel. Man betrachte die multiplikative Halbgruppe der ganzen Zahlen. Dann erkennt man, dass diese Halbgruppe subdirekt zerfällt in $\mathfrak{Z}_p \ (\mathfrak{Z}_p = (\mathbf{Z}, +)) \ (p \text{ prim})$.

8. 3. 11 Beispiel. Man betrachte etwa die additive Gruppe der *reellen*, der *stetigen*, der *differenzierbaren* Funktionen $\mathbf{R} \longmapsto \mathbf{R}$. Dann sieht man unmittelbar, dass diese Gruppen subdirekt zerfallen in *homomorpheBilder* $\mathfrak{R}_i$ vom Typ $(\mathbf{R}, +) \ (i \in I)$.

Ist $A_i \ (i \in I)$ eine subdirekte Zerlegung von $\mathfrak{A}$, so existiert aber zu dieser-Familie $\mathfrak{A}_i \ (i \in I)$ eine kanonisch korrespondierende Familie $\equiv_i \ (i \in I)$ und umgekehrt, so dass wir alle subdirekten Zerlegungen von $\mathfrak{A}$ auf dem Wege über Kongruenzrelationen mit Durchschnitt ι erhalten.

Sei hiernach $a \neq b$ ein Paar verschiedener Elemente aus $\mathfrak{A}$. Dann gibt es zumindest eine trennende Kongruenz auf $\mathfrak{A}$, nämlich ι.

Weiter sieht man leicht, dass mit einer aufsteigenden Folge von Kongruenzen auch deren mengentheoretische Vereinigung eine Kongruenz liefert. Das bedeutet aber, dass es unter den a und b trennenden Kongruenzen von $\mathfrak{A}$ nach dem ZORNschen Lemma mindestens eine *maximale* gibt, bezeichnet etwa mit $\equiv_{a,b}$.

Jede echte Oberkongruenz *führt* dann a und b *zusammen*.

Nun ist aber leicht zu sehen, dass jede Kongruenz $\overline{\theta}$ einer *Restklassenalgebra* $\overline{\mathfrak{A}} := \mathfrak{A}/_{\equiv}$ in kanonischer Weise eine Kongruenz auf $\mathfrak{A}$ induziert und zwar vermöge der definierenden Äquivalenz: $a\,\theta\,b :\Longleftrightarrow \overline{a}\ \overline{\theta}\ \overline{b}$.

Folglich führt jede echte Kongruenz von $\overline{\mathfrak{A}} := \mathfrak{A}/_{\equiv_{a,b}}$ die Elemente a und b zusammen.

8. 3. 12 Definition. $\mathfrak{A}$ heißt *subdirekt irreduzibel*, wenn es in A zwei verschiedene Elemente gibt, die von keiner echten Kongruenz getrennt werden.

Hiermit folgt dann nach dem bisherigen unmittelbar

8. 3. 13 Theorem. *Jede Algebra zerfällt subdirekt in subdirekt irreduzible Algebren (vom gleichen Typ).*

Das letzte Theorem weist auf die große Bedeutung subdirekt irreduzibler Algebren hin. So können wir uns z.B. bei der Behandlung des *Wortproblems* auf die Betrachtung subdirekt irreduzibler Vertreter beschränken.

Als Beispiel sei hier der distributive Verband genannt. Wie wir sofort sehen, ist jeder subdirekt irreduzible distributive Verband 2-elementig. Denn bildet $a < b$ ein *kritisches Paar*, so liefern die Homomorphismen $x \mapsto x \wedge b$ und $x \mapsto x \vee a$ je einen a und b *trennenden Homomorphismus,* also den identischen Homomorphismus, weshalb a als Minimum und b als Maximum dieses Verbandes fungiert. Liegt nun c zwischen a und b, so können wir analog $x \mapsto x \wedge c$ betrachten, wodurch a und b wieder getrennt werden, weshalb das betrachtete c gleich a oder gleich b sein muss. Das liefert dann auf neue Weise, dass sich jeder distributive Verband auffassen lässt als ein Verband von 0-1-Folgen und damit als ein Verband von Mengen.

Also brauchen wir für Terme $t\,[x_1, \ldots, x_n],\ s\,[x_1, \ldots, x_n]$ lediglich alle (0,1)-Belegungen zu *testen*, um zu ermitteln, ob diese beiden Terme für jede Belegung den gleichen Wert liefern.

Wir gehen noch kurz auf den Verband der Kongruenzen unter Berücksichtigung der Verkettung ein.

Wie man sofort sieht, ist der Durchschnitt einer Familie von Kongruenzrelationen wieder eine Kongruenzrelation und ebenso das Supremum zweier Kongruenzrelationen, betrachtet als Äquivalenzrelationen, wieder eine Kongruenzrelation.

DENN: $a\,(\theta_1 \vee \theta_2)\,b$ ist gleichbedeutend mit der Existenz von Elementen $x_1, \ldots, x_n$ mit

$$a\ \theta_1\ x_1\ \theta_2\ x_2\ \theta_1\ x_3\ \theta_2\ \ldots\ \theta_2\ x_n = b$$

und hieraus folgt für das Gruppoid durch Multiplikation von links bzw. rechts unmittelbar, dass mit $\theta_1\,,\ \theta_2$ auch $\theta_1 \circ \theta_2$ eine Kongruenzrelation ist.

Schreiben wir allgemein $f(a_1, \ldots, a_2)$ anstelle von $a_1 \cdot a_2$, so erkennen wir, dass sich unsere speziellen Überlegungen übertragen, und das bedeutet:

8. 3. 14 Proposition. *Der Verband der Kongruenzen einer Algebra ist algebraisch.*

HINWEIS: In einem Kapitel über Verbände haben wir gesehen, dass es keine anderen algebraischen Verbände gibt als die Verbände der Ideale von Halbverbänden bzw. als die Verbände von Unteralgebren einer Algebra.

Doch es gilt mehr, nämlich, was wir hier nur hinnehmen wollen:

8. 3. 15 The celebrated Theorem of Grätzer&Schmidt. *Es gibt keine anderen algebraischen Verbände als die Kongruenzverbände von Algebren.*

Als eine der ganz großen Herausforderungen der abstrakten Algebra sei an dieser Stelle formuliert:

PROBLEM: Ist jeder endliche Verband Kongruenzverband einer endlichen Algebra ?

8.4 Vertauschbarkeit und Distributivität

So reizvoll das genannte Resultat und so herausfordernd dieses Problem aber auch sein mögen, relevanter sind Einsichten über Kongruenzen, von denen hier einige vorgestellt seien.

Ein Exempel für vertauschbare Kongruenzrelationen liefert die Gruppe.

DENN: Ist $\mathfrak{G}$ eine Gruppe und sind $\theta_1\,,\ \theta_2$ zwei Kongruenzen auf $\mathfrak{G}$, so gilt:

$$a\ \theta_1\ x\ \theta_2\ b \Longrightarrow a\ \theta_2\ a \cdot x^{-1} \cdot b\ \theta_1\ b\,.$$

Demzufolge sind je zwei Kongruenzen immer dann vertauschbar, wenn sich aus den vorgegebenen Operationen eine Gruppenoperation *komponieren* lässt.

Die Vertauschbarkeit von Kongruenzen ist höchst relevant für das Verhalten allgemeiner Algebren. Dies sei erläutert an einem Beispiel.

Sei $\mathfrak{R}$ ein kommutativer Ring mit 1. Dann ist mit $u = u^2$ auch $v := 1 - u$ idempotent, wegen $v^2 = (1-u)^2 = 1-u-u+u^2 = 1-u = v$. Wir definieren nun $a \mapsto au$. Dann sieht man leicht, dass dies ein Homomorphismus von $\mathfrak{R}$ auf $\mathfrak{R} \cdot u$ also von $\mathfrak{R}$ in $\mathfrak{R}$ und damit ein *Endomorphismus* ist. Definieren wir nun weiter $a \mapsto av$, so erhalten wir ein zweites homomorphes Bild von $\mathfrak{R}$.

Die korrespondierenden Homomorphismen sind dabei θ_u und θ_v – definiert vermöge der Äquivalenz: $a\,\theta_u\,b \iff au = bu$ und $a\,\theta_v\,b \iff av = bv$.

Weiter sehen wir, dass $a\,\theta_u\,b \;\&\; a\,\theta_v\,b \implies a = b$ erfüllt ist und ebenso die Gleichung $a\,\theta_u\,(au + bv)\,\theta_v\,b$. Demzufolge erfüllen die von u und v erzeugten Kongruenzen θ_u und θ_v die Bedingungen:

$$\begin{aligned} &(i) && \theta_u \cap \theta_v &&= \iota \\ &(ii) && \theta_u \circ \theta_v &&= \theta_v \circ \theta_u \\ &(iii) && \theta_u \vee \theta_v &&= \omega\,. \end{aligned}$$

Diese drei Gleichungen sind nun in der Tat dafür *verantwortlich*, dass die beiden homomorphen Bilder $\mathfrak{R}/_{\theta_\mathfrak{u}}$ und $\mathfrak{R}/_{\theta_\mathfrak{v}}$ eine *Koordinatisierung* von $\mathfrak{R}$ liefern.

Wir führen dies nacheinander zunächst konkret und danach abstrakt vor.

KONKRET: Ordne jedem $a \in R$ als 2-tupel das Paar (au, av) zu. Dann erhält jedes a ein *Koordinatenpaar* (au, av), je zwei verschiedene Elemente a und b erhalten verschiedene Koordinatenpaare und schließlich wird jedes Paar (au, bv) als Bild, etwa von $au + bv$ berücksichtigt. Darüber hinaus gilt

$$ab \longmapsto (au \cdot bu\,,\; av \cdot bv) \text{ und } a + b \longmapsto (au + bu\,,\; av + bv)$$

das heißt, es entsprechen den Operationen in $\mathfrak{R}$ die *Stellenoperationen* in $\mathfrak{R}/_{\theta_\mathfrak{u}} \times \mathfrak{R}/_{\theta_\mathfrak{v}}$.

Damit haben wir unsere komplexere Algebra zurückgeführt auf zwei schlichtere Strukturen.

ABSTRAKT: Ordne jedem $a \in R$ als 2-tupel das Paar $(a\,\theta_u\,,\; a\,\theta_v)$ zu. Dann erhält jedes a ein Koordinatenpaar $(a\,\theta_u\,,\; a\,\theta_v)$, je zwei verschiedene Elemente a und b erhalten verschiedene Koordinatenpaare und schließlich wird jedes Paar $(a\,\theta_u\,,\; b\,\theta_v)$ als Bild erfasst. Eine Situation, die sich anschaulich erfassen lässt mittels der Abbildung 8.1

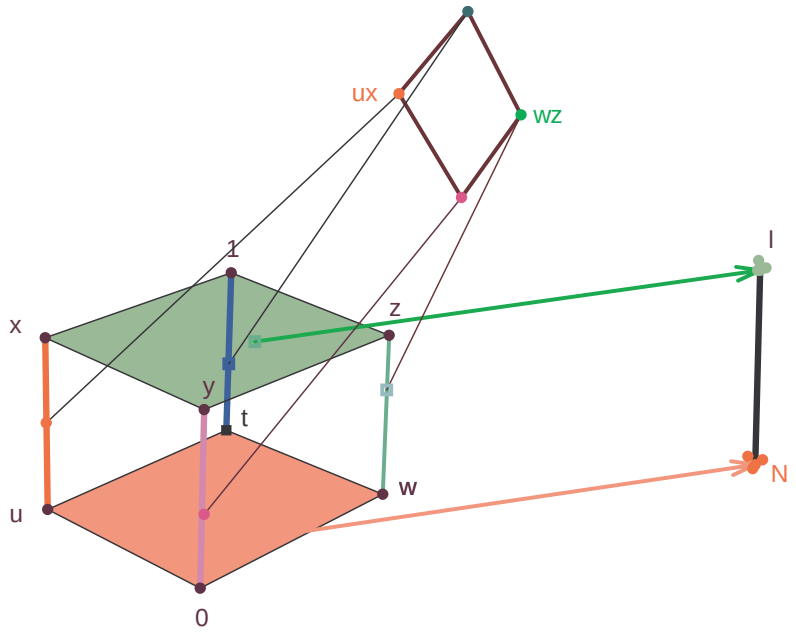


Abbildung 8.1: Zur (sub-) direkten Zerlegung

DENN: Da θ_u und θ_v vertauschbar sind, ist $\theta_u \circ \theta_v = \theta_u \vee \theta_v$ und da $\theta_u \vee \theta_v$ die Allrelation ist, existiert dann ein x mit

$$a\,\theta_u\,x \;\&\; x\,\theta_v\,b\,,$$

also mit $x\,\theta_u = a\,\theta_u$ und $x\,\theta_v = b\,\theta_v$.

Wie der Leser sofort sieht, besagt das letzte Beispiel u.a., dass subdirekt irreduzible Ringe mit 1 höchstens zwei Idempotente, nämlich 1 und 0 besitzen.

Das liefert uns insbesondere , dass subdirekt irreduzible Boolesche Algebren 2-elementig sind, und damit als Nebenprodukte die bereits in [6] bzw. oben bewiesenen Sachverhalte:

8. 4. 1 Korollar. *Das Wortproblem für Boolesche Algebren lässt sich mittels Tafeltests lösen.*

8. 4. 2 Korollar. *Jede Boolesche Algebra lässt sich auffassen als eine Boolesche Algebra von* $0,1$*-Folgen und damit als ein Mengenkörper.*

Als nächstes zeigen wir:

8. 4. 3 Proposition. *Ist* $\mathfrak{A}$ *kongruenzvertauschbar, so ist* $\mathfrak{A}$ *auch kongruenzmodular.*

BEWEIS. Seien θ_1 , θ_2 , θ_3 Kongruenzen auf $\mathfrak{A}$ und gelte $\theta_1 \supseteq \theta_3$. Es ist zu zeigen

$$\theta_1 \cap (\theta_2 \vee \theta_3) \subseteq (\theta_1 \cap \theta_2) \vee \theta_3 .$$

Sei also

$$(a, b) \in \theta_1 \cap (\theta_2 \vee \theta_3) .$$

Zur Erinnerung: wegen der Vertauschbarkeit gilt $\circ = \vee$, insbesondere existiert daher wegen $\theta_2 \vee \theta_3 = \theta_2 \circ \theta_3$ ein c mit $a\,\theta_2\,c\,\theta_3\,b$. Folglich gilt aufgrund der Symmetrie auch $b\,\theta_3\,c$, also wegen $\theta_1 \supseteq \theta_3$ auch $b\,\theta_1 c$. Hieraus folgt aber aufgrund der Transitivität $a\,\theta_1 c$. Folglich haben wir $a\,(\theta_1 \cap \theta_2)\,c$, und $c\,\theta_3\,b$ und damit dann auch $a\,(\theta_1 \cap \theta_2) \circ \theta_3\,b$ also

$$(a, b) \in (\theta_1 \cap \theta_2) \vee \theta_3 .$$

Damit sind wir am Ziel □

Als ein weiteres Beispiel einer Algebra mit einer Gruppenoperation und möglicherweise unendlich vielen einstelligen Operationen sei der Vektorraum erwähnt. Erneut, wir brauchen ja lediglich die Skalare zu begreifen als 1-stellige Operatoren im Sinne von $f_s(\mathfrak{a}) := s\mathfrak{a}$.

Da jeder Vektorraum Träger einer Gruppenoperation ist, sind je zwei Kongruenzen vertauschbar und somit ist der Verband der Kongruenzrelationen eines Vektorraumes stets modular. Weiterhin ist ein Vektorraum subdirekt irreduzibel, wenn er die Dimension 1 hat, klar. Und schließlich können wir die Unterräume eines Vektorraumes identifizieren mit seinen Kongruenzen *via*

$$\mathfrak{a} \equiv \mathfrak{b} \ (U) :\Longleftrightarrow \mathfrak{a} - \mathfrak{b} \in U .$$

Dies liefert uns den Satz der linearen Algebra, dass die Unterräume eines Vektorraumes einen modularen Verband bilden.

Ebenso relevant wie die Vertauschbarkeit der Kongruenzen ist im gegebenen Fall die Distributivität eines Kongruenzrelationen-Verbandes.

Prototyp einer Algebra mit distributivem Kongruenzrelationen-Verband ist der Verband. Um dies zu zeigen, gehen wir aus von einem Verband $\mathfrak{V}$ und drei Kongruenzen θ_1, θ_2, θ_3. Zu beweisen ist dann

$$\theta \cap (\theta_1 \vee \theta_2) \subseteq (\theta \cap \theta_1) \vee (\theta \cap \theta_2) . \tag{8.17}$$

Sei also $(a, b) \in \theta \cap (\theta_1 \vee \theta_2)$ erfüllt. Dann folgt

$$a\ \theta\ b\ \&\ a\ \theta_1\ x_1\ \theta_2\ x_2\ \theta_1\ x_3\ \theta_2\ x_4\ \theta_1\ x_5\ \ \ldots\ \ \theta_2\ b .$$

Weiter sehen wir

$$\begin{array}{ccccc} a\ \theta\ b & & a\wedge x\ \theta\ b\wedge x & & a\ \theta\ a\vee(b\wedge x)\\ \& & \Longrightarrow & \& & \Longrightarrow & \&\\ a\,\theta_1\,x & & b\wedge a\ \theta_1\, b\wedge x & & a\ \theta_1\, a\vee(b\wedge x)\end{array}$$

Das bedeutet aber

$$a\ (\theta\wedge\theta_1)\ a\vee(b\wedge x) \tag{8.18}$$

Setzen wir nun $y_i := a\vee(b\wedge x_i)$, so erhalten wir

$$a\ \theta_1\ y_1\ \theta_2\ y_2\ \theta_1\ y_3\ldots\ldots\ldots\ \theta_1\ y_n = a\vee b \tag{8.19}$$

$$a\ \theta\ \ y_1\ \theta\ \ y_2\ \theta\ \ y_3\ldots\ldots\ldots\ \theta\ \ y_n = a\vee b \tag{8.20}$$

und damit

$$a\ (\theta\cap\theta_1)\ y_1\ (\theta\cap\theta_2)\ y_2\ (\theta\cap\theta_1)\ y_3\ldots\ldots\ldots\ (\theta\cap\theta_1)\ y_n = a\vee b\,, \tag{8.21}$$

also

$$a\ \ (\theta\cap\theta_1)\vee(\theta\cap\theta_2)\ \ a\vee b\,, \tag{8.22}$$

was aus Gründen der Dualität zu

$$a\ \ (\theta\cap\theta_1)\vee(\theta\cap\theta_2)\ \ b \tag{8.23}$$

und damit zu (8.17) führt.

Ist eine Algebra nun sowohl Gruppe als auch Verband, wie etwa die *Verbandsgruppe* oder die *Boolesche Algebra,* so erfüllt sie beide Bedingungen. In solchen Fällen sprechen wir von einer *arithmetischen Algebra.*

Sind sogar alle Algebren eines bestimmten Typs arithmetisch, so sprechen wir von einer *arithmetischen Varietät.*

Betrachten wir noch einmal die Varietät der Gruppen. Wir sehen sofort, dass es weniger auf den speziellen *Ausdruck* $a\cdot x^{-1}\cdot b$ ankommt als vielmehr auf die Existenz eines Ausdrucks $p\,[\,x,y,z\,]$ mit

$$p\,[x,z,z] = x\ \&\ p\,[x,x,z] = z$$

der gleich b wird, wenn a gleich x gewählt wird, und gleich a, wenn b gleich x gewählt wird.

Einen solchen Ausdruck nennt man auch ein *Mal'cev-Polynom*, zu Ehren des russischen Mathematikers I.A. MAL'CEV, der als erster zeigte, dass für die Kongruenzvertauschbarkeit einer Varietät die Existenz eines Polynoms der oben vorgestellten Art nicht nur hinreicht, sondern sogar notwendig ist.

Ähnliches gilt für den Term $(x \vee y) \wedge (y \vee z) \wedge (z \vee x)$. $=: m\,[x, y, z]$. Was wir tatsächlich nur heranziehen ist die Besonderheit:

$$m\,[x, x, a] = m\,[x, a, x] = m\,[a, x, x] = x\,.$$

Ist dieser Sachverhalt für irgendein Polynom erfüllt, so ist Kongruenzdistributivität gesichert. Man wähle etwa jeweils $m\,[a, b, x_i]$ statt $a \vee (b \wedge x_i)$. Allerdings, die Existenz eines Terms der gewünschten Art ist nicht notwendig.

Ist aber eine Varietät *kongruenzvertauschbar* und *kongruenzdistributiv*, und damit *arithmetisch*, so existiert stets ein Polynom $m\,[x, y, z]$ mit der Eigenschaft

$$m\,[x, x, a] = m\,[x, a, x] = m\,[a, x, x] = x\,.$$

Ja noch mehr: Es gibt ein Polynom, das charakteristisch ist für arithmetische Varietäten, nämlich das *Pixley-Polynom* $q\,[x, y, z]$ mit

$$q\,[z, x, z] = q\,[x, x, z] = q\,[z, x, x] = z\,.$$

Wir zeigen hier nur, dass die Existenz eines $q\,[x, y, z]$ von der genannten Art sich komponieren lässt aus den Polynomen $p\,[x, y, z]$ und $m\,[x, y, z]$ und umgekehrt.

Dass die hier genannten Polynome tatsächlich existieren, weist man nach mit Methoden der Universellen Algebra, könnte aber auch in diese Veranstaltung eingebaut werden. Der interessierte Leser konsultiere etwa BURRIS-SANKAPPANAVAR, [8].

Sei also zunächst $p\,[x, y, z]$ und $m\,[x, y, z]$ im Sinne des Satzes gegeben. Wir wählen $q\,[x, y, z] := p\,[x, m\,[x, y, z], z]$.

Sei hiernach ein $q\,[x, y, z]$ im Sinne des Satzes gegeben. Dann haben wir schon ein $p\,[x, y, z]$, nämlich q, und wir erhalten ein $m\,[x, y, z]$ vermöge der Festsetzung $q\,[x, q\,[x, y, z], z]$, was der Leser durch Einsetzen bestätigt.

Als den Klassiker schlechthin aller arithmetischen Varietäten nennen wir hier die Klasse der kommutativen Ringe mit 1, die der Bedingung genügen

TO CONTAIN IS TO DIVIDE

Genauer halten wir fest:

8. 4. 4 Proposition. *Ein kommutativer Ring mit 1 ist arithmetisch gdw. seine endlich erzeugten Ideale der Implikation genügen:* $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \,|\, \mathfrak{b}$.

Es ist demnach die Teilbarkeitsforderung $\mathfrak{a} \supseteq \mathfrak{b} \Longrightarrow \mathfrak{a} \,|\, \mathfrak{b}$ eine rein kongruenztheoretische Forderung, und es führt diese Forderung zu Teilbarkeitsverhältnissen in $\mathfrak{R}$ wie sie besser nicht sein könnten. studiere - etwa - [7].

Kapitel 9

Allgemein Geometrisches

Die nachfolgenden Ausführungen sind in enger inhaltlicher und stilistischer Anlehnung an die Darstellung der verbandstheoretischen Charakterisierung kontinuierlicher Geometrien des „Jahrhundert-Mathematikers" JOHN VON NEUMANN in der empfehlenswerten Monographie [22] der Verbandstheorie von HANS HERMES verfasst. Man beachte vor allem die kombinatorischen Aspekte dieses Kapitels.

9.1 Lineare Teilräume

In der Geometrie spielt seit PONCELET das Begriffspaar des *Schneidens* und *Verbindens* eine zentrale Rolle.

Betrachten wir den $\mathbf{R}^3$. Sind hier zwei verschiedene Geraden g und h gegeben, so besitzen sie genau einen gemeinsamen Punkt P oder aber keinen gemeinsamen Punkt. Im ersten Fall setzen wir $g \wedge h = P$ und sagen, dass sich g und h in P *schneiden*.

Im zweiten Fall aber ist der mengentheoretische Durchschnitt von g und h – aufgefasst als Mengen – gleich der leeren Menge ℓ, also $g \cap h = \ell$ und wir setzen $g \wedge h = \ell$.

Ist in diesem Falle g parallel zu h, so bestimmen g und h erneut eine Ebene E als engsten g und h umfassenden Teilraum, d.h. es gilt erneut $g \vee h = E$. Andernfalls aber ist $\mathbf{R}^3$ selbst der engste g und h umfassende Teilraum, und wir setzen $g \vee h = \mathbf{R}^3$.

Es zeigt sich, dass die Menge der linearen Teilräume von $\mathbf{R}$ in bezug auf die soeben eingeführten Operationen $\wedge$ und $\vee$ einen Verband bildet. Wir werden

erwarten dürfen, einen besonders einfachen Verband zu erhalten, wenn wir nicht, wie in diesem Falle, einen affinen, sondern einen *projektiven* Raum R zugrunde legen – und zwar wegen der Selbstdualität projektiver Räume. Das soll im folgenden geschehen.

Wir wollen dabei die projektiven Räume geometrisch charakterisieren durch Forderungen, die im wesentlichen mit den klassischen Axiomen übereinstimmen, die von VEBLEN und YOUNG[1)] herausgestellt worden sind.

Allerdings soll auf zwei Annahmen in unseren allgemeinen Überlegungen verzichtet werden, die normalerweise in der Geometrie gemacht werden:

1. Wir wollen die Dimension keinen Einschränkungen unterwerfen.

2. Wir wollen nicht voraussetzen, dass auf jeder Geraden mindestens drei Punkte liegen.

Wenn wir diese Forderungen nachträglich adjungieren, lassen sich die erzielten allgemeinen Ergebnisse mühelos spezialisieren.

Die Überlegungen, die wir in diesem und im nächsten Paragraphen anstellen, werden uns zu den folgenden Ergebnissen führen:

> **Die Verbände der linearen Teilräume der projektiven Räume lassen sich rein verbandstheoretisch charakterisieren. Sie stimmen überein mit den algebraischen, atomaren, modularen, komplementären Verbänden. Man kann diese Verbände in einem noch zu präzisierenden Sinne mit den projektiven Räumen identifizieren.**

In der damit gewonnenen *rein verbandstheoretischen Charakterisierung der projektiven Geometrie* treten als einzige Grundbegriffe $\wedge$ und $\vee$ auf, d. h., genau die fundamentalen Begriffe des Schneidens und Verbindens. Aufgrund dieser Tatsache darf man die angegebene Charakterisierung als eine besonders geglückte Festlegung des Begriffs der *projektiven Geometrie ansehen.*

Wir haben es hier nur mit jenen geometrischen Sätzen zu tun, die sich mit dem Schneiden und Verbinden befassen, also mit den Sätzen der sogenannten *Verknüpfungsgeometrie.* Jeder Satz der Verknüpfungsgeometrie kann demnach aufgefasst werden als ein Satz über die genannten speziellen modularen

[1)] Vgl. VEBLEN-YOUNG, Projective Geometry, 2 vols. Boston 1910/1917, letzter Druck 1938/1946.

Verbände. Dieser Tatsache war man sich unausgesprochen schon immer bewusst. Das zeigt die Geschichte der projektiven Geometrie, in der man Sätze über Verbände, insbesondere auch über modulare Verbände, in geometrischer Einkleidung gewonnen hat, lange Zeit bevor sie explizit verbandstheoretisch formuliert worden sind. Wir nennen als Beispiele das geometrische Dualitätsprinzip und den Dimensionssatz der projektiven Geometrie.

BEGINNEN WIR MIT DER AUSFÜHRUNG des skizzierten Programms. Zunächst wollen wir eine axiomatische Festlegung des Begriffs der *projektiven Geometrie* formulieren[2)]. Eine projektive Geometrie G ist gegeben durch zwei elementfremde Mengen und eine Relation, in der ein Element der ersten Menge zu einem Element der zweiten Menge stehen kann. Die Elemente der ersten Menge nennen wir *Punkte*, die Menge aller Punkte den zu G gehörigen *projektiven Raum* $R(G)$. Die Elemente der zweiten Menge heißen *Geraden*. Wenn ein Punkt α zu einer Geraden g in der für die projektive Geometrie grundlegenden Relation steht, so wollen wir sagen, dass α *auf* g *liegt*. Synonym verwenden wir die Redeweise: g *geht durch* α. g *und* h *schneiden sich*, wenn es einen Punkt α gibt, der zugleich auf g und h liegt. Wir nennen α, β, γ *kollinear*, wenn es eine Gerade g gibt, auf der diese Punkte liegen. Die Kollinearität von α, β, γ drücken wir abkürzend aus durch $\alpha\beta\gamma$. Wir sprechen erst dann von einer *projektiven Geometrie*, wenn drei *Axiome* (P0), (P1), (P2) gelten. Von diesen werden wir aber zunächst nur die beiden letzten heranziehen.

Wenn diese gültig sind, wollen wir von einer *verallgemeinerten projektiven Geometrie* sprechen. Inhaltlich besagen (P1) und (P2):

(P1) Zwei verschiedene Punkte liegen stets auf einer und nur einer Geraden, sowie

(P2) $\alpha^\circ \beta\, \gamma \;\&\; \alpha\, \beta^\circ \gamma \Longrightarrow \exists \gamma^\circ : \alpha\, \beta\, \gamma^\circ \;\&\; \alpha^\circ\, \beta^\circ\, \gamma^\circ$.

Anstelle dieses Axioms (P2) findet man häufig eine Formulierung (P2*), die besagt, dass (P2) gelten soll, wenn α, β, γ nicht kollinear sind. Man kann sich aber leicht davon überzeugen, dass aus (P1), (P2*) die Gültigkeit von (P2) geschlossen werden kann. Es ist dazu zu zeigen, dass (P2) auch unter der Voraussetzung gilt, dass α, β, γ kollinear sind, also auf einer Geraden g liegen.

[2)] In der Literatur spricht man oft von einem *projektiven Raum*, wenn wir von einer projektiven Geometrie sprechen. In der hier gewählten Terminologie ist der zu einer projektiven Geometrie gehörige projektive Raum durch die Menge aller Punkte der projektiven Geometrie gegeben.

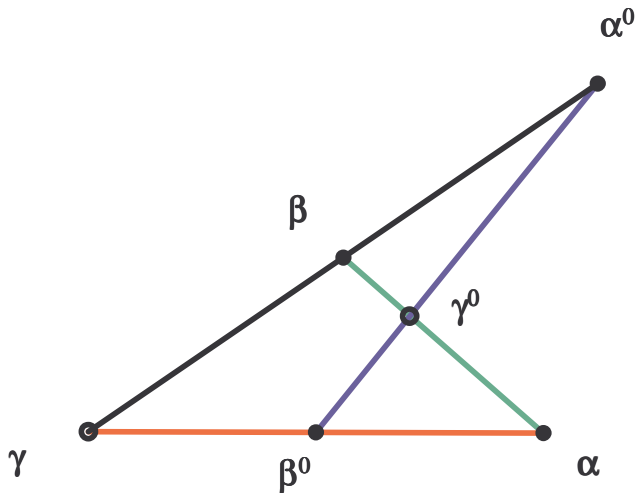


Abbildung 9.1: Basis-Relation

Sei zunächst $\beta \neq \gamma$. Dann bestimmen β und γ die Gerade g, so dass α° auf g liegt. Dann leistet $\gamma^\circ = \alpha^\circ$ das Verlangte. Es liegen dann nämlich α, β und α° auf g, woraus vorab $\alpha\beta\gamma^\circ$ resultiert;

Falls nun zusätzlich $\alpha^\circ \neq \beta^\circ$ erfüllt ist, so liegen α° und β° auf $\alpha^\circ\beta^\circ$, so dass auch $\alpha^\circ\beta^\circ\gamma^\circ$ erfüllt ist.

Gilt aber zusätzlich $\alpha^\circ = \beta^\circ$, so liegt auch β° auf g, weshalb auch in diesem Falle $\alpha^\circ\beta^\circ\gamma^\circ$ resultiert.

Analog schließt man im Falle $\alpha \neq \gamma$.

Bleibt der Fall $\alpha = \gamma$ und $\beta = \gamma$. Dann gilt $\alpha = \beta = \gamma$, und $\gamma^\circ = \alpha^\circ$ erfüllt die Forderungen, wie man ohne Schwierigkeiten erkennt. □

Im folgenden wollen wir die nach (P1) durch zwei verschiedene Punkte α, β bestimmte Gerade mittels $\alpha\beta$ symbolisieren. Dan gilt natürlich $\alpha\beta = \beta\alpha$.

Aus $\alpha\beta\gamma$ *und* $\alpha \neq \beta$ *ergibt sich, dass* γ *auf* $\alpha\beta$ *liegt.* α, β und γ liegen ja auf einer Geraden g, und diese Gerade muss nach (P1) mit $\alpha\beta$ übereinstimmen.

9. 1. 1 Definition. Sei G sei eine verallgemeinerte projektive Geometrie. Dann heißt eine Teilmenge x von $R(G)$ ein *linearer Teilraum* von G, wenn für je zwei verschiedene Punkte $\alpha, \beta \in x$ und jeden Punkt γ, der auf $\alpha\beta$ liegt, auch γ zu x gehört.

Wir geben einige Beispiele für lineare Teilräume:

(a) Die leere Menge ℓ und die *einpunktigen Mengen* sind lineare Teilräume, da es in ihnen nicht zwei verschiedene Punkte gibt, und daher die in der Definition ausgesprochene Forderung trivialerweise erfüllt ist.

(b) Die Menge $R(G)$ ist ein linearer Teilraum, da γ stets zu $R(G)$ gehört.

(c) Jede Menge $[g]$ aller Punkte, die auf einer Geraden g liegen, ist ein linearer Teilraum. Sind nämlich α, β verschiedene Punkte von g und liegt γ auf $\alpha\beta$, so liegt γ auf g, da $g = \alpha\beta$ ist nach (P1).

In diesem Abschnitt werden wir die Menge der linearen Teilräume einer verallgemeinerten projektiven Geometrie charakterisieren. Bevor wir hier in die Einzelheiten gehen, erinnern wir an 8.1.7, d. h. an den Satz für nach oben gerichtete Mengen B algebraischer Verbände, der besagt:

$$L := a \cap \bigvee(b_i \in B) = \bigvee(a \cap b_i) \ \ (b_i \in B) =: R \ .$$

Wie üblich bezeichnen wir im weiteren die oberen Nachbarn der 0 als *Atome* und die oberen Nachbarn der Atome als *Hyperatome.* Weiter nennen wir einen Verband *atomar,* wenn jedes von 0 verschiedene Element mindestens ein Atom enthält.

Hiernach beweisen wir:

9. 1. 2 Proposition. *Die Menge der linearen Teilräume einer verallgemeinerten projektiven Geometrie G bildet in bezug auf die mengentheoretische Schnittbildung und die Erzeugnisbildung $\bigvee$ einen $\bigvee$-algebraischen, atomaren Verband $\mathfrak{V}(G)$. Dabei stimmen die Atome überein mit den einpunktigen Mengen.*

BEWEIS. Die Algebraizität folgt unmittelbar daraus, dass eine Teilmenge genau dann ein linearer Teilraum T von G ist, wenn sie abgeschlossen ist bezüglich der Relation

$$R(\alpha, \beta\,\gamma) :\Longleftrightarrow \alpha\beta\gamma \ \&\ \alpha, \beta \subseteq T \ .$$

Dass jede einpunktige Menge ein linearer Teilraum ist, haben wir bereits gesehen. Eine solche Menge ist ein Atom, da sie als Teilraum von $R(G)$ nur die leere Menge echt enthält. Ein mehrpunktiger Teilraum besitzt jedes $\{\alpha\}$ seiner Punkte α als echten Teilraum, kann also kein Atom sein. Diese Überlegung zeigt, dass $\mathfrak{V}(G)$ atomar ist. □

Für das Folgende benötigen wir zunächst einen Hilfssatz, der die Vereinigung zweier linearer Teilräume charakterisiert.

9. 1. 3 Der Verbindungssatz. *Seien a, b zwei Teilräume und gelte $\ell \neq a \neq b \neq \ell$. Dann besteht die Vereinigung $a \vee b$ zweier linearer Teilräume a, b von $\mathfrak{V}(G)$ aus denjenigen Punkten, die auf Geraden des Typs $\alpha\beta$ mit $\alpha \subseteq a$ & $\beta \subseteq b$ $(\alpha \neq \beta)$ liegen*[3)].

BEWEIS. Sei die Voraussetzung erfüllt und sei x die Menge der Punkte, die auf wenigstens einer der genannten Verbindungsgeraden liegen. Da $a \vee b$ definitionsgemäß der kleinste a und b umfassende lineare Teilraum ist, genügt es, die drei folgenden Sachverhalte zu verifizieren:

(1) $x \subseteq a \vee b$,

(2) $a \subseteq x,\ b \subseteq x$,

(3) x ist ein linearer Teilraum.

Zu (1). Jeder Punkt von a und jeder Punkt von b gehört zu $a \vee b$, also nach Definition der linearen Teilräume auch jeder Punkt von x.

Zu (2). Es genügt zu zeigen, dass jeder Punkt $\alpha \in a$ zu x gehört. Dies lässt sich aufgrund der Voraussetzung wie folgt einsehen:

Wenn $b = \{\alpha\}$ ist, so gibt es wegen $a \neq b$ in a einen weiteren Punkt $\alpha' \neq \alpha$, und α liegt auf der Verbindungsgeraden $\alpha'\alpha$ des Punktes α' von a und des Punktes α von b, also in x. Wenn aber $b \neq \{\alpha\}$ ist, so gibt es in b ein $\beta \neq \alpha$, und α liegt auf $\alpha\beta$, also wieder in x.

Zu (3). Man hat zu zeigen, dass x mit zwei verschiedenen Punkten μ, ν jeden beliebigen Punkt ϱ von $\mu\nu$ enthält. Zunächst betrachten wir den *Sonderfall*, dass wenigstens einer der Punkte μ, ν in a oder in b liegt. Wir dürfen uns auf die Annahme $\mu \in a$ beschränken.

Zu $\nu \in x$ gibt es ein $\alpha \in a$ und ein $\beta \in b$, so dass $\alpha \neq \beta$ und $\alpha\beta\nu$ erfüllt sind.

Und damit erhalten wir nach (P2) ein σ mit:

$$(1)\ \alpha\beta\nu\ \&\ (2)\ \varrho\mu\nu \Longrightarrow (3)\ \alpha\mu\sigma\ \&\ (4)\ \varrho\beta\sigma\,.$$

Gilt nun $\alpha = \mu$, so haben wir nach (1) und (2) $\alpha\nu\beta$ und $\alpha\nu\varrho$. Dies bedeutet, dass β und ϱ auf Geraden $\alpha\nu = \mu\nu$ liegen; auf dieser Geraden liegt auch α; damit haben wir $\alpha\beta\varrho$, also $\varrho \in x$.

[3)] Man veranschauliche sich die Aussage des Verbindungssatzes an den linearen Teilräumen des dreidimensionalen Raumes!

Gilt aber $\alpha \neq \mu$, so liegt wegen (3) σ in a. Hieraus folgt für $\sigma \neq \beta$ aus (4), dass $\varrho \in x$. Falls aber $\sigma = \beta$, so ergibt sich der Reihe nach $\beta \in a$, $\nu \in a$ (1), $\varrho \in a$ (2), also $\varrho \in x$.

Hiernach behandeln wir den allgemeinen Fall, also den Fall, in dem weder μ noch ν in a oder in b liegen.

Zu $\nu \in x$ gibt es ein $\alpha \in a$ und ein $\beta \in b$, so dass $\alpha \neq \beta$ und $\alpha\beta\nu$ ist.

Und damit erhalten wir nach (P2) ein σ mit:

$$(5)\ \alpha\beta\nu\ \&\ (6)\ \varrho\mu\nu \Longrightarrow (7)\ \alpha\mu\sigma\ \&\ (8)\varrho\beta\sigma$$

Aus $\alpha\mu\sigma$ folgt wegen $\alpha \neq \mu$ nach dem Sonderfall, dass $\sigma \in x$, und wieder nach dem Sonderfall aus $\varrho\sigma\beta$, dass im Falle $\sigma \neq \beta$ der Punkt ϱ in x liegt. Wenn aber $\sigma = \beta$ ist, so liegen μ (wegen (7)) und ν auf $\alpha\beta$, so dass $\alpha\beta = \mu\nu$ nach (P1) erfüllt ist. ϱ liegt auf $\mu\nu$, also auf $\alpha\beta$. Dies zeigt dann, dass auch in diesem Falle ϱ in x liegt. □

9. 1. 4 Proposition. *Der Verband $\mathfrak{V}(G)$ ist modular und komplementär.*

BEWEIS. (a) $\mathfrak{V}(G)$ ist modular,

DENN: Sei $a \subseteq c$ erfüllt. Dann ist

$$(a \vee b) \wedge c \subseteq a \vee (b \wedge c)$$

zu verifizieren. Dies ist klar im Falle $a = \ell$ oder $b = \ell$ oder $a = b$. Deshalb dürfen wir annehmen, dass $a \vee b$ durch den soeben bewiesenen Verbindungssatz charakterisiert wird.

Sei hierzu $\gamma \in (a \vee b) \wedge c$, also $\gamma \in a \vee b$ und $\gamma \in c$. Nach dem Verbindungssatz gibt es ein $\alpha \neq \beta$ mit $\alpha \in a,\ \beta \in b,\ \alpha\beta\gamma$.

Gilt nun $\gamma = \alpha$, so ist $\gamma \in a \vee (b \wedge c)$ trivialerweise erfüllt.

Ist aber $\gamma \neq \alpha$, so liegt β auf $\alpha\gamma$, also mit α und γ in c und damit auch in $b \wedge c$. Daher folgt aus $\alpha\beta\gamma$, dass $\gamma \in a \vee (b \wedge c)$ erfüllt ist, q.e.d

(b) $\mathfrak{V}(G)$ ist komplementär,

DENN: $\mathfrak{V}(G)$ hat ℓ als kleinstes und die Menge $r = R(G)$ aller Punkte als größtes Element. Wir müssen zeigen, dass ein beliebiger linearer Teilraum a ein Komplement besitzt. Dazu betrachten wir die Menge B derjenigen

linearen Teilräume, die mit a einen leeren Durchschnitt besitzen. B ist eine Poset bezüglich der Inklusion und nicht leer, da $\ell \in B$. Es liegt nahe, zu vermuten, dass ein maximales Element b von B – sofern ein solches existiert – ein Komplement von a ist. Hierzu ist nachzuweisen, dass $a \vee b$ gleich dem ganzen Raum r ist.

Wir schließen indirekt und nehmen an, es sei $a \vee b \subset r$. Dann gibt es einen Punkt ϱ aus r, der nicht zu $a \vee b$, also insbesondere nicht zu a und nicht zu b gehört. Vereinigt man das Atom $p = \{\varrho\}$ mit b, so erhält man einen Teilraum $b \vee p$, der b echt umfasst, also wegen der Maximalität von b nicht zu B gehört. Es ist also $a \wedge (b \vee p) \neq \ell$.

Sei nun α ein Punkt aus $a \wedge (b \vee p)$, also $\alpha \in a$ und $\alpha \in b \vee p$.

Dann folgt $b \neq \ell$, da sonst $\alpha \in p$, also $\alpha = \varrho$ und damit $\varrho \in a$ – mit Widerspruch zur Wahl von $p = \{\varrho\}$ – erfüllt wäre. Auch muss $b \neq p$ gelten, da ϱ nicht Element von b ist.

Somit greift der Verbindungssatz. Aufgrund dieses Satzes gibt es zu α ein $\beta \in b$, derart dass $\beta \neq \varrho$ und $\beta\varrho\alpha$ erfüllt ist. Es gilt aber $\alpha \neq \beta$, da $a \wedge b = \ell$ ist. Folglich liegt ϱ wegen $\alpha\beta\varrho$ auf $\alpha\beta$ und damit in $a \vee b$ entgegen der Wahl von ϱ. Dieser Widerspruch zeigt, dass $a \vee b = r$.

Wir müssen noch einsehen, dass B wenigstens ein maximales Element besitzt. Dazu haben wir zu beweisen, dass auf B die Voraussetzungen des ZORNschen Lemmas zutreffen.

Wir behaupten, dass jede Kette K aus B eine obere Grenze in B besitzt. Obere Grenze von K ist das im vollständigen Verband $\mathfrak{V}(G)$ gebildete Element $\bigvee K$. Es genügt nun zu zeigen, dass $\bigvee K \in B$, d. h. dass $a \wedge \bigvee K = \ell$ erfüllt ist. Durchläuft k_ϱ die Elemente von K, so folgt nach 8.1.7 $a \wedge \bigvee K = a \wedge \bigvee k_\varrho = \bigvee(a \wedge k_\varrho) = \ell$, da jedes $a \wedge k_\varrho = \ell$ ist.

Damit ist Satz 9.1.2 vollständig bewiesen. □

Wir erinnern noch einmal daran, dass wir von einer *projektiven Geometrie* nur sprechen wollen, wenn neben (P1) und (P2) zusätzlich gilt:

(P0) Auf jeder Geraden liegen wenigstens *zwei* verschiedene Punkte.

9. 1. 5 Proposition. *In dem Verband $\mathfrak{V}(G)$ einer projektiven Geometrie G stimmen die Hyperatome überein mit den Punktmengen $[g]$, deren g eine Gerade ist.*

BEWEIS. Zunächst haben wir zu zeigen, dass es zu jedem Hyperatom a eine Gerade g gibt, so dass $[g] = a$. Hierzu benötigen wir das neue Axiom (P0) noch nicht.

Sind α und β verschiedene Punkte, so behaupten wir:

$$\{\alpha\} \vee \{\beta\} = [\alpha\beta]\,. \tag{9.1}$$

Jedenfalls ist $[\alpha\beta]$ ein linearer Teilraum, der $\{\alpha\}$ und $\{\beta\}$ umfasst. Es bleibt zu zeigen, dass $[\alpha\beta]$ in jedem $\{\alpha\}$ und $\{\beta\}$ umfassenden Teilraum x enthalten ist:

Gilt nun $\gamma \in [\alpha\beta]$, so folgt wegen $\alpha \in x$ und $\beta \in x$ auch $\gamma \in x$, da x ein linearer Teilraum ist. Das bedeutet $[\alpha\beta] \subseteq x$.

Ein beliebiges Hyperatom a von $\mathfrak{V}(G)$ ist definitionsgemäß oberer Nachbar eines Atoms $\{\alpha\}$. a enthält ein $\beta \neq \alpha$ als Element. Es folgt

$$\{\alpha\} \subset \ \{\alpha\} \vee \{\beta\} = [\alpha\beta] \subseteq a\,,$$

also $[\alpha\beta] = a$.

Damit ist gezeigt, dass man jedes Hyperatom in der Form $[g]$ schreiben kann.

Nach (P0) liegen nun aber auf jeder Geraden wenigstens zwei verschiedene Punkte. Daher ist $[g]$ weder das Nullelement noch ein Atom. Sei $\alpha \in [g]$. Um zu beweisen, dass $[g]$ ein Hyperatom ist, genügt es wegen der Modularität nach dem Nachbarsatz 4.2.12 zu zeigen, dass es keinen linearen Teilraum gibt, der echt zwischen $\{\alpha\}$ und $[g]$ liegt. Angenommen nun, es wäre x ein derartiger linearer Teilraum. Dann enthielte x neben α noch einen weiteren Punkt β, und es würde folgen $g = \alpha\beta$, also $[g] = [\alpha\beta] = \{\alpha\} \vee \{\beta\} \subseteq x$, was der Voraussetzung $x \subset [g]$ widerspräche. □

9.2 Projektive Geometrien

Im letzten Paragraphen haben wir jeder projektiven Geometrie G den Verband $\mathfrak{V}(G)$ der linearen Teilräume zugeordnet. Wir haben bewiesen, dass $\mathfrak{V}(G)$ $\bigvee$-algebraisch, atomar, modular und komplementär ist.

In diesem Paragraphen wollen wir jedem Verband V, der den oben angegebenen Bedingungen genügt, umgekehrt eine projektive Geometrie $\mathfrak{G}(V)$ zuordnen. Darüber hinaus wollen wir zeigen, dass $\mathfrak{G}(V)$ die Umkehrabbildung

von $\mathfrak{V}(G)$ ist, so dass wir eine eindeutige Abbildung der projektiven Geometrien auf die soeben gekennzeichneten Verbände haben, und infolgedessen die projektiven Geometrien mit diesen Verbänden identifizieren können.

Streng gilt dies alles nur dann, wenn wir isomorphe Verbände bzw. isomorphe Geometrien als gleichwertig ansehen. Dabei wollen wir zwei *projektive* Geometrien genau dann als *isomorph* ansehen, wenn es eine umkehrbar eindeutige Abbildung ϑ der Menge der Punkte der ersten Geometrie auf die Menge der Punkte der zweiten Geometrie, und eine umkehrbar eindeutige Abbildung Θ der Menge der Geraden der ersten Geometrie auf die Menge der Geraden der zweiten Geometrie gibt, so dass in der ersten Geometrie ein Punkt α auf einer Geraden g genau dann liegt, wenn in der zweiten Geometrie $\vartheta(\alpha)$ auf $\Theta(g)$ liegt.

Dass $\mathfrak{G}(V)$ die Umkehrabbildung von $\mathfrak{V}(G)$ ist, wenn wir isomorphe Verbände bzw. Geometrien identifizieren, beweisen wir dadurch, dass wir in Hilfssatz 1 und 2 zeigen:

$$\mathfrak{G}(\mathfrak{V}(G)) \cong G \quad \text{und} \quad \mathfrak{V}(\mathfrak{G}(V)) \cong V\,.$$

Wir beginnen damit, dass wir einem Verband V eine Geometrie $\mathfrak{G}(V)$ zuordnen. Wir setzen dabei für V zunächst nur die *Modularität* voraus; wir wollen in diesem Fall zeigen, dass $\mathfrak{G}(V)$ eine *verallgemeinerte projektive Geometrie* ist.

Wir setzen fest, dass die Atome von V die *Punkte* von $\mathfrak{G}(V)$ und die Hyperatome von V die *Geraden* von $\mathfrak{G}(V)$ sein sollen. Ein *Punkt* p soll *auf einer Geraden* g liegen genau dann, wenn $p \leq g$ in V erfüllt ist.

Zum Nachweis von (P1) und (P2) wollen wir den Dimensionsbegriff zu Hilfe nehmen. Da unser Verband modular ist, haben Atome die Dimension 1 und Hyperatome die Dimension 2. Man beachte, dass damit die Punkte der Geometrie $\mathfrak{G}(V)$ als Elemente von V die Dimension 1 und entsprechend die Geraden der Geometrie $\mathfrak{G}(V)$ die Dimension 2 haben. Diese verbandstheoretischen Dimensionen sind also jeweils um 1 größer – definiert – als die in der reellen projektiven Geometrie geläufigen topologischen Dimensionen. Im folgenden werden für verschiedene Elemente von V die Dimensionen gebildet. Man mache sich klar, dass diese Elemente eine *endliche* Dimension besitzen, während wir dies keineswegs für *alle* Elemente von V voraussetzen.

Beginnen wir mit (P1). Wir haben zunächst zu beweisen, dass zwei verschiedene Punkte p und q immer auf einer Geraden liegen. Wegen $p \wedge q = 0$ (p und

q sind Atome) ist p oberer Nachbar von $p \wedge q$, und damit nach dem Nachbarsatz $p \vee q$ ein oberer Nachbar von q, also eine Gerade. Wegen $p \leq p \vee q$, $q \leq p \vee q$ liegen p und q folglich auf dieser Geraden.

Wir müssen weiter zeigen, dass jede Gerade g, auf der diese verschiedenen Punkte p und q liegen, mit $p \vee q$ übereinstimmt. Wegen $p \leq g$, $q \leq g$ gilt $p \vee q \leq g$. Aus der Gleichheit der Dimension resultiert hieraus $p \vee q = g$.

Zum Beweis von (P2) gehen wir von Punkten p, q, r, p', q' aus, zu denen es Geraden g und h gibt, so dass p', q, r auf g und p, q', r auf h liegen. Wir müssen zeigen, dass es einen Punkt r' gibt, so dass p, q, r' sowie p', q', r' auf je einer Geraden liegen. Dies erledigen wir durch Fallunterscheidung:

FALL 1. Sei $p = q = q'$. Dann leistet $r' = r$ das Verlangte. Denn sowohl p, q, r' als auch p', q', r' liegen auf g.

FALL 2. Sei $p = q \;\&\; q \neq q'$. Dann leistet $r' = q'$ das Verlangte. Denn p, q, r' liegen auf $q \vee q'$ und p', q', r' auf $p' \vee q'$, falls $p' \neq q'$, und auf g, falls $p' = q'$.

Damit ist der Fall $p = q$ vollständig erledigt, also aus Gründen der Symmetrie auch der Fall $p' = q'$, und wir dürfen ausgehen von

FALL 3. Es gilt $p \neq q \;\&\; p' \neq q'$.

Es genügt zu zeigen, dass $d((p \vee q) \wedge (p' \vee q')) \geq 1$ erfüllt ist, da dann ein Punkt r' sowohl auf der Geraden $p \vee q$ als auch auf der Geraden $p' \vee q'$ liegt.

Da p', q und r auf g liegen, gilt $p' \vee q \vee r \leq g$, also $d(p' \vee q \vee r) \leq 2 = d(g)$. Ebenso hat man $d(p \vee q' \vee r) \leq 2$. Somit folgt nach dem Dimensionssatz zunächst

$$\begin{aligned}
& d((p' \vee q \vee r) \vee (p \vee q' \vee r)) \\
= \;& d(p' \vee q \vee r) + d(p \vee q' \vee r) - d((p' \vee q \vee r) \wedge (p \vee q' \vee r)) \\
\leq \;& d(p' \vee q \vee r) + d(p \vee q' \vee r) - d(r) \\
\leq \;& 2 + 2 - 1 \\
= \;& 3
\end{aligned}$$

und dies liefert uns wie gewünscht – erneut nach dem Dimenssionssatz –

$$\begin{aligned} & d((p \vee q) \wedge (p' \vee q')) \\ = \; & d(p \vee q) + d(p' \vee q') - d((p \vee q) \vee (p' \vee q')) \\ \geq \; & d(p \vee q) + d(p' \vee q') - d((p' \vee q \vee r) \vee (p \vee q' \vee r)) \\ \geq \; & 2 + 2 - 3 \\ = \; & 1\,. \end{aligned}$$

Damit ist auch (P2) gesichert.

Erst jetzt nehmen wir zusätzlich an, dass der modulare Verband V *komplementär* sei. Wir behaupten, dass für die zugeordnete Geometrie $\mathfrak{G}(V)$ auch das Axiom (P0) gilt. Wir haben also zu zeigen, dass auf jeder Geraden g wenigstens zwei Punkte liegen. g ist ein Hyperatom, also oberer Nachbar eines Atoms p. Damit haben wir einen ersten Punkt auf g. Sei nun $\overline{p}$ ein Komplement zu p, dann ist wegen der Modularität $\overline{p} \wedge g =: q$ ein Komplement zu p in $([0, g], \wedge, \vee)$, und es gilt $d(q) = 0$ oder $d(q) = 1$ oder $d(q) = 2$, wegen $q \subseteq g$ und $\dim(g) = 2$.

Es kann aber nicht $d(q) = 0$ gelten, da sonst $q = 0$ und $p \vee q = p \neq g$ erfüllt wäre.

$d(q)$ kann auch nicht gleich 2 sein, da sonst $q = g$ und $p \wedge q = p \neq 0$ erfüllt wäre.

Also ist $d(q) = 1$ und damit q ein auf g gelegener Punkt, der von p wegen $p \vee q = g$ verschieden ist. Und dies liefert uns:

9. 2. 1 Proposition. Ist V ein atomarer, modularer und komplementärer Verband, so ist $\mathfrak{G}(V)$ eine projektive Geometrie.

Nun kommen wir zum Beweis der oben angekündigten Gleichwertigkeit von projektiven Geometrien und gewissen Verbänden. Wir haben bereits gesehen, dass wir hierzu nur die beiden nachfolgenden Lemmata zu beweisen haben:

9. 2. 2 Lemma. *Ist G eine projektive Geometrie, so ist $\mathfrak{G}(\mathfrak{V}(G))$ isomorph zu G.*

BEWEIS. Für einen Punkt α bzw. eine Gerade g von G setze man:

$$(*) \quad \vartheta(\alpha) := \{\alpha\} \text{ bzw. } \Theta(g) := [g]\,.$$

Wie wir bereits in Satz 9.1.2 gesehen haben, ist ϑ eine umkehrbar eindeutige Abbildung der Menge der Punkte von G auf die Menge der Atome von $\mathfrak{V}(G)$, also auf die Menge der Punkte von $\mathfrak{G}(\mathfrak{V}(G))$. Nach Satz 9.1.5 ist Θ eine umkehrbar eindeutige Abbildung der Menge der Geraden von G auf die Menge der Hyperatome von $\mathfrak{V}(G)$ und damit auf die Menge der Geraden von $\mathfrak{G}(\mathfrak{V}(G))$. Schließlich gilt:

$$\begin{array}{lll} \alpha \text{ auf } g & \iff \alpha \in [g] & \text{(Definition von } [g]) \\ & \iff \{\alpha\} \leq [g] & (\text{ Inklusion in } \mathfrak{V}(G)) \\ & \iff \{\alpha\} \text{ auf } [g] & \text{(Definition von } \mathfrak{G}(V)) \\ & \iff \vartheta(\alpha) \text{ auf } \Theta(g). & ((*)) \end{array}$$

Damit ist die behauptete Isomorphie vollständig bewiesen. □

9. 2. 3 Lemma. *Ist V ein nach oben algebraischer, atomarer, modularer und komplementärer Verband, so ist $\mathfrak{V}(\mathfrak{G}(V))$ isomorph zu V.*

BEWEIS. Wir bilden das Element a von V ab auf die Menge $\varphi(a)$ aller in a enthaltenen Atome von V. Wir wollen zeigen, dass die so definierte Abbildung φ ein Isomorphismus ist von V auf $\mathfrak{V}(\mathfrak{G}(V))$. Dazu haben wir zu beweisen:

(1) $\varphi(a)$ ist ein Element von $\mathfrak{V}(\mathfrak{G}(V))$.

(2) Jedes Element von $\mathfrak{V}(\mathfrak{G}(V))$ ist φ-Bild eines Elementes aus V.

(3) $a \leq b \iff \varphi(a) \leq \varphi(b)$ (Isotonie).

Zunächst überlegen wir uns, wie die Elemente von $\mathfrak{V}(\mathfrak{G}(V))$ beschaffen sind. Ein jedes dieser Elemente ist ein linearer Teilraum M von $\mathfrak{G}(V)$, also eine Menge von Punkten aus $\mathfrak{G}(V)$, die mit je zwei verschiedenen Punkten auch stets alle weiteren zu diesen kollinearen enthält. Dabei ist ein Punkt der projektiven Geometrie $\mathfrak{G}(V)$ ein Atom aus V. Sind nun aber p, q zwei verschiedene solcher Punkte, so bedeutet die *Kollinearität* der Punkte p, q, r, dass r auf der Geraden pq liegt. pq ist aber gleich $p \vee q$. Damit haben wir:

M ist genau dann ein Element von $\mathfrak{V}(\mathfrak{G}(V))$, wenn M eine Menge von Atomen von V ist mit der Eigenschaft, dass für drei Atome $p, q, r \in V$ aus $p \in M$, $q \in M$, $p \neq q$, $r \leq p \vee q$ stets $r \in M$ folgt.

Hiernach kommen wir zu (1) bis (3).

Zu (1). $p, q \in \varphi(a)$ & $p \neq q$ & $r \leq p \vee q \Longrightarrow p, q \leq a$ & $p \vee q \leq a$ & $r \leq a$. Also ist unter der gemachten Prämisse $r \in \varphi(a)$ und damit $\varphi(a)$ ein Element von $\mathfrak{V}(\mathfrak{G}(V))$.

Zu (2) Sei M ein Element von $\mathfrak{V}(\mathfrak{G}(V))$, also eine Menge von Atomen von V. Im vollständigen Verband V bilden wir $a := \bigvee M$. Wir wollen zeigen, dass $\varphi(a) = M$ ist. Dazu genügt der Nachweis von $p \in \varphi(a) \iff p \in M$, d. h. der Äquivalenz $p \leq a \iff p \in M$. Nichttrivial ist nur die Teilbehauptung $p \leq a \implies p \in M$, mit anderen Worten

$$p \leq \bigvee M \implies p \in M\,.$$

y_e durchlaufe die Menge $\mathfrak{M}$ aller Vereinigungen von je endlich vielen Elementen aus M. $\mathfrak{M}$ ist offenbar eine gerichtete Menge. Dann ist $\bigvee M = \bigvee y_e$, und es gilt nach Voraussetzung und 8.1.7

$$p \leq \bigvee y_e \implies p \wedge \bigvee y_e = p \implies \bigvee(p \wedge y_e) = p\,.$$

Da p ein Atom ist, gilt für jedes e entweder $p \wedge y_e = 0$ oder $p \wedge y_e = p$. Es muss daher wenigstens ein e mit $p \wedge y_e = p$ geben. Wegen der Algebraizität gibt es dann endlich viele Atome $p_1, \ldots, p_m \in M$ mit

$$p \leq p_1 \vee \cdots \vee p_m\,.$$

Zu zeigen bleibt $p \in M$. Dies beweisen wir durch Induktion nach m.

Für $m = 1$ gilt $p = p_1 \in M$.

Für den Induktionsschluss setzen wir $x = p_1 \vee \cdots \vee p_{m-1}$. Es sei $p \leq x \vee p_m$. Wir sind fertig, falls $p_m \leq x$ oder $p = p_m$. Diese beiden Fälle seien jetzt ausgeschlossen. Beachten wir, dass alle im folgenden auftretenden Elemente eine endliche Dimension besitzen, so haben wir nach dem Dimensionssatz

$$d(x \vee p_m) = d(x) + d(p_m) - d(x \wedge p_m) = d(x) + 1 - 0 = d(x) + 1$$

und weiter

$$\begin{aligned} d(x \wedge (p \vee p_m)) &= d(x) + d(p \vee p_m) - d(x \vee (p \vee p_m)) \\ &= d(x) + d(p \vee p_m) - d(x \vee p_m) \qquad (p \leq x \vee p_m) \\ &= d(x) + 2 - (d(x) + 1) \qquad\qquad (p_m \not\leq x) \\ &= 1\,. \end{aligned}$$

Daher ist $x \wedge (p \vee p_m) =: q$ ein Atom. q ist in x enthalten, liegt also nach Induktionsvoraussetzung in M. Wegen $p_m \not\leq x$ ist $q \neq p_m$. Schließlich ist $q \leq p \vee p_m$, und man erhält

$$\begin{aligned} d(p \vee p_m \vee q) &= d(p \vee p_m) \\ &= 2 \\ &= d(p_m \vee q)\,. \end{aligned}$$

Hieraus folgt $p \leq p_m \vee q$. Da M ein linearer Teilraum ist, ergibt sich $p \in M$, was zu beweisen war.

Zu (3). V ist komplementär und modular, also abschnittskomplementär. Ist $(b]$ nämlich ein beliebiges Hauptideal, $x \leq b$ und y das Komplement zu x in V, so bildet $y \wedge b$ das Komplement von x in $(b]$. Denn es gelten

$$x \wedge (y \wedge b) = (x \wedge y) \wedge b = 0 \wedge b = 0$$

und

$$x \vee (y \wedge b) = (x \vee y) \wedge b = 1 \wedge b = b.$$

Daher impliziert $a < b$ auch $\varphi(a) < \varphi(b)$. Einerseits sind nämlich alle in a enthaltenen Atome auch in b enthalten, andererseits umfasst b aber zusätzlich Atome des Komplements a' von a.

Schließlich gilt $\varphi(a \wedge b) = \varphi(a) \cap \varphi(b)$. Folglich ist die Abbildung φ ein Isomorphismus. □

Wir fassen die Resultate dieses Paragraphen zusammen zu dem

9. 2. 4 Theorem. *Man kann die projektiven Geometrien identifizieren mit den nach oben algebraischen, atomaren, modularen und komplementären Verbänden, sofern man isomorphe Geometrien zum einen und isomorphe Verbände zum anderen als im wesentlichen gleich erachtet.*

Literaturverzeichnis

[1] Aigner, M.: *Diskrete Mathematik.* Friedrich Vieweg & Sohn Verlag, Braunschweig, 1993.

[2] Birkhoff ,G.: *Lattice theory.* Amer. Math. Soc. Colloq. Publ. 35, 1st, 2nd, 3rd. ed. Providence, R. I. 1940, 1948, 1967.

[3] Blyth, T. S.: *Lattices of ordered Algebraic Structures.* Springerverlag London Limited, 2005.

[4] Boole, G.: *The mathematical analysis of logic: being an essay towards a calculus of deductive reasoning*, 1847.

[5] Boole, G.: *An Investigation of the Laws of Thought on which are Founded the Mathematical Theories of Logic and Probabilities.* 1854.

[6] Bosbach, B.: *Elementaria Mathematicae*, 749 S., KOBRA Kassel, 2015.

[7] Bosbach, B.: *Topics in Divisibility*, 928 S., KOBRA Kassel , 2015.

[8] Burris, S. & H. P. Sankappanavar: *A Course in Universal Algebra.* Springer, Berlin-Heidelberg-New York, 1981.

[9] Day, A.: *A characterization of modularity for congruence lattice of algebras.* Canadian Math. Bull. **12** (1969), 167-173.

[10] Dedekind, R.: *Über die Zerlegung von Zahlen durch ihre größten gemeinsamen Teiler.* Ges. Werke, Bd. 1 pp 103-148, 1897.

[11] Dedekind, R.: *Über die von drei Moduln erzeugte Dualgruppe.* Math. Ann. **53** (1900), 371-403.

[12] Dilworth, R. P.: *Lattices with unique complements.* Trans. Amer. Math. Soc.,**57**, (1945) 123-154.

[13] Dilworth, R. P.: *A decomposition theorem for partially ordered sets.* Ann. Math. (2) **51**, (1950) 161-166.

[14] Dörge, K.&K. Wagner: *Differential- und Integral-Rechnung, Teil I.* Ferdinand Dümmlers Verlag, 1948.

[15] Fraenkel, A.: *Über den Begriff Definit und die Unabhängigkeit des Auswahlaxioms.* Sizungsberichte Preuß. Akad. Wiss., math. naturw. Kl. (1922), 353-257.

[16] Fraenkel, A.: *Untersuchungen über die Grundlagen der Mengenlehre.* Math. Zeitschr. **22** (1925), 250-273.

[17] Fraenkel, A.: *Über die Ordnungsfähigkeit beliebiger Mengen.* Sitzungsberichte Preuß. Akad. Wiss. math.-naturw. Kl. (1928), 90-91.

[18] Grätzer, G.: *Two Mal'cev type theorems in universal algebra.* J. Combinat. Theory **8** (1970), 334-342.

[19] Grätzer, G.: *On the spectra classes of algebras.* Proc. Amer. Math. Soc. **18** (1967), 729-735.

[20] Harzheim, E.: *Ordered Sets.* Springer, Science+Business, Inc., 2005.

[21] Hausdorff F.: *Grundzüge der Mengenlehre.* Verlag Veit & Co, mit 53 Figuren, Leipzig, 476 S., 1914, Nachdruck Chelsea 1949.

[22] Hermes, H.: *Einführung in die Verbandstheorie.* Grundlehren der Mathematischen Wissenschaften, zweite, erweiterte Auflage, Springer, 1967.

[23] Jónsson, B.: *Algebras whose congruence lattices are distributive.* Math. Scand. **21** (1967), 110 - 121.

[24] Kneser, H.: *Eine direkte Ableitung des Zornschen Lemmas aus dem Auswahlaxiom.* Math. Z. **53** (1950), 110 - 113.

[25] Koethe, G. M. .: *Die Theorie der Verbände, ein neuer Versuch zur Grundlegung der Algebra und projektiven Geometrie.* Jber. DMV **47**, 125-144, 1937.

[26] Lindenbaum, A. und Mostowski, A.: *O niezaleznosci pewinka wyboru niektorich jego konsekwencji.* C. R. Varsovie 31 (1938), 21-32.

[27] Mal'cev, A. I.: *On the general theory of algebraic systems.* Mat. Sbornik **35** (1954) [russisch].

[28] McKenzie, R.: *On equational theories of lattices.* Math. Scand. **27** (1970), 24-38.

[29] Miller, B. A.: *On a method due to Galois.* Quaterly J. of Math. **41** (1910), 382-384.

[30] Mitschke, A.: *Implication algebras are 3-permutable and 3-distributive.* (preprint).

[31] Mostowski, A.: *Über die Unabhängigkeit des Wohlordnungssatzes vom Ordnungsprinzip.* Fund. Math. 32 (1939), 201-252.

[32] Mostowski, A.: *On the principle of dependent choices.* Fund. Math. 35, (1948), 127-130.

[33] A. F. Pixley. *Distributivity and permutability of congruence-relations in equational classes of algebras.* Proc. Amer. Math. Soc. **14** (1963), 105-109.

[34] Ross, R. R.: *Lattice orderings on the real field.* Pacific J. Math. **63**, no 2 (1976), 571-577.

[35] Rubin, H and Rubin, Jean E. *Equivalents of the axiom of choice.* Studies in Logic and the Foundations of Mathematics, 116. North-Holland Publishing Co., Amsterdam, 1985. xxviii+322 pp.

[36] Tarski, A.: Fund. Math. **16** (1929), 195 - 197.

[37] Wille, R.: *Kongruenzklassengeometrien.* Lecture notes vol. 113. Springer, Berlin-Heidelberg-New York, 1970.

[38] Zermelo, E.: *Beweis, daß jede Menge wohlgeordnet werden kann.* Math. Ann. **59** (1904), 514-516.

[39] Zermelo, E.: *Neuer Beweis für die Möglichkeit einer Wohlordnung.* Math. Ann. **65** (1908), 107-128.

[40] Zermelo, E.: *Untersuchungen über die Grundlagen der Mengenlehre.* Math. Ann. **65** (1908), 262-281.

[41] Zorn, M.: *A remark on a method in transfinite algebra.* Bull. Amer, Math. Soc. **41** (1935), 667 - 670.

Index

Graphen für alle

Bruno Bosbach
1994

Karl Menger
1914 -1992

Inhaltsverzeichnis

Kapitel 1

Elemente

Dieser Entwurf war Gegenstand einer 2+1 – stündigen Vorlesung m. Ü. „Graphen für alle" im SS 1991, basierend auf den Büchern von Dénes König [2] und Klaus Wagner [3], aufgezeichnet in handschriftlichen Notizen in weit gehender sprachlicher und symbolischer Anlehnung an die genannten Autoren.

Als eine Heimbibliothek zur Theorie der Graphen möchten wir dem Leser die Buchbeiträge von Rainer Bodendiek et. al., insbesondere das Lehrbuch [1] empfehlen.

1.1 Grundbegriffe

1. 1. 1 Definition. Als (gerichteten) beliebigen $Graphen$ bezeichnen wir jedes System $\mathcal{G} = (\mathbf{E}, \mathbf{K}, \kappa)$, gebildet aus einer Menge $\mathbf{E} := \{A, B, C, ...\}$ von $Knoten$, einer Menge $\mathbf{K} := \{a, b, c, ...\}$ von Kanten und einer Vorschrift κ, die jeder Kante eindeutig ein (geordnetes Paar (A, B)) eine Menge $\{A, B\}$ von Ecken zuordnet.

Ist $\mathcal{G}$ ein beliebiger Graph und gilt $\kappa(a) = \{B, C\}$, so nennen wir B und C auch die Endpunkte von a und schreiben $a = BC = CB$ und sagen in diesem Fall a verbinde B und C.

Ist $\mathcal{G}$ ein geordneter Graph und gilt $\kappa(a) = (B, C)$, so nennen wir B den Anfangspunkt und C den Endpunkt von a und schreiben $a = \overrightarrow{BC}$.

Ist $\mathcal{G}$ ein Graph und hat $\mathbf{E}$ höchstens kontinuum viele Ecken, so können wir $\mathbf{E}$ natürlich bijektiv abbilden in den $\mathbf{R}^3$ und je zwei Bildpunkte im $\mathbf{R}^3$ durch so viele verschiedene Jordanbögen verbinden, wie es verschiedene Kanten in $\mathcal{G}$ gibt, die die korrespondierenden Urbild-Knoten verbinden.

Dies motiviert die Bezeichnungen $Ecke$ statt Knoten für die Elemente aus $\mathbf{E}$, die wir, siehe oben, mit großen lateinischen Buchstaben bezeichnen wollen.[1)]

Ist G ein Graph mit endlich vielen Ecken, so bietet sich aus didaktischer Sicht als eine sehr plastische Auffassung die $Nagelbrett\text{-}Darstellung$ an.

Dabei verstehen wir unter einem $Nagelbrett$ eine kariertes Brett dessen Gitterpunkte jeweils durch einen eingeführten Stift markiert sind. Hier können wir dann die Kanten durch gespannte Gummiringe markieren.

Eine $Kante\ entfernen$ heißt im geometrischen Fall den offenen Jordanbogen zu entfernen. Das können wir im endlichen Fall bezogen auf das Nagelbrett dann auch ganz einfach verstehen als ein Durchtrennen (und fliegen lassen der gespannten) korrespondierenden Gummibänder.

Im weiteren bezeichnen wir Eckenmengen $\{A, B, C, ..., U, ..\}$, mit fetten großen lateinischen Buchstaben $\mathbf{A}, \mathbf{B}, \mathbf{C}, ..., \mathbf{W}$, Kanten, siehe oben, mit kleinen lateinischen Buchstaben, Kantenmengen mit römischen Kapitalen A, B, C, ..., W, und Graphen mit großen Skriptbuchstaben $\mathcal{A}, \mathcal{B}, \mathcal{C}, ..., \mathcal{X}$.

HINWEIS: Von einem A können natürlich mehrere Kanten $auslaufen$ bzw. an ein A können auch mehrere Kanten $anstoßen$. Weiter können zwei Ecken durch $Mehrfachkanten$ verbunden sein. Anschaulich, wir können über einen Nagel beliebig endlich viele Gummiringe spannen. Schließlich können in einem Graphen $Schlingen\ AA$ auftreten. Man betrachte hierzu die Abbildung 1.1.

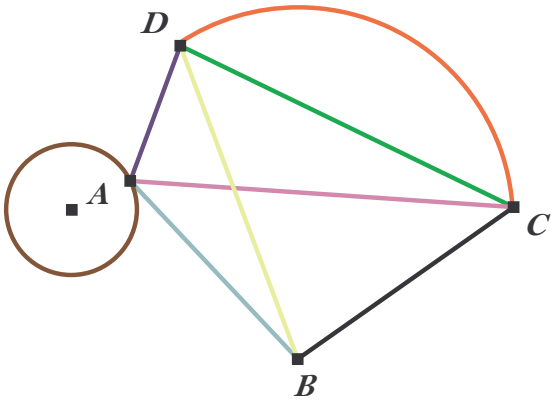


Abbildung 1.1: Ecken zu Kanten

1. Ein Graph heiße $schlicht$, wenn er weder Mehrfach-Kanten noch Schlingen hat.

[1)] Natürlich stellt sich sofort die Frage, ob wir statt der Jordanbögen gar Strecken fordern könnten, sie einander im Inneren nicht kreuzen. Dass dies tatsächlich möglich ist, zeigen wir im nächsten Abschnitt.

2. Ein Graph heißt $endlich$, wenn er nur endlich viele Ecken und Kanten hat.

3. Ein Graph heißt $gerichtet$, vgl. 1.1.1, wenn alle Kanten eine Richtung haben, anschaulich Pfeile sind.

Man denke etwa an ein Flusssystem. Hier repräsentieren die $Quellen$ und $Mündungen$ die Knoten und die Flussabschnitte dazwischen die Kanten eines gerichteten Graphen.

4. Eine Kante heißt eine $Schlinge$, s.o., wenn ihre $Endpunkte$ übereinstimmen, wenn sie also vom Typ AA ist.

5. Eine Ecke heißt ein $innerer\ Punkt$, falls mindestens 2 Kanten an sie anstoßen, bzw. von ihr auslaufen, sie heißt ein $Endpunkt$, falls genau eine Kante anstößt, und schließlich heißt eine Ecke $isoliert$, wenn keine Kante an sie anstößt.

6. Eine Kantenfolge heißt ein $Kantenzug$, wenn jede Kante genau einmal vorkommt.

7. Eine Kantenfolge heißt ein Weg, wenn ihre Ecken paarweise verschieden sind.

8. $Eine\ Kantenfolge$ heißt ein $Kreis$, wenn $Anfangs$ - und $Endpunkt$ aber keine weiteren Punkte übereinstimmen.

9. Unter der $Länge\ einer\ Kantenfolge$ verstehen wir die Anzahl ihrer Kanten.

10. Unter dem $Grad\ einer\ Ecke$ verstehen wir die Anzahl der anstoßenden Kanten.

11. Ein Graph heißt n-regulär, auch regulär vom Grade n, wenn alle seine Ecken den Grad n besitzen..

12. Ein Graph $\mathcal{G}'$ heißt $Teilgraph$ des Graphen $\mathcal{G}$, wenn die beiden Graphen in ihrer Eckenmenge übereinstimmen und jede Kante von $\mathcal{G}'$ auch Kante von $\mathcal{G}$ ist.

13. Ein Graph $\mathcal{G}'$ heißt Untergraph des Graphen $\mathcal{G}$, wenn jede Ecke von $\mathcal{G}'$ auch Ecke von $\mathcal{G}$ und jede Kante von $\mathcal{G}'$ auch Kante von $\mathcal{G}$ ist.

EIN WICHTIGER HINWEIS: Ist $\mathcal{G}$ ein Graph, so erhalten wir einen eindeutig bestimmten $Interchange\text{-}Graphen\ \mathcal{G}^*$, wenn wir die Kanten von $\mathcal{G}$ als Ecken von $\mathcal{G}^*$ auffassen und zwei der „neuen" Ecken genau dann verbinden, wenn sie, aufgefasst als Kanten von $\mathcal{G}$, aneinander stoßen, vgl. Abbildung 1.2. Man beachte, dass der Interchange-Graph nach Konstruktion in keinem Falle Mehrfachkanten aufweist.

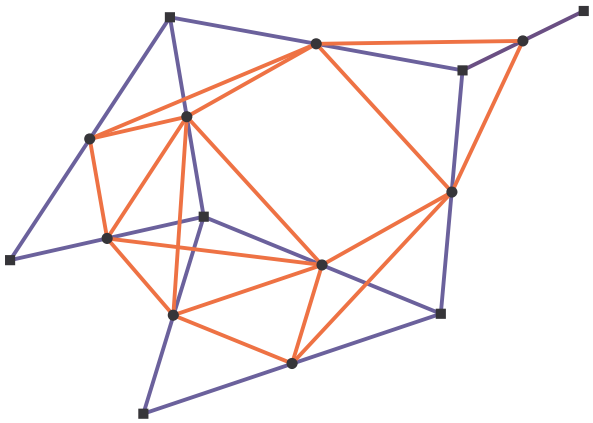


Abbildung 1.2: Ecken zu Kanten

1.2 Ein Einbettungssatz

Ist $\mathcal{G}$ ein endlicher schlichter Graph, so ist leicht zu zeigen, dass er nicht zwangsläufig *plättbar* ist, d.h. in der Ebene als ein Punkt-Kanten-Gebilde mit einander nicht kreuzenden Kanten darstellbar ist. Man denke an die Gas-Wasser-Strom-Versorgung etwa dreier Ortschaften über Erdleitungen.

Jedoch gilt der folgende irritierende Sachverhalt:

1. 2. 1 Satz. *Ist $\mathcal{G}$ ein schlichter Graph mit höchstens kontinuum vielen Ecken, so können wir $\mathcal{G}$ auffassen als einen Graphen mit Punkten aus dem $\mathbf{R}^3$ als Ecken und kreuzungsfreien Strecken aus dem $\mathbf{R}^3$ als Kanten.*

BEWEIS. Wir übernehmen den Beweis [3] in leichter sprachlicher Abwandlung.

Sei $\mathbf{E}$ die Menge aller Punkte $P = (x, y, z) \in \mathbf{R}^3$ mit den Koordinaten $x = t^1, y = t^2, z = t^3$ für eine geeignete reelle Zahl t. Geometrisch ist $\mathbf{R}$ eine Parameterkurve im $\mathbf{R}^3$. Wir wollen zunächst zeigen, dass je 4 verschiedene Punkte aus $\mathbf{R}$ affin unabhängig sind, d.h. dass sie ein Tetraeder von einem nicht verschwindenden Volumen aufspannen. Es seien hierzu vier Punkte

$$P_i = (t_i, t_i^2, t_i^3) \qquad (i = 1, 2, 3, 4)$$

gegeben. Ferner sei $\mathbf{T}$ das von diesen Punkten aufgespannte Tetraeder und $|\mathbf{T}|$ der Inhalt von $\mathbf{T}$. Dann gilt nach der bekannten Inhaltsformel für Tetraeder

$$6 \cdot |\mathbf{T}| = \begin{vmatrix} 1 & x_1 & y_1 & z_1 \\ 1 & x_2 & y_2 & z_2 \\ 1 & x_3 & y_3 & z_3 \\ 1 & x_4 & y_4 & z_4 \end{vmatrix}$$

worin $P_i = (x_i, y_i, z_i)$ die vier Ecken von $\mathbf{T}$ bedeuten. Für den Inhalt dieses Tetraeders folgt dann:

$$6 \cdot |\mathbf{T}| = \begin{vmatrix} 1 & t_1 & {t_1}^2 & {t_1}^3 \\ 1 & t_2 & {t_2}^2 & {t_2}^3 \\ 1 & t_3 & {t_3}^2 & {t_3}^3 \\ 1 & t_4 & {t_4}^2 & {t_4}^3 \end{vmatrix}$$

Die rechte Seite dieser Gleichung ist aber die bekannte *Vandermond'sche Determinante,* deren Wert gleich dem Produkt

$$\prod_{1 \leq \nu < \mu \leq 4} (t_\mu - t_\nu)$$

ist. Da die Punkte $P_1, ..., P_4$ paarweise verschieden angenommen wurden, folgt hieraus $|\mathbf{T}| \neq 0$.

Es hat sich also ergeben, dass je 4 paarweise verschiedene Punkte ein echtes Tetraeder aufspannen. Man verbinde nun je zwei Punkte P und Q aus $\mathbf{E}$ geradlinig durch die Strecke $\overline{PQ}$. Wir betrachten die Menge all dieser Strecken.

Haben dann zwei verschiedene Strecken $\overline{P_1P_2}$ und $\overline{P_3P_4}$ etwa den Endpunkt $P_1 = P_3$ gemeinsam, so wähle man in E irgendeinen von P_1, P_2, P_4 verschiedenen Punkt P_5. Da P_1, P_2, P_3, P_5 ein echtes Tetraeder aufspannen, haben $\overline{P_1P_2}$ und $\overline{P_3P_4}$ nur den Punkt P_2 gemeinsam.

Sind aber die Endpunkte von $\overline{P_1P_2}$ und $\overline{P_3P_4}$ paarweise verschieden, so spannen P_1, P_2, P_3, P_4 ein echtes Tetraeder auf. Also müssen $\overline{P_1P_2}$ und $\overline{P_3P_4}$ in diesem Falle sogar punktfremd sein.

Damit sind wir am Ziel. □

Mit anderen Worten

Nichts spricht gegen eine „euklidisch-räumliche" Auffassung „unserer Graphen" in dieser Note, mit Punkten des $\mathbf{R}^3$ als Ecken und offenen Strecken $(\overline{AB})$ als Kanten.

Eine Kante streichen bedeutet dann, um dies noch einmal zu betonen, die Endpunkte der abgeschlossenen Strecke $\overline{AB}$ „stehen" zu lassen, die inneren hingegen zu löschen.

1.3 Kantenfolgen

Unter einer $Kantenfolge$ verstehen wir eine Folge von Kanten des Typs

$$AB, BC, CD, DE, ..., XY, YZ.$$

Eine Kantenfolge heißt $offen$ im Falle $A \neq Z$ und $geschlossen$ im Falle $A = Z$.

Wir notieren Kantenfolgen auch mittels ihrer Knotenpunkte, also etwa AB, BC, $CD, ..., YZ$ vermöge $A, B, C, D, ...Y, Z$.

OBACHT: Zwei verschiedene Kantenfolgen können natürlich sehr wohl in ihren Kantenmengen übereinstimmen. Man betrachte ein Dreieck ABC. Ferner ist zu beachten, dass Kantenfolgen stets einen Durchlaufungssinn haben, auch wenn der Graph nicht gerichtet ist.

Vor allem aber bestimmt $AB, BC, CD, ..., YZ$ nicht eindeutig, welche von mehreren Kanten zwischen zwei aufeinander folgenden Ecken jeweils gemeint ist. Denn man betrachte Abbildung 1.1.

Was soll hier mit der Kantenfolge A, B, C, D, A gemeint sein. Es gibt zwei Kanten von C nach D. Eindeutigkeit schaffte etwa eine Benennung nach Farben, also die Wahl hellblau , schwarz , grün , blau oder aber hellblau , schwarz , rot , blau.

In der Realität begegnen uns Doppel- und Mehrfach-Kanten häufig als mehrspurige Leitungsbahnen, wie Straßenführungen, Elektrokabeln, Nervenbahnen,..

Wir umgehen im folgenden alle Probleme, wenn wir die Formulierung

sei $A, B, C, ...$ eine Kantenfolge

verstehen als:

> Es wurde $\overline{AB}$ als eine der Kanten von A nach B, $\overline{BC}$ als eine der Kanten von B nach C, $\overline{CD}$ als eine der Kanten von C nach D,..... ausgewählt. Ist dann $\overline{AB}, \overline{BC}, \overline{CD}, ...$ die korrespondierende Kantenfolge, so...

1. 3. 1 Satz. *Sei $A, B, C, ..., Y, Z$ eine Kantenfolge mit $A \neq Z$, betrachtet als Graph. Dann sind A und Z von ungeradem Grad und alle übrigen Knoten von geradem Grad.*

HINWEIS: Im Fall $A \neq P \neq Z$ kann eine Kante die bei P ankommt nicht die letzte sein. Ist $A = P$ V $P = Z$ ist nach endlich vielen Durchläufen eine Kante die letzte.

1. 3. 2 Satz. *Verbindet eine offene Kantenfolge die Punkte $A \neq Z$, so bilden gewisse Kanten dieser Folge einen Weg $A_i, ..., A_n$.*

HINWEIS: Kehren wir beim Durchlaufen der Kanten zu einem Punkt P zurück, so löschen wir den entsprechenden Kantenzug von P nach P und wiederholen das Verfahren bis sich ein Weg ergibt.

1. 3. 3 Satz. *Bilden gewisse Kanten eines Graphen einen geschlossenen Kantenzug, welcher den Knotenpunkt A enthält, so kann man aus gewissen Kanten dieses Kantenzuges einen Kreis bilden, welcher A ebenfalls enthält.*

HINWEIS: Siehe Satz 1.3.2.

1. 3. 4 Satz. *Sind A, B, C drei verschiedene Ecken aus $\mathcal{G}$ und gibt es eine (offene) Kantenfolge $\mathcal{F}_1$, die A mit B verbindet und eine (offene) Kantenfolge $\mathcal{F}_2$, die B mit C verbindet, so bilden gewisse Kanten aus $\mathcal{F}_1$ und $\mathcal{F}_2$ einen Weg von A nach B.*

HINWEIS: Siehe Satz 1.3.2.

1. 3. 5 Satz. *Gibt es einen Weg von P nach einem Endpunkt der Kante k, so gibt es auch einen von P auslaufenden Weg mit k als letzter Kante.*

EVIDENT.

1. 3. 6 Satz. *Sind $\mathcal{W}_1$ und $\mathcal{W}_2$ zwei verschiedene Wege von P nach Q, so bilden gewisse Kanten, die alle zu $\mathcal{W}_1$ oder $\mathcal{W}_2$ gehören, einen Kreis.*

ÜBUNG: Gehe bis zum ersten Punkt M, an dem sich die Wege trennen, von hieraus auf $\mathcal{W}_1$ bis zum ersten N, an dem die Wege wieder zusammenlaufen und danach auf $\mathcal{W}_2$ zurück zu M. Dann ist $M \xrightarrow{\mathcal{W}_1} N \xrightarrow{\mathcal{W}_2} M$ ein Kreis.

1. 3. 7 Satz. *Sind die Kanten eines Graphen $\mathcal{G}$ jeweils rot oder grün so gefärbt, dass jeder Kreis in $\mathcal{G}$ eine gerade Anzahl grüner Kanten enthält, so*

ist die Anzahl der grünen Kanten je zweier Wege mit gleichen Endpunkten stets von gleicher Parität (d.h. gleich modulo 2).

ÜBUNG: Überlagert man die beiden Wege, so liefert das Überlagerungsbild gemeinsame Wegstücke und zusammengesetzte Kreise.

1. 3. 8 Satz. *Gibt es in einem Graphen zwei verschiedene Kreise $\mathcal{K}_1$ und $\mathcal{K}_2$ mit gemeinsamer Kante k, so kann man aus gewissen Kanten dieser Kreise einen Kreis bilden, der diese Kante nicht enthält.*

HINWEIS: Lösche k. Es entsteht eine geschlossene Kantenfolge, an der notwendig beide Kreise beteiligt sind. Wähle nun eine Kante aus $\mathcal{K}_1$, die nicht zu $\mathcal{K}_2$ gehört, und wandere in beiden Richtungen bis zur ersten Kante aus $\mathcal{K}_2$ die nicht zu $\mathcal{K}_1$ gehört ...

1. 3. 9 Satz. *Sind $\mathcal{Z}_1$ und $\mathcal{Z}_2$ zwei geschlossene Kantenzüge, die keine gemeinsame Kante, wohl aber mindestens einen gemeinsamen Knoten P enthalten, so bildet die Gesamtheit der Kanten aus $\mathcal{Z}_1$ und $\mathcal{Z}_2$ einen geschlossenen Kantenzug.*

EVIDENT.

1. 3. 10 Satz. *Gibt es in einem Graphen einen Kreis $\mathcal{K}_1$, der die Kanten $k_1 \neq k_2$ enthält und einen Kreis $\mathcal{K}_2$, der die Kanten k_2 und k_3 enthält, so gibt es auch einen Kreis $\mathcal{K}$, der die Kanten k_2 und k_3 enthält.*

ÜBUNG: Laufe von k_1 in verschiedenen Richtungen entlang $\mathcal{K}_1$. Sind dann P und Q jeweils die ersten Knoten aus $\mathcal{K}_2$, so liegt k_3 in einem der beiden Teilwege von $\mathcal{K}_2$ zwischen P und Q.

1. 3. 11 Definition. Sei K′ Teilmenge der Kantenmenge K des Graphen $\mathcal{G}$ mit der Eigenschaft, dass nach jedem Knotenpunkt von $\mathcal{G}$ genau eine Kante aus K′ läuft. Dann nennen wir den von K′ bestimmten Teilgraphen $\mathcal{G}'$ von $\mathcal{G}$ einen Faktor 1. Grades von $\mathcal{G}$.

1. 3. 12 Satz. *Ist der Graph $\mathcal{G}$ ein Kreis mit einer geraden Anzahl von Kanten, oder aber ein einseitig bzw. beidseitig unendlicher Weg, so besitzt $\mathcal{G}$ einen Faktor 1.Grades.*

EVIDENT.

1.4 Zusammenhängende Graphen

1. 4. 1 Definition. Ein Graph $\mathcal{G}$ heißt *zusammenhängend*, wenn je zwei verschiedene Knoten P, Q durch einen Weg verbunden sind.

1. 4. 2 Satz. *Gibt es in einem zusammenhängenden Graphen einen Weg $\mathcal{W}$, der die Endpunkte einer Kante AB verbindet, diese Kante aber nicht enthält, so ist auch der Graph $\mathcal{G}'$, der aus $\mathcal{G}$ durch Entfernen der Kante AB entsteht, zusammenhängend.*

BEWEIS. EVIDENT. □

1. 4. 3 Satz. *Entfernt man aus einem zusammenhängenden Graphen einen seiner Endpunkte und alle an diesen Endpunkt anstoßenden Kanten oder eine Kante eines seiner Kreise, so bilden die verbleibenden Kanten zusammen mit ihren Endpunkten ebenfalls einen zusammenhängenden Graphen.*

BEWEIS. EVIDENT. □

1. 4. 4 Satz. *Sei $\mathcal{G}'$ ein nicht zusammenhängender Teilgraph eines zusammenhängenden Graphen $\mathcal{G}$. Dann gibt es in $\mathcal{G}$ eine nicht zu $\mathcal{G}'$ gehörende Kante mit der Eigenschaft, dass jeder Kreis von $\mathcal{G}$, der diese Kante enthält, auch noch wenigstens eine weitere Kante enthält, die nicht zu $\mathcal{G}'$ gehört.*

HINWEIS: Seien A und Z aus $\mathcal{G}'$ unverbunden in $\mathcal{G}'$ und sei $\mathcal{W}$ ein Weg von A nach Z in $\mathcal{G}$ mit einer minimalen Anzahl von Kanten aus $\mathcal{G}\backslash\mathcal{G}'$. Wir wählen eine dieser Kanten. Würde sie nicht den Bedingungen des Satzes genügen, so entspräche $\mathcal{W}$ nicht unserer Annahme.

1. 4. 5 Satz. *Ist $\mathcal{G}'$ ein beliebiger Teilgraph des zusammenhängenden Graphen $\mathcal{G}$ und P irgendein Knotenpunkt von $\mathcal{G}$, der nicht zu $\mathcal{G}'$ gehört, so gibt es einen Weg $\mathcal{W} = P, P_1, ..., P_{n-1}, P_n$, derart dass P_n zu $\mathcal{G}'$ gehört, aber weder die übrigen Knoten, noch seine Kanten zu $\mathcal{G}'$ gehören.*

HINWEIS: Wähle ein Z aus $\mathcal{G}'$ und einen Weg $P, ..., Z$. Ist dann M der erste Punkt des Weges $P, ..., Z$ aus $\mathcal{G}'$, so ist $P, ..., M$ von der gewünschten Art.

1. 4. 6 Definition. Als *Abstand* $|AB|$ bezeichnen wir die Länge des kürzesten Weges von A nach B.

Es folgt sofort

$$|AB| + |BC| \leq |AC| \,. \tag{1.1}$$

1. 4. 7 Definition. $A\rho B$ bedeute: es gibt einen Weg von A nach B.

1. 4. 8 Satz. *ρ ist eine Äquivalenzrelation, die $\mathcal{G}$ in zusammenhängende Bestandteile zerlegt. Genauer: es ist*

$$\mathcal{G} = \mathcal{G}_1 \cup \ldots \cup \mathcal{G}_n$$

mit

$$P \rho\, Q \Longleftrightarrow (P \in \mathcal{G}_i \Leftrightarrow Q \in \mathcal{G}_i) \,.$$

Sind umgekehrt $\mathcal{G}_i$ $(1 \leq i \leq n)$ paarweise disjunkte Graphen, so bildet auch $\bigcup_1^n \mathcal{G}_i =: \mathcal{G}$ einen Graphen, und es sind die $\mathcal{G}_i$ exakt die Zusammenhangskomponenten von $\mathcal{G}$. Hierfür schreiben wir dann auch: $\mathcal{G} = \sum \mathcal{G}_i$.

1. 4. 9 Satz. *Jeder Graph zerfällt auf eine und nur eine Weise in Zusammenhangskomponenten.*

BEWEIS. EVIDENT. □

1. 4. 10 Satz. *Laufen zu jedem Knotenpunkt eines endlichen Graphen $\mathcal{G}$ höchstens zwei Kanten, so ist jede Zusammenhangskomponente von $\mathcal{G}$ entweder ein Weg oder ein Kreis.*

HINWEIS: Wähle ein P aus $\mathcal{G}$ und gehe in eine Richtung. Dann ist eine Rückkehr nur möglich nach P. Somit entsteht im endlichen Fall ein Kreis oder ein Weg.

Lässt sich die Wanderung aber beliebig fortsetzen, so entsteht ein einseitig bzw. beidseitig unendlicher Weg.

1. 4. 11 Satz. *Laufen zu jedem Knotenpunkt eines endlichen Graphen $\mathcal{G}$ genau zwei Kanten, anders: hat jeder Knotenpunkt von $\mathcal{G}$ die Ordnung 2, so ist $\mathcal{G}$ die Summe von Kreisen.*

HINWEIS: Dies ist ein Korollar zu 1.4.10.

1. 4. 12 Satz. (a) *Zerlegt man die Menge der Knotenpunkte eines zusammenhängenden Graphen in zwei oder mehr nicht leere paarweise disjunkte Klassen, so gibt es eine Kante, deren Endpunkte in zwei verschiedenen Klassen liegen.*

(b) *Ist aber $\mathcal{G}$ nicht zusammenhängend, so lässt sich die Knotenpunktmenge derart in zwei Klassen zerlegen, dass jede Kante Knoten aus zwei verschiedenen Klassen verbindet.*

HINWEIS:

Zu **(a)**: Bilde einen Weg $A, ..., Z$ mit A, Z aus verschiedenen Klassen. Dann gibt es eine erste Klasse der gewünschten Art.

Zu **(b)**: Evident

1.5 Eulersche und hamiltonsche Linien

1. 5. 1 Definition. Ein Graph heißt *eulersch*, wenn alle seine Ecken von geradem Grad sind.

1. 5. 2 Satz. *Jeder Knotenpunkt eines eulerschen Graphen ist in einem Kreis dieses Graphen enthalten.*

BEWEIS. ÜBUNG □

1. 5. 3 Satz. *Genau dann ist ein Graph in einem Zug zu durchlaufen (eine eulersche Linie), wenn er zusammenhängend und eulersch ist.*

BEWEIS. ÜBUNG □

1. 5. 4 Satz. *In jedem endlichen Graphen ist die Anzahl der Ecken ungeraden Grades gerade.*

BEWEIS. ÜBUNG □

1. 5. 5 Satz. *Enthält eine endlicher zusammenhängender Graph $\mathcal{G}$ genau $2p$ viele Ecken ungeraden Grades, so gibt es ein aus p offenen Kantenzügen $\mathcal{Z}_1, ..., \mathcal{Z}_p$ bestehendes System, derart dass jede Kante aus $\mathcal{G}$ in einem und nur einem $\mathcal{Z}_i$ enthalten ist, und es muss jedes System dieser Art mindestens p Kantenzüge enthalten.*

BEWEIS. ÜBUNG □

1. 5. 6 Satz. *Jeder endliche zusammenhängende Graph $\mathcal{G}$ kann als eine geschlossene Kantenfolge so beschrieben werden, dass jede Kante genau zweimal durchlaufen wird.*

BEWEIS: ÜBUNG

1. 5. 7 Satz. *Genau dann ist ein Graph eulersch, wenn ein System von Kreisen existiert, derart dass jede Kante in genau einem dieser Kreise liegt.*

BEWEIS. ÜBUNG □

ANWENDUNGSBEISPIELE

1. 5. 8 Beispiel. *Das Rösselsprungproblem*

1. 5. 9 Beispiel. *Das Tram-Bahn-Problem: Jede Strecke soll nur von einer Linie befahren werden.*

1. 5. 10 Beispiel. *Das Brücken-Problem: Jede von 7 Brükcken (der 7 Brükken von Königsberg) soll auf einer Wanderung genau einmal durchlaufen werden.*

1. 5. 11 Beispiel. *Das Dominoproblem: Gegeben sei eine Menge von Dominosteinen. Lässt sich eine „ausschöpfende" Folge finden?*

1. 5. 12 Definition. Unter einer *hamiltonschen Linie* eines Graphen verstehen wir einen geschlossenen Kantenzug, der alle Knoten des Graphen enthält.

1. 5. 13 Beispiel.

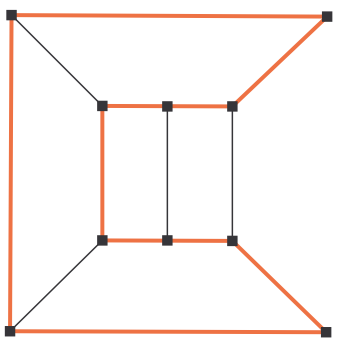


Abbildung 1.3: Ein hamiltonscher Graph

Die Bezeichnung hamiltonscher Graph rührt daher, dass R.W. HAMILTON 1859 ein Spiel vorstellte, welches u. a. das Auffinden einer heute nach ihm benannten hamiltonschen Linie für das Kantensystem des Dodekaeders erforderte.

1. 5. 14 Beispiel.

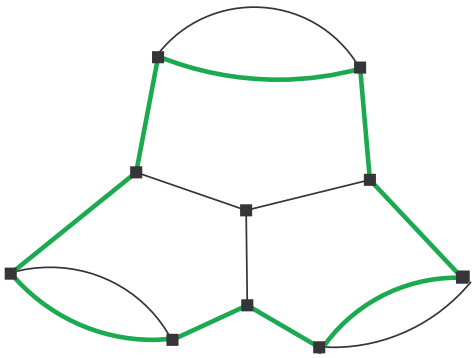


Abbildung 1.4: Ein nicht hamiltonscher Graph

1.6 Übertragung auf gerichtete Graphen

1. 6. 1 Satz. *Genau dann kann man einen gerichteten Graphen in einem Zug durchlaufen, wenn der Graph zusammenhängend ist und an jedem Knoten ebenso viele Kanten „ankommen" wie „abgehen".*

BEWEIS. ÜBUNG □

Unter einem *Zyklus* eines gerichteten Graphen verstehen wir einen gerichteten Kreis dieses Graphen.

1. 6. 2 Satz. *Für einen gerichteten Graphen gibt es genau dann ein System $\mathcal{S}$ von Zyklen $\mathcal{C}_1, ..., \mathcal{C}_n$, derart dass jede gerichtete Kante in jedem Zyklus in ursprünglicher Richtung genau einmal vorkommt, wenn alle Knotenpunkte von $\mathcal{G}$ ebenso als Start wie als Zielpunkte erscheinen.*

BEWEIS. ÜBUNG □

1. 6. 3 Satz. *Jeder ungerichtete eulersche Graph lässt sich richten.*

BEWEIS. ÜBUNG □

1. 6. 4 Satz. *Jeder endliche zusammenhängende Graph kann kontinuierlich so durchlaufen werden, dass jede Kante genau zweimal und zwar in entgegen gesetzter Richtung durchlaufen wird.*

BEWEIS. ÜBUNG □

1. 6. 5 Definition. Ein kontinuierlich gerichteter Weg heißt eine *Bahn* des gerichteten Graphen $\mathcal{G}$, wenn jede Kante des Weges die gleiche Richtung wie in $\mathcal{G}$ besitzt.

1. 6. 6 Satz. *Sei $\mathcal{G}$ ein endlicher gerichteter Graph, in dem jedes Eckenpaar P, Q entweder durch eine Kante $\overrightarrow{PQ}$ oder eine Kante $\overrightarrow{QP}$ verbunden ist. Dann besitzt $\mathcal{G}$ eine Bahn, die jeden Knotenpunkt von $\mathcal{G}$ enthält.*

BEWEIS. Der Satz gilt für jeden gerichteten Graphen mit zwei Knoten.

Er sei nun schon bewiesen für alle gerichteten Graphen mit höchstens n Knoten. Wir zeigen, dass er dann auch für alle gerichteten Graphen mit höchstens $n+1$ Knoten gilt.

Sei also $\mathcal{G}$ ein Graph im Sinne des Satzes mit $n+1$ Knoten.

Wir entfernen einen Knoten P mit allen anstoßenden Kanten und erhalten so einen Graphen $\mathcal{G}'$, der seinerseits eine Bahn der gewünschten Art besitzt, etwa $Q_1, ..., Q_n$.

Ist dann Q_nP nach P gerichtet, so sind wir fertig.

Sonst aber dürfen wir voraussetzen, dass eine der Kanten PQ_i $(1 \leq i \leq n)$ zu dem Punkt Q hin gerichtet ist, so dass es ein erstes PQ_i dieser Art gibt. Dann ist aber $\overrightarrow{Q_1, ..., Q_{i-1}, P, Q_i, ..., Q_n}$ eine Bahn der verlangten Art. □

1. 6. 7 Beispiel. *In einem (Würfel-) Billard- (Tennis-) Turnier soll jeder gegen jeden genau einmal spielen. Was wissen wir schon im Vorhinein?*

Man beachte, dass in diesen Turnieren jedes match entschieden wird, es also kein Unentschieden bzw. Remis gibt, wie etwa in einem Boxturnier oder Schachturnier.

1.7 Keislose Graphen

1. 7. 1 Definition. Ein Graph heißt *kreislos*, wenn er keinen Kreis enthält. Ein Graph heißt ein *Baum*, wenn er endlich, kreislos und zusammenhängend ist.

1. 7. 2 Satz. *Ein endlicher Graph ist genau dann ein Baum, wenn er zu je zwei Knoten genau einen Weg enthält, der diese beiden Knoten verbindet.*

BEWEIS. EVIDENT □

1. 7. 3 Satz. *Ein Graph ist dann und nur dann kreislos, wenn zu je zwei Knoten höchstens ein Weg existiert, der sie verbindet.*

BEWEIS. EVIDENT □

1. 7. 4 Satz. *Sind $\mathcal{G}_1$ und $\mathcal{G}_2$ zwei zusammenhängende Teilgraphen des kreislosen Graphen $\mathcal{G}$, so bestimmen auch die Kanten, die sowohl zu $\mathcal{G}_1$ als auch zu $\mathcal{G}_2$ gehören, einen kreislosen zusammenhängenden Teilgraphen $\mathcal{G}'$ von $\mathcal{G}$.*

BEWEIS. ÜBUNG □

1. 7. 5 Satz. *Jeder Baum besitzt mindestens zwei Endpunkte.*

BEWEIS. KLAR □

1. 7. 6 Satz. *Sind $P_0, ..., P_m$ und $Q_0, ..., Q_n$ zwei Wege eines kreislosen Graphen mit dem gemeinsamen Endpunkt $P_0 = Q_0$, aber $P_1 \neq Q_1$, so bildet die Gesamtheit der Kanten dieser Wege ebenfalls einen Weg, nämlich $P_m, ..., P_0 = Q_0, ..., Q_n$.*

BEWEIS. ÜBUNG □

1. 7. 7 Satz. *Es sei P ein Knoten und AB eine Kante des zusammenhängenden kreislosen Graphen $\mathcal{G}$, und es seien*

$$\mathcal{W}_1 = P, Q_1, ..., Q_m, A \text{ und } \mathcal{W}_2 = P, R_1, ..., R_n, B$$

die (einzigen) Wege, die P mit A bzw. P mit B verbinden. Dann ist AB entweder die letzte Kante Q_mA von $\mathcal{W}_1$ oder aber es ist AB die letzte Kante R_nB von $\mathcal{W}_2$

BEWEIS. ÜBUNG □

1. 7. 8 Satz. *Jeder endliche kreislose Graph ist eine Summe von Bäumen.*

BEWEIS. ÜBUNG □

1. 7. 9 Definition. Ein Baum heißt ein *Stern*, wenn es einen Knoten gibt, der gemeinsamer Endpunkt aller Kanten ist.

1. 7. 10 Satz. *Sind sämtlich Kanten eines Baumes Endkanten, so ist dieser Baum ein Stern.*

BEWEIS. KLAR □

1. 7. 11 Satz. *In jedem Baum ist die Anzahl der Knoten um 1 größer als die Anzahl der Kanten.*

BEWEIS. KLAR □

1. 7. 12 Satz. *Es seien α die Anzahl der Knoten, β die Anzahl der Kanten sowie κ die Anzahl der Komponenten eines kreislosen endlichen Graphen. Dann gilt:*

$$\alpha = \beta + \kappa \tag{1.2}$$

BEWEIS. KLAR □

1.8 Die Zusammenhangszahl

1. 8. 1 Satz. *Jeder zusammenhängende endliche Graph $\mathcal{G}$ enthält einen baumförmigen Teilgraphen $\mathcal{B}$ mit denselben Knotenpunkten wie $\mathcal{G}$.*

1. 8. 2 Satz. *Entsteht aus einem endlichen Graphen $\mathcal{G}$ der Eckenzahl α_0 und der Kantenzahl α_1 durch Streichen von Kanten ein Baum mit der gleichen Eckenmenge, so ist die Anzahl μ der gestrichenen Kanten gleich*

$$\mu = \alpha_1 - \alpha_0 + 1 .$$

BEWEIS. ÜBUNG □

Die Zahl μ heißt auch die Zusammmenhangszahl von $\mathcal{G}$. Anschaulich ist μ demnach das Maximum von möglichen Streichungen ohne Zusammenhangsveränderungen.

Ist $\mathcal{G}$ nicht zusammenhängend, so macht diese Zahl ebenfalls Sinn und ist – wie man leicht sieht – gleich

$$\mu = \alpha_1 - \alpha_0 + \nu\,,$$

worin ν die Zahl der Komponenten ist.

Für die Zusammenhangszahl gilt:

1. 8. 3 Satz. *Dann und nur dann ist die Zusammenhangszahl eines endlichen Graphen gleich* 0*, wenn der Graph eine Summe von Bäumen, also kreislos ist.*

BEWEIS. ÜBUNG □

1. 8. 4 Satz. *Ein endlicher zusammenhängender Graph mit* α_0 *vielen Ecken enthält mindestens* $\alpha_0 - 1$ *viele Kanten.*

BEWEIS. ÜBUNG □

1. 8. 5 Satz. *Streicht man in einem endlichen zusammenhängenden Graphen* $\mathcal{G}$ *eine Kante eines Kreises, so reduziert sich die Zusammenhangszahl um* 1*.*

BEWEIS. ÜBUNG □

1. 8. 6 Satz. *Entsteht ein zusammenhängender Teilgraph* $\mathcal{G}'$ *aus einem zusammenhängenden Graphen* $\mathcal{G}$ *von der Zusammenhangszahl* μ *durch Streichen von* μ *Kanten, so ist* $\mathcal{G}'$ *ein Baum.*

BEWEIS. ÜBUNG □

Der nun folgende Satz wurde schon von KIRCHHOFF im Zusammenhang mit physikalischen Untersuchungen ausgesprochen.

1. 8. 7 Satz. *Um aus einem endlichen zusammenhängenden Graphen von der Zusammenhangszahl* μ *durch Streichen von Kanten einen kreislosen Graphen zu erhalten, müssen mindestens* μ *Kanten gestrichen werden.*

BEWEIS. ÜBUNG □

1. 8. 8 Satz. *Ist $\mathcal{G}'$ aus $\mathcal{G}$ durch Streichen von μ' vielen Kanten hervorgegangen und zudem kreislos, so gelangt man durch rückläufige Verbindung der Komponenten zu einem Baum i. S. von Satz 1.8.2.*

BEWEIS. ÜBUNG □

1. 8. 9 Satz. *Unterwirft man einen endlichen Graphen $\mathcal{G}$ von der Zusammenhangszahl μ einer sukzessiven Kantenstreichung, so bricht er spätestens nach $\mu + 1$ Streichungen auseinander.*

BEWEIS. ÜBUNG □

Satz 1.8.8 beschreibt μ offenbar als eine Minimalzahl, Satz 1.8.9 hingegen charakterisiert μ als Maximalzahl.

Tatsächlich haben JORDAN und SKOLEM μ als Maximalzahl eingeführt, wohingegen KIRCHHOFF μ als Minimalzahl definierte.

1.9 Gerüst und Fundamentalsystem

Als *Gerüst* eines Graphen bezeichnen wir jeden Untergraphen $\mathcal{G}'$ mit der Eigenschaft

(*i*) $\mathcal{G}'$ ist kreislos.

(*ii*) Nimmt man noch eine Kante hinzu, so entsteht ein Kreis.

1. 9. 1 Satz. *Ist $\mathcal{G}'$ ein Gerüst zu $\mathcal{G}$, so ist $\mathcal{G}'$ sogar ein Teilgraph zu $\mathcal{G}$.*

BEWEIS. ÜBUNG □

1. 9. 2 Satz. *Ist $\mathcal{G}$ zusammenhängend, so auch jedes Gerüst von $\mathcal{G}$.*

BEWEIS. ÜBUNG □

1. 9. 3 Satz. *Ist $\mathcal{G}'$ ein zusammenhängender und kreisloser Teilgraph von $\mathcal{G}$, so ist $\mathcal{G}'$ ein Gerüst von $\mathcal{G}$.*

BEWEIS. ÜBUNG □

1. 9. 4 Satz. *Ist $\mathcal{G} = \sum \mathcal{G}_i$ und $\mathcal{S}_i$ jeweils ein Gerüst zu $\mathcal{G}_i$, so ist $\sum \mathcal{S}_i$ ein Gerüst zu $\mathcal{G}_i$.*

BEWEIS. ÜBUNG □

1. 9. 5 Satz. *Jedes Gerüst eines endlichen Graphen der Zusammenhangszahl μ entsteht durch Streichen von μ Kanten.*

BEWEIS. ÜBUNG □

1. 9. 6 Satz. *Es sei α_0 die Zahl der Knoten, α_1 die Zahl der Kanten und κ die Anzahl der Komponenten eines endlichen Graphen $\mathcal{G}$ und $\mathcal{S}$ ein Gerüst. Ist μ dann sie Anzahl derjenigen Kanten von G, die nicht zu $\mathcal{S}$ gehören, so gilt:*

$$\alpha_0 + \mu = \alpha_1 + \kappa\,.$$

HINWEIS: Hat $\mathcal{S}$ λ viele Kanten, so folgt $\lambda + \mu = \alpha_1$, und es hat $\mathcal{S}$ andererseits $\alpha_0 - \kappa$ viele Kanten.

1. 9. 7 Satz. *Jeder (beliebige) Graph besitzt mindestens ein Gerüst (bemühe* Zorn*).*

BEWEIS. ÜBUNG □

1. 9. 8 Satz. *Ist $\mathcal{S}$ ein Gerüst von $\mathcal{G}$ und k eine Kante von $\mathcal{G}$, die nicht zu $\mathcal{S}$ gehört, so gibt es einen, aber auch nur einen Kreis, der k enthält, ansonsten aber lauter Kanten aus $\mathcal{S}$.*

BEWEIS. ÜBUNG □

Es gehört also zu jeder Kante k, die nicht in $\mathcal{S}$ liegt, genau ein Kreis $\mathcal{K}_k$ mit maximalem Anteil in $\mathcal{S}$. Dies gibt Anlass zu der

1. 9. 9 Definition. Ist $\mathcal{F}_\mathcal{S}$ das System aller Kreise $\mathcal{K}_k$ i. S. der getroffenen Feststellungen, so nennen wir $\mathcal{F}_\mathcal{S}$ das zu $\mathcal{S}$ gehörende *Fundamentalsystem.*

1. 9. 10 Satz. *Jeder Kreis eines Fundamentalsystems enthält eine Kante, die keinem anderen Kreis dieses Fundamentalsystems angehört.*

BEWEIS. ÜBUNG □

1. 9. 11 Satz. *Jedes Fundamentalsystem eines endlichen Graphen von der Zusammenhangszahl ν besteht aus μ Kreisen.*

BEWEIS. ÜBUNG □

Damit hat die Zusammenhangszahl eine weitere Deutung erfahren.

1.10 Achse bzw. Zentrum eines Baumes

1. 10. 1 Satz. *Ist P Knoten eines zusammenhängenden kreislosen Graphen $\mathcal{G}$, so gibt es zwischen der Menge der von P verschiedenen Knoten von $\mathcal{G}$ und der Menge sämtlicher Kanten von $\mathcal{G}$ eine Bijektion, die jeder Kante einen ihrer Endpunkte zuordnet.*

BEWEIS. ÜBUNG □

1. 10. 2 Satz. *Ist P ein beliebiger Knoten eines Baumes $\mathcal{B}$, so ist jeder Knotenpunkt von maximaler Entfernung von P ein Endpunkt.*

BEWEIS. ÜBUNG □

1. 10. 3 Satz. *Streicht man sämtliche Endpunkte eines Baumes $\mathcal{B}$, so erhält man einen Baum $\mathcal{B}^{(1)}$, streicht man hiernach alle Endpunkte von $\mathcal{B}^{(1)}$, so erhält man einen Baum $\mathcal{B}^{(2)}$ usf. Schließlich erhalten wir $\mathcal{B}^{(r-1)}$ als Stern.*

BEWEIS. ÜBUNG □

1. 10. 4 Definition. Besteht der oben erwähnte *Stern* aus genau einer Kante, so nennen wir diese Kante die *Achse des Baumes* und ihre Endpunkte die *Bizentren* des Baumes. Enthält $\mathcal{B}^{(r-1)}$ hingegen mehr als eine Kante, so nennen wir den allen gemeinsamen Kanten gemeinsamen Knoten das *Zentrum des Baumes.*

Genauer auch:*Achse, Bizentrum, Zentrum der linearen Ausdehnung.*

1. 10. 5 Satz. *Die Bäume $\mathcal{B}$, $\mathcal{B}^{(1)}$, $\mathcal{B}^{(2)}$... haben alle dasselbe Zentrum bzw. dieselbe Achse.*

BEWEIS. ÜBUNG □

1. 10. 6 Definition. Unter dem *Durchmesser eines endlichen Baumes* verstehen wir die (gemeinsame) Länge aller numerisch längsten Wege.

1. 10. 7 Satz. *Ist $P_0, P_1, ..., P_{d-1}, P_d$ ein längster Weg eines Baumes $\mathcal{B}$, so ist $P_0, P_1, ..., P_{d-1}$ ein längster Weg von $\mathcal{B}^{(1)}$.*

BEWEIS. ÜBUNG □

1. 10. 8 Satz. *Der Durchmesser eine Baumes $\mathcal{B}$ ist um 2 größer als der Durchmesser des Baumes $\mathcal{B}^{(1)}$.*

BEWEIS. ÜBUNG □

1. 10. 9 Definition. Unter dem *Radius eines endlichen Baumes* vertstehen wir die Anzahl der sukzessiven Endkantenstreichungen, die erforderlich sind, um den Baum auf den *Nullgraphen* zu reduzieren.

1. 10. 10 Satz. *Ist r der Radius und d der Durchmesser des Baumes $\mathcal{B}$, so ist $d = 2r$ bzw. $d = 2r - 1$ je nachdem, ob $\mathcal{B}$ ein Zentrum oder eine Achse besitzt, und es gilt auch der Kehrsatz.*

BEWEIS. ÜBUNG □

1. 10. 11 Satz. *Ein Baum besitzt ein Zentrum oder eine Achse, je nachdem ob sein Durchmesser gerade oder ungerade ist.*

BEWEIS. ÜBUNG □

1. 10. 12 Satz. *Sei $\mathcal{W}$ ein längster Weg des Baumes $\mathcal{B}$. Ist dann die Kantenzahl von $\mathcal{W}$ gerade, so bildet der mittlere Knoten von $\mathcal{W}$ das Zentrum von $\mathcal{B}$. Ist die Kantenzahl von $\mathcal{W}$ hingegen ungerade, so bildet die mittlere Kante die Achse von $\mathcal{B}$.*

BEWEIS. ÜBUNG □

1.11 Charakteristische Eigenschaften von Achsen und Zentren

1. 11. 1 Satz. *Ist r der Radius und C das Zentrum oder Bizentrum des Baumes $\mathcal{B}$, so ist die Länge des längsten Weges der nach C läuft gleich r.*

BEWEIS. ÜBUNG □

1. 11. 2 Satz. *Ist A irgendein Knotenpunkt des Baumes $\mathcal{B}$, welcher vom Zentrum C bzw. Bizentrum C, C' verschieden ist, so gibt es einen in A endenden Weg, dessen Länge größer ist als r.*

BEWEIS. ÜBUNG □

Weiter erhalten wir

1. 11. 3 Satz. *In jedem Baum nimmt die maximale Entfernung eines Knoten von seinem Mittelknoten ihr Minimum nur im Zentrum bzw. den beiden Bizentren an.*

Ist nun d der Durchmesser des Baumes, so ist dieses Minimum im Falle eines Zentrums gleich $d/2$ und im Falle eines Bizentrums gleich $(d+1)/2$.

BEWEIS. ÜBUNG □

Als weitere Kriterien erhalten wir:

1. 11. 4 Satz. *Hat der Baum $\mathcal{B}$ ein Zentrum C, so ist C der einzige Knotenpunkt von $\mathcal{B}$ mit der Eigenschaft:*

Es gibt zwei nach C verlaufende gleich lange Wege , die zwei verschiedene nach C laufende Kanten besitzen und deren Länge zumindest ebenso groß ist wie die Länge eines jeden anderen Weges QC.

BEWEIS. ÜBUNG □

1. 11. 5 Satz. *Hat der Baum $\mathcal{B}$ eine Achse a, so ist a die einzige Kante von $\mathcal{B}$, deren Endpunkte C, C' die folgende Eigenschaft besitzen:*

Es gibt zwei gleichlange Wege, die nach C bzw. C' laufen, die Kante a nicht enthalten und mindestens so lang sind wie jeder weitere Weg, der nach C bzw. C' läuft und a ebenfalls nicht enthält.

BEWEIS. ÜBUNG □

Wir verzichten hier auf die Begriffe $Massenzentrum$ und $Massenachse$ (siehe D. KÖNIG) und wenden uns nun einer Anwendung zu.

1.12 Eine Anwendung aus der Chemie

Durch die Angabe der Symmetriegruppe eines Graphen $\mathcal{G}$ werden die Symmetrieeigenschaften von $\mathcal{G}$ bestimmt, so dass man im endlichen Fall die Ordnung dieser Gruppe als $Symmetriegrad$ bezeichnen kann.

Wird in $\mathcal{G}$ zusätzlich ein Punkt P als $Fixpunkt$ bestimmt, so spricht man von einem $Wurzelgraphen$ und bezeichnet $\mathcal{G}$ auch mit $\mathcal{G}_P$.

Damit stellt sich die natürliche Frage, welche Graphen bzw. Wurzelgraphen es bei vorgegebener Kantenzahl gibt. Natürlich hängt diese Frage aufs Engste mit der Frage zusammen: Wie lässt sich der Symmetriegrad eines vorgelegten Graphen bestimmen? Hierzu hat JORDAN ein Verfahren angedeutet, das am Ende zu einem Fall von Bäumen führt.

Danach geht es dann darum, die Symmetrieeigenschaften von Bäumen zu untersuchen. Dabei geht das (Bi-)Zentrum wegen seiner eindeutigen Bestimmtheit (es gibt genau ein (Bi-)Zentrum), zwangsläufig bei jedem $Automorphismus$ in sich selbst über. Und das deutet schon an, wie die Theorie der Bäume fruchtbringend genutzt werden kann. Hierzu geben wir

Ein Beispiel aus der Chemie: $Paraffine$ sind gegeben durch die Formel C_nH_{2n+2}. Wir lassen nun den n C-Atomen je einen Punkt $C^{(i)}(1 \leq i \leq n)$ entsprechen und den $2n+2$ H-Atomen je einen Punkt $C^{(j)}(1 \leq j \leq 2n+2)$. Es hat aber C die Valenz 4 und H die Valenz 1. Folglich wird die Konstitution des Paraffins dadurch bestimmt, dass man einen Graphen angibt, in dem jeder C-Punkt den Grad 4 und jeder H-Punkt den Grad 1 hat.

Dieser Graph besitzt dann $\alpha_0 = 3n+2$ Knotenpunkte, und es ist die doppelte Anzahl seiner Kanten gleich

$$2\alpha_1 = 4 \cdot n + 1 \cdot (2n+2)\,. \tag{1.3}$$

Folglich ist $\alpha_1 = 3n+1$, so dass der Graph die Zusammenhangszahl

$$\mu = \alpha_1 - \alpha_0 + 1 = 0 \tag{1.4}$$

besitzt, d.h. ein Baum $\mathcal{B}$ ist.

Es sind aber die H-Punkte die Endpunkte dieses Baumes $\mathcal{B}$.

Wir entfernen nun die sämtlichen Endkanten und erhalten $\mathcal{B}^{(1)} =: \overline{\mathcal{B}}$. $\mathcal{B}$ ist aber in seiner Struktur durch die Struktur von $\overline{\mathcal{B}}$ vollkommen bestimmt. Ist nämlich $k_i (\leq 4)$ die Anzahl der nach dem Knotenpunkt $C^{(i)}$ von $\overline{\mathcal{B}}$ laufenden Kanten, so ergibt sich $\mathcal{B}$ aus $\overline{\mathcal{B}}$, indem man jedem Knoten $C^{(i)}$ $4 - k_i$ viele Kanten anhängt.

Damit ist die Bestimmung aller Paraffine dem graphentheoretischen Problem äquivalent, alle Bäume zu bestimmen, welche n Knoten von einem Grad ≤ 4 besitzen.

Kapitel 2

Färbungen und Faktoren

2.1 Blau und Rot

Die Konstruktion neuer Objekte mittels bekannter Objekte und invers hierzu die Zurückführung von gegebenen Objekten auf bekannte sind Standardverfahren im Bereich der Strukturmathematik.

Der klassischste aller Sätze dieser Art ist der auf Euklid zurückgehende Fundamentalsatz der elementaren Zahlentheorie, der besagt, dass sich jede natürliche Zahl eindeutig in Primzahlen zerlegen lässt.

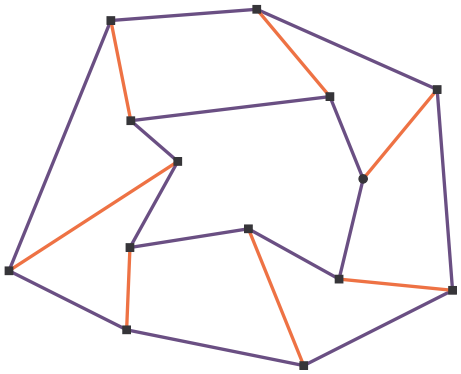


Abbildung 2.1: 3-regulär blau-rot

In diesem Abschnitt wollen wir uns mit der Analyse gewisser spezieller Graphen befassen. Ist $\mathcal{G}$ etwa eine Summe von paarweise ecken-fremden Kanten, so hat jede Ecke die Ordnung 1. Ist $\mathcal{G}$ hingegen eine Summe von paarweise ecken-fremden Kreisen, so hat jede Ecke die Ordnung 2. Haben all diese Kreise eine gerade Kantenzahl, so können wir zusätzlich den gesamten Graphen mit 2 Farben,

etwa blau und rot (alternativ) so färben, dass in keiner Ecke zwei gleichfarbige Kanten aneinander stoßen.

Unsere Frage in diesem Abschnitt: Was lässt sich sagen über 3-reguläre Graphen? Sie sind die nächstliegenden Kandidaten für ein „Stück" Strukturanalyse.

Offenbar erhalten wir 3-reguläre Graphen, wenn wir etwa zwei Kreise gleicher Kantenzahl eckenweise durch Stege verbinden.

Färben wir dann die Stege rot und die Kreise blau, so laufen an jeder Ecke zwei blaue und ein rote Kante zusammen.

Gilt dies für einen beliebigen Graphen, so ist dieser natürlich 3-regulär, was bedeutet, dass er in zwei Faktoren, nämlich einen 1-regulären und einen 2-regulären zerfällt.

Doch dies gilt, wie zu erwarten, nicht für jeden 3-regulären Graphen. Man betrachte etwa Abbildung 2.2. Hier enden wir bei konsequenter Färbung, ausgehend von dem roten Steg, bei einem Widerspruch.

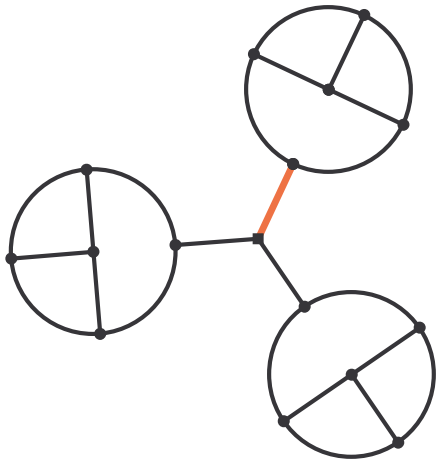


Abbildung 2.2: 3-regulär nicht blau-rot

Das Besondere an diesem Graphen ist die Existenz von *Brücken*, im Sinne der folgenden Erklärung.

2. 1. 1 Definition. Eine Kante b eines Graphen $\mathcal{G}$ heißt eine *Brücke* von $\mathcal{G}$, wenn b weder Endkante noch Kante eines Kreises ist.

Später wird sich das Element der Brücke als fruchtbares Charakter-Merkmal erweisen. Das bedeutet natürlich u. a. dass sich Definitionen, Sätze, Beweise und

Übungen immer wieder unter Bezugnahme auf die Abbildungen 2.1 und 2.2 anschaulich „festmachen" lassen.

2. 1. 2 Satz. *Ist b eine Brücke des zusammenhängenden Graphen $\mathcal{G}$, so zerfällt $\mathcal{G} - \{b\}$ in zwei Komponenten, bezeichnet als die Ufer zur Brücke b.*

BEWEIS. ÜBUNG □

2. 1. 3 Satz. *Gehört die Brücke PQ nicht zu dem Kantenzug $P, P_1, ..., P_n$, so liegt $P, P_1, ..., P_n$ ganz „an" einem der beiden Ufer*

BEWEIS. ÜBUNG □

2. 1. 4 Satz. *Ist $\mathcal{G}$ zusammenhängend und b eine Brücke sowie $\mathcal{T}$ ein Teilgraph von $\mathcal{G}$ ohne b, so liegt $\mathcal{T}$ ganz an einem Ufer.*

BEWEIS. ÜBUNG □

Wir kommen jetzt zur alles entscheidenden Definition für einen Zerlegungssatz von O.FRINK.

2. 1. 5 Definition. Sei in $\mathcal{G}$ ein Untergraph vom Typus P, Q, M, N, R, S gegeben mit $MN =: x$, siehe Abbildung 2.3.

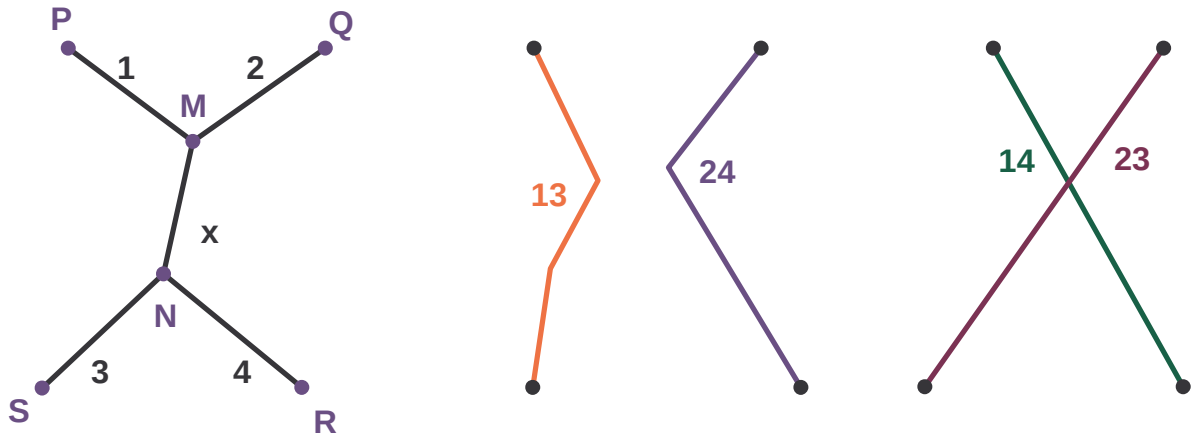


Abbildung 2.3: Zur Spaltung einer Kante

Dann verstehen wir unter der *Spaltung 1. Art* von x die simultane Ersetzung des Kantenzuges $PMNS$ durch eine neue Kante $PS =: 13$ und des Kantenzuges $QMNR$ durch eine neue Kante $QR =: 24$.

Und wir verstehen unter der Spaltung 2. Art der Kante x die simultane Ersetzung des Kantenzuges $PMNR$ durch eine neue Kante $PR =: 14$ und des Kantenzuges $QMNS$ durch eine neue Kante $QS =: 23$.

Nach diesen Vorbemerkungen lässt sich als ein erster Struktursatz beweisen:

2. 1. 6 Ein Satz von Frink. *Sei $\mathcal{G}$ 3-regulär, zusammenhängend, brückenlos und schlingenfrei. Ist dann x eine Kante, die in keinem Zweieck liegt, und führen die beiden verschiedenen Spaltungen von x zu den Graphen $\mathcal{G}_1$ und $\mathcal{G}_2$, so ist mindestens einer dieser beiden Graphen $\mathcal{G}_1, \mathcal{G}_2$ ebenfalls 3-regulär, zusammenhängend, brückenlos und schlingenfrei.*

BEWEIS. Offenbar sind die beiden angesprochenen Graphen zwangsläufig 3-regulär und schlingenfrei.

(a) *Wir betrachten nun $\mathcal{G}_1$ und nehmen an, $\mathcal{G}_1$ sei nicht zusammenhängend. Dann ist zwingend $\mathcal{G}_2$ zusammenhängend.*

DENN: Ist $\mathcal{G}_1$ nicht zusammenhängend, so hat $\mathcal{G}_1$ genau zwei zusammenhängende Bestandteile, von denen der eine die Kante 13 und der andere die Kante 24 enthält.

Angenommen nämlich $\mathcal{B}$ wäre ein maximaler zusammenhängender Bestandteil und enthielte weder 13 noch 24, so wäre $\mathcal{B}$ ein Teilgraph von $\mathcal{G}$. Ist nun $A \neq M$ irgendein Knoten von $\mathcal{B}$, dann gibt es einen Wege von A nach M, der P, Q, R oder S enthalten muss.

Wir nehmen an, es sei P der erste dieser Punkte, der von A aus „durchlaufen" wird. Dann ist der Anteil von A bis P ein Weg in $\mathcal{G}_1$. Daher gehört in diesem Falle 13 zu $\mathcal{B}$, da $\mathcal{B}$ maximal zusammenhängend sein sollte. Analog schließen wir in den anderen Fällen, dass 13 oder 24 zu $\mathcal{B}$ gehört. Es können aber nicht beide Kanten 13, 24 zu $\mathcal{B}$ gehören, da $\mathcal{G}_1$ sonst zusammenhängend wäre, entgegen unserer Annahme.

(b) *Weder* 13 *noch* 24 *ist eine Brücke in $\mathcal{G}_1$.*

DENN: Wir nehmen an, 13 wäre eine Brücke in $\mathcal{G}_1$. Die Kante 1 ist keine Brücke in $\mathcal{G}$, da $\mathcal{G}$ brückenlos ist. Also gibt es, da 1 in einem Kreis liegt, einen Weg $\mathcal{W}$ von P nach M ohne die Kante 1, der S oder R oder Q „anläuft".

Eine „Einmündung" in S widerspräche aber der angenommenen Brückeneigenschaft von 13 in $\mathcal{G}_1$, also muss $\mathcal{W}$ die Knoten R oder Q anlaufen, und es gibt analog einen Weg von S nach N über Q oder R.

Dann liefert aber Durchmusterung der Fälle

(a) $(P, ..., Q \,\&\, S, ..., Q)$
(b) $(P, ..., Q \,\&\, S, ..., R)$
(c) $(P, ..., R \,\&\, S, ..., Q)$
(d) $(P, ..., R \,\&\, S, ..., R)$,

dass 13 keine Brücke in $\mathcal{G}_1$ sein kann, was dem Leser als ÜBUNG überlassen sei.

Dual ergibt sich – natürlich – dass auch 24 keine Brücke in $\mathcal{G}_1$ sein kann.

(c) *Sei $\mathcal{G}_1$ nicht notwendig zusammenhängend und $b = A_1A_2$ eine Brücke von $\mathcal{G}_1$. Dann enthält das eine Ufer von b die Kante* 13 *das andere die Kante* 24.

DENN: Es gibt in $\mathcal{G}$ einen Kreis mit der Kante b, da $\mathcal{G}$ brückenlos ist, und es muss dieser Kreis mindestens eine der Kanten $1, 2, 3, 4$ enthalten, da b Brücke in $\mathcal{G}_1$ ist und jeder Kreis, der x als Kante enthält, auch eine der Kanten $1, 2, 3, 4$ enthält. Folglich gibt es auf diesem Kreis eine erste Ecke aus P, Q, R, S, wenn wir von A_1 aus in Richtung A_2A_1 gehen und eine erste Ecke aus P, Q, R, S, wenn wir von A_2 aus in Richtung A_1A_2 gehen, und diese beiden Ecken müssen zu verschiedenen der Kanten 13, 24 gehören, da b eine Brücke aus $\mathcal{G}_1$ ist. Es liegt aber nach Hilfssatz 2.1.4 jede der beiden Kanten ganz auf einem Ufer von b, also liegen 13 und 24 auf verschiedenen Ufern von b.

Nach **(c)** und 2.1.4 existiert in $\mathcal{G}_1$ ein Kreis $\mathcal{K}_1$, der die Kante 13 enthält und ebenso eine Kreis $\mathcal{K}_2$, der die Kante 24 enthält.

(d) *Die unter* **(c)** *nachgewiesenen Kreise für* 13 *und* 24 *sind fremd.*

DENN: Ist $\mathcal{G}_1$ unzusammenhängend, so liegen 13 und 24 nach (a) in verschiedenen Komponenten, also auch die Kreise $\mathcal{K}_1$ und $\mathcal{K}_2$.

Ist $\mathcal{G}_1$ hingegen zusammenhängend und nicht brückenlos und ist etwa b eine Brücke, so folgt nach **(b)** und 2.1.4, dass $\mathcal{K}_1$ und $\mathcal{K}_2$ jeweils gänzlich einem Ufer angehören.

Hiernach kommen wir zu einem letzten Schritt

(e) *Von den beiden Graphen $\mathcal{G}_1$ und $\mathcal{G}_2$ ist mindestens einer zugleich zusammenhängend und brückenlos.*

DENN: Nach **(a)** ist $\mathcal{G}_1$ oder $\mathcal{G}_2$ zusammenhängend. Wir nehmen hier an, dass $\mathcal{G}_1$ zusammenhängend ist, aber nicht brückenlos, und überlassen den Fall, in dem $\mathcal{G}_2$ zusammenhängend, aber nicht brückenlos ist dem Leser als ÜBUNG.

Sei also $\mathcal{G}_1$ zusammenhängend, aber nicht brückenlos. Dann gelangen wir wie folgt ans Ziel: Wir entfernen 13 bzw. 24 aus $\mathcal{K}_1$ bzw. $\mathcal{K}_2$. Dies führt zu fremden Wegen $\mathcal{W}_1$, $\mathcal{W}_2$ von P nach S bzw. von Q nach R, die zu $\mathcal{G}_2$ gehören, weshalb auch $\mathcal{G}_2$ zusammenhängend ist, da wir in jedem Weg aus $\mathcal{G}_1$ die Kanten 13 und 24 in $\mathcal{G}_1$ durch einen Streckenzug aus $\mathcal{G}_2$ ersetzen können.

Sei hiernach AB eine Kante von $\mathcal{G}_2$ außerhalb der oben konstruierten „Acht". Dann gibt es in $\mathcal{G}_1$ einen Weg von A nach R und einen Weg von B nach S. Also gibt es nach Ersetzung auch in $\mathcal{G}_2$ einen Weg von A nach R und einen Weg von B nach S. Folglich kann AB keine Brücke sein, weshalb $\mathcal{G}_2$ brückenlos ist. □

ANMERKUNG: Es sei noch erwähnt, dass jeder 3-reguläre Graph eine Brücke enthält oder schlingenfrei ist.

Denn: eine Schlinge führt in 3-regulären Graphen zwangsläufig zu einer Brücke.

2. 1. 7 Satz. *Sei $\mathcal{G}$ ein zusammenhängender endlicher, brückenloser Graph, derart dass von jeder Ecke genau zwei blaue und genau eine rote Kante auslaufen. Dann ist jede Kante aus $\mathcal{G}$ in genau einem alternierend(rot-blauen)en Kreis enthalten.*

BEWEIS. Wir gehen aus von einem Gegenbeispiel von minimaler Eckenzahl.

(a) $\mathcal{G}$ besitze ein Zweieck AB, BA. Dann kann es keine dritte Kante mit den Endpunkten A und B geben, da $\mathcal{G}$ zusammenhängend sein sollte, und es können die dritten Kanten mit A oder B als Ecke keine gemeinsame Ecke haben, da $\mathcal{G}$ brückenlos sein sollte. Folglich haben wir eine Situation, wie skizziert mittels Abbildung 2.4.

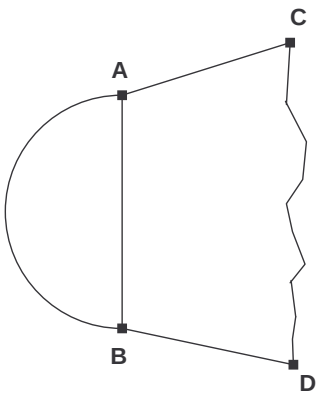


Abbildung 2.4: Zur alternierenden Färbung

Wir löschen nun in $\mathcal{G}$ die Ecken A, B, sowie die Kanten AB, BA, AC, BD und ziehen eine neue Kante CD ein. Der so entstehende Graph $\mathcal{G}'$ besitzt zwei Ecken weniger und erfüllt die Voraussetzungen des Satzes. Also erfüllt er bei entsprechender Färbung auch die Behauptung des Satzes. Dann überträgt sich aber nach Konstruktion diese Eigenschaft von $\mathcal{G}'$ auf $\mathcal{G}$, wie der Leser leicht bestätigt (ÜBUNG) □

Hiernach lässt sich beweisen:

2.1.8 Der Petersensche Satz. *Jeder endliche, brückenlose, 3-reguläre Graph lässt sich so färben, dass an jede Ecke (genau) zwei blaue und (genau) eine rote Kante anstoßen.*

BEWEIS. Sei $\mathcal{G}$ unter allen Gegenbeispielen eines von kleinster Eckenzahl. Dann ist $\mathcal{G}$ insbesondere zusammenhängend und wir dürfen den 2-Eckenfall ausschließen, da er eine Färbung der gewünschten Art evidenterweise zulässt.

Folglich verfügen wir im „Minimalfall" über einen Untergraphen des Typs der Abbildung 2.5.

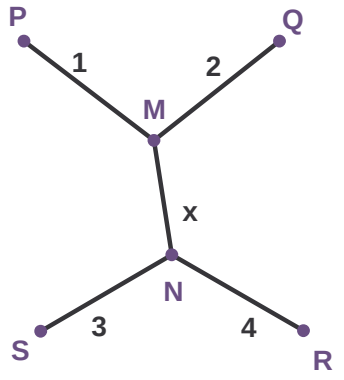


Abbildung 2.5: Zur alternierenden Färbung

und demzufolge über ein zusammenhängendes brückenloses 3-reguläres $\mathcal{G}_1$, das sich faktorisieren lässt.

Dann lässt sich aber auch $\mathcal{G}$ faktorisieren. Denn man dekliniere

- (α) PS=13 blau und 24=QR blau
- (β) PS=13 blau und 24=QR rot
- (γ) PS=13 rot und 24=QR blau
- (δ) PS=13 rot und 24=QR rot.

Wir färben jeweils 1,3 wie 13 und 2,4 wie 24 und wählen unter (α) für x die Farbe rot und unter (β), (γ) und (δ) für x die Farbe blau. □

HINWEIS: Der hier bewiesene Satz geht im wesentlichen auf PETERSEN zurück.

Kapitel 3

Trennungssätze

3.1 König – Hall – und van der Waerden

Vorweg einige Begriffe:

3. 1. 1 Definition. Seien $\mathbf{A} = \{A_1, ..., A_p\}$ und $\mathbf{B} = \{B_1, ..., B_q\}$ disjunkte Eckenmengen aus $\mathcal{G}$. Dann sagen wir, dass $\mathbf{A}$ und $\mathbf{B}$ durch die Eckenmenge $\mathbf{T}$ getrennt werden, wenn jeder Weg, der einen Punkt aus $\mathbf{A}$ mit einem Punkt aus $\mathbf{B}$ verbindet, durch mindestens eine Ecke aus $\mathbf{T}$ läuft. $\mathbf{T}$ heißt in diesem Fall auch eine *trennende Eckenmenge*.

Unter allen $\mathbf{A}$ und $\mathbf{B}$ trennenden Eckenmengen gibt es (natürlich) eine von kleinster Mächtigkeit. Ist diese Mächtigkeit gleich n, so heißt n die *Trennungszahl* zu $\mathbf{A}$ und $\mathbf{B}$, i.Z. $n =: \tau(\mathbf{A}, \mathbf{B})$.

Ein Graph $\mathcal{G}$ heißt paar, wenn sich seine Eckenmenge derart in zwei Untermengen $\mathbf{A}, \mathbf{B}$ zerlegen lässt, dass jede Kante aus $\mathcal{G}$ eine Ecke aus $\mathbf{A}$ mit einer Ecke aus $\mathbf{B}$ verbindet.

Am Anfang steht

3. 1. 2 Der Satz von König. *Sei $\mathcal{G}$ ein paarer Graph bezüglich $\mathbf{A}, \mathbf{B}$ mit der Trennungszahl n. Dann gibt es mindestens n paarweise ecken-disjunkte Kanten A_iB_i $(A_i \in \mathbf{A}, B_i \in \mathbf{B},\ 1 \leq i \leq n)$.*

BEWEIS. (a) Sei $A_1B_1, ..., A_mB_m$ eine maximale Menge paarweise disjunkter Kanten. Dann kann keine von allen $A_1, ..., A_m$ verschiedene Ecke mit einer von allen $B_1, ..., B_m$ verschiedenen Ecke verbunden sein. Deshalb ist jedes A außerhalb

$\{A_1, ..., A_m\}$ verbunden mit einem B aus $\{B_1, ..., B_m\}$. Wir nehmen o.B.d.A. an, es seien dies die Ecken B_1 bis B_k.

(b) Es kann aber auch kein Element aus $\{A_{k+1}, ..., A_m\}$ mit einem Element aus $\mathbf{B} - \{B_1, ..., B_m\}$ verbunden sein. Denn wäre etwa o.B.d.A. A_m verbunden mit $B \in \mathbf{B} - \{B_1, ..., B_m\}$ und B_m verbunden mit $A \in \mathbf{A} - \{A_1, ..., A_m\}$,so könnten wir die Kante A_mB_m ersetzen durch die Kante A_mB und die Kante AB_m hinzunehmen, mit Widerspruch zu der angenommenen Maximalität.

(c) Wir betrachten nun die Ecken aus $\{A_{k+1}, ..., A_m\}$, die mit einer der Ecken B_1 bis B_k verbunden sind. Sei etwa o.B.d.A. A_m verbunden mit B_1.

Ist dann auch eine Ecke $B \in \mathbf{B} - \{B_1, ..., B_m\}$ mit A_1 verbunden, so ersetzen wir die Kanten A_1B_1 und A_kB_k durch die Kanten A_kB_1 und A_1B. Dies führt zu einer maximalen Menge paarweise disjunkter Kanten der gegebenen Art mit den gleichen Ecken A_1 bis A_m, in der allerdings eine B-Ecke weniger verbunden ist mit Ecken aus $\mathbf{A} - \{A_1, ..., A_m\}$.

Deshalb dürfen wir davon ausgehen, dass schon in unserem „Start-n-tupel" keins der $A_{k+1}, ..., A_m$ verbunden ist mit einem $B_1, ..., B_k$, so dass alle Kanten, die auslaufen von B_1 bis B_k in $A_1, ..., A_k$ enden, also, vgl. (a), dass alle Kanten, die auslaufen von $\mathbf{B} - \{B_{k+1}, ..., B_m\}$ in $\{A_1, ..., A_k\}$ enden.

(d) Dann bildet aber $\{A_1, ..., A_k, B_{k+1}, ..., B_m\}$ eine trennende Eckenmenge zu $\mathbf{A}, \mathbf{B}$. Und das bedeutet, dass $m = n$ erfüllt sein muss. □

Aus dem Satz von König folgt der *Transversalensatz*, auch bekannt als

3. 1. 3 Der Satz von Hall. *Sei $\mathcal{M} = \{\mathbf{T}_1, ..., \mathbf{T}_l\}$ ein System von Mengen, derart dass für $k = 1, ..., n$ die Vereinigung je k vieler dieser Mengen mindestens k viele verschiedene Elemente enthalten. Dann existiert ein Repräsentantensystem von n paarweise verschiedenen Elementen $a_i \in \mathbf{T}_i$.*

BEWEIS. Wir bilden $\mathbf{M} = \bigcup_1^l \mathbf{T}_i$ und hiernach $\mathcal{M} \cup \mathbf{M}$ [1)] und verbinden x mit A gdw. $x \in A$. Auf diese Weise entsteht ein paarer Graph, seine Trennungszahl sei n. Ist dann $\mathbf{T} = \{a_1, ..., a_k, \mathbf{T}_{k+1}, ..., \mathbf{T}_n\}$ eine trennende Eckenmenge minimaler Anzahl, eine solche Annahme ist bei entsprechender Etikettierung möglich, so „hängt" an jedem $a_i, 1 \leq i \leq k$ eins der $\mathbf{T}_j, j \notin \{k+1, ..., n\}$ o.B.d.A. das $\mathbf{T}_i$ und an jedem der $\mathbf{T}_j,\ k+1 \leq j \leq n\}$ ein $a_l, l \notin \{1, ..., k+1\}$, o.B.d.A. das Element a_j.

[1)] Obacht: Es ist also zu unterscheiden zwischen a und $\{a\}$.

Damit sind n der Mengen aus dem System $\mathcal{M}$ berücksichtigt.

Wäre nun $n < l$, so gäbe es noch mindestens ein $\mathbf{T}_\lambda$ das unberücksichtigt blieb. Dann bilden wir $\mathbf{N} = \mathbf{T}_\lambda \cup \bigcup_1^n \mathbf{T}_i$ i. S. unserer Etikettierung. $\mathbf{N}$ enthält mindestens $n+1$ verschiedene Elemente, also auch eines, etwa a_λ, verschieden von allen $a_i, 1 \leq i \leq n$. Dann wäre aber $\mathbf{T}$ keine trennende Eckenmenge, da $\mathbf{T}$ von der Kante $\mathbf{T}_\lambda, a_\lambda$ $\mathbf{T}$ nicht getroffen würde.

Also wurden alle Elemente aus $\mathcal{M} = \{\mathbf{T}_1, ..., \mathbf{T}_l\}$ berücksichtigt. □

Als Interpretation des Satzes von Hall ergibt sich

3. 1. 4 Der Heiratssatz. *Sei h die Anzahl der Herren auf einer Party, d die Anzahl der Damen. Dann kann jeder der Herren eine ihm bekannte Dame „heimführen", wenn j $(1 \leq j \leq h)$ viele Herren jeweils gemeinsam mindestens j viele der Damen kennen.*

BEWEIS. Bezeichnen wir die Menge der mit einem Herren A jeweils bekannten Damen mit $D(A)$, so bildet die Menge aller dieser $D(A)$ ein Mengensystem im Sinne des Satzes von HALL, weshalb es eine Transversale gibt, d.h. eine Menge von Damen, so dass aus den einzelnen $D(A)$ paarweise verschiedene Damen gewählt werden können, also jeder Herr in der Tat eine ihm bekannte Dame „heimführen" kann. □

Und als eine weitere Interpretation des Satzes von Hall ergibt sich

3. 1. 5 Der Satz für Demokraten. *Damit ein Gemeinderat unter Berücksichtigung der Geschlechter-, Konfessions-, Vereins-, der Alters-Interessen ... frei von Interessenkonflikten besetzt werden kann, genügt es, wenn sich unter den Mitgliedern je k vieler Interessengruppen, wenigstens k viele finden, die paarweise verschiedenen dieser Gruppen angehören.*

Beachte: In kleinen Gemeinden sind gewisse „Vereinsmeier" zugleich in allen Vereinen vertreten, Kaninchenzuchtverein... inklusive.

Weiter folgt

3. 1. 6 Der Satz von van der Waerden. *Es sei die Menge M auf zwei verschiedene Weisen in n paarweise disjunkte Klassen zerlegt* [2)], *etwa $M =$*

[2)] Dies gilt etwa für die Felder einer $n \times n$-Matrix, insbesondere also eines Schachbrettes, die ja nach Zeilen und Spalten aufgeteilt sind

$\bigcup_1^n A_i = \bigcup_1^n B_i$. *Dann gibt es ein Repräsentantensystem* $x_1, ..., x_n$, *derart dass jedes seiner Elemente zu (genau) einem Paar von Klassen* A_k, B_l *gehört.*

BEWEIS. Wir betrachten die A_i und B_i als Ecken eines Graphen und verbinden ein A_k mit einem B_l genau dann, wenn diese beiden Komponenten ein gemeinsames Element besitzen. Auf diese Weise entsteht ein paarer Graph.

Sei nun m die Trennungszahl und $(A_1, ..., A_k, B_{k+1}, ..., B_m)$ eine trennende Eckenmenge – eine solche Indizierung ist durch Umnummerierung möglich. Dann muss m gleich n sein, denn es ist ja jedes der $B_1, ..., B_k$ mit einem der $A_1, ..., A_k$ und jedes der $A_{k+1}, ..., A_n$ mit einem der $B_{k+1}, ..., B_m$ verbunden. Das bedeutet: wäre $m < n$, also $\bigcup B_1^m \subset M$, so gäbe es ein a, das in zwei verschiedenen B-Komponenten läge, mit Widerspruch! □

Aus dem Satz von van der Waerden folgt natürlich unmittelbar

3. 1. 7 Der Satz von Miller. *Ist* $\mathfrak{G}$ *eine endliche Gruppe und* $\mathfrak{U}$ *eine Untergruppe von* $\mathfrak{G}$, *so besitzen das System Rechtsklassen nach* $\mathfrak{U}$ *und das System der Linksklassen nach* $\mathfrak{N}$ *ein gemeinsames Repräsentantensystem.*

Nach diesem Ausflug in die Kombinatorik nun zu

3.2 Menger – Ford – und – Fulkerson

3. 2. 1 Der S(ch)atz von Menger. *Sind* $\mathbf{A}$ *und* $\mathbf{B}$ *zwei disjunkte Eckenmengen eines endlichen Graphen und ist* n *die zugehörige Trennungszahl, so gibt es mindestens* n *kreuzungsfreie Wege von* $\mathbf{A}$ *nach* $\mathbf{B}$.

BEWEIS. **(a)** Wir reduzieren $\mathcal{G}$ durch Kantenstreichung solange dies ohne Reduktion der Trennungszahl möglich ist. Dann erhalten wir einen Teilgraphen, in dem die Trennungszahl für $\mathbf{A}, \mathbf{B}$ ebenfalls gleich n ist, und dessen Wege natürlich auch Wege in $\mathcal{G}$ sind.

Wir können also gleich von dieser Voraussetzung ausgehen.

(b) Im Falle $\mathbf{A} \cup \mathbf{B} = \mathbf{G}$ greift der Satz von König, man betrachte den Untergraphen aller Kanten von $\mathbf{A}$ nach $\mathbf{B}$.

(c) Daher dürfen wir ein $R_0 \notin \mathbf{A} \cup \mathbf{B}$ annehmen.

(d) Der Satz gilt für die Kantenzahl 1.

(e) Wir heben nun R_0 mit allen anstoßenden Kanten ab und gelangen so zu $\mathcal{G}'$, in dem $\mathbf{A}$ und $\mathbf{B}$ durch $\{R_1, ..., R_{n-1}\}$ getrennt werden und $n-1$ paarweise ecken-disjunkte Wege von $\mathbf{A}$ nach $\mathbf{B}$ existieren.

Dann werden $\mathbf{A}$ und $\mathbf{B}$ in $\mathcal{G}$ aber getrennt durch $\mathbf{M} = \{R_0, R_1, ..., R_{n-1}\}$.

(f) Wir setzen $\mathbf{M}_0 := \mathbf{M} - \{\mathbf{A} \cup \mathbf{B}\}$, $\mathbf{M}_1 := \mathbf{M} \cap \mathbf{A}$, $\mathbf{M}_2 := \mathbf{M} \cap \mathbf{B}$ und $m_0 := |\mathbf{M}_0|$, $m_1 := |\mathbf{M}_1|$, $m_2 := |\mathbf{M}_2|$. Dann ist $\mathbf{M}_0 + \mathbf{M}_1 + \mathbf{M}_2 = \mathbf{M}$ und $m_0 + m_1 + m_2 = n$.

Läuft nun jeder Weg von $\mathbf{A}$ nach $\mathbf{B}$, der durch R_0 läuft auch durch eine der Ecken $R_1, ..., R_{n-1}$, so sind wir fertig. Sonst aber ist $\mathbf{M}$ eine trennende Eckenmenge zu $\mathbf{A}$ und $\mathbf{B}$ von minimaler Anzahl in $\mathcal{G}$, und es gibt einen Weg $\mathcal{W}$, der von $\mathbf{A}$ nach $\mathbf{B}$ durch R_0 läuft nicht aber durch $\mathbf{M}_1$ oder $\mathbf{M}_2$.

(g) Als nächstes halten wir fest, dass $\mathbf{A} - \mathbf{M}_1$ nicht leer ist. Beachte, wäre $\mathbf{A} - \mathbf{M}_1 = \emptyset$, so wäre $\mathbf{A}$ in $\mathbf{M}$ enthalten, also $|\mathbf{A}| < n = |\mathbf{M}|$, wegen $R_0 \notin \mathbf{A}$, mit Widerspruch dazu, dass $\mathbf{A}$ eine trennende Eckenmenge und n Trennungszahl ist.

(h) Hiernach bilden wir die Graphen $\mathcal{G}_1$ aller unverkürzbaren Wege von $\mathbf{A} - \mathbf{M}_1$ nach $\mathbf{M}_0 \cup \mathbf{M}_2$, die frei sind von Punkten aus $\{R_1, ..., R_{n-1}\}$, und analog den Graphen $\mathcal{G}_2$.

$\mathcal{G}_1$ und $\mathcal{G}_2$ sind nicht leer, man beachte den Weg $\mathcal{W}$ aus **(f)**.

(i) Gehört nun eine Ecke sowohl zu $\mathcal{G}_1$ als auch zu $\mathcal{G}_2$, so gehört sie natürlich zu $\mathbf{M}_0$, da $\mathbf{A}$ und $\mathbf{B}$ ja fremd sind, und es sind $\mathcal{G}_1$ und $\mathcal{G}_2$ kanten-disjunkt, da die Wege aus $\mathcal{G}_1$ und $\mathcal{G}_2$ ja unverkürzbar sein sollten.

(k) $\mathcal{G}_1$ und $\mathcal{G}_2$ sind nicht leer, man beachte den Weg $\mathcal{W}$ aus **(e)**, und haben weniger Kanten als $\mathcal{G}$, erfüllen also die Induktionsvoraussetzung.

(l) Die Trennungszahl p von $\mathbf{A} - \mathbf{M}_1$ und $\mathbf{M}_0 \cup \mathbf{M}_2$ in $\mathcal{G}_1$ ist gleich $m_0 + m_2$, da wir sonst $\mathbf{A}$ und $\mathbf{B}$ durch $p + m_1 < n$ viele Ecken trennen könnten.

(m) Schließlich ziehen wir die Induktionsvoraussetzung heran und gehen aus von $m_0 + m_1$ bzw. $m_0 + m_2$ vielen Wegen aus $\mathcal{G}_1$ bzw. $\mathcal{G}_2$, die paarweise kanten-disjunkt sind und von denen sich m_0 viele an Ecken aus $\mathbf{M}_0$ anstoßende Wege aus $\mathcal{G}_2$ zu m_0 vielen Wegen von $\mathbf{A}$ nach $\mathbf{B}$ so zusammensetzen lassen, dass schließlich n viele ecken-disjunkte Wege von $\mathbf{A}$ nach $\mathbf{B}$ konstruiert sind. □

ÜBUNG: Man bestätige, dass der Satz von Menger auch für gerichtete Graphen gilt, wenn man Wege durch Bahnen ersetzt.

ÜBUNG: Man zeige: Der Satz von Menger ist gleichbedeutend damit, dass in jedem endlichen Graphen gilt: Lassen sich A und B durch n Ecken aus $\mathbf{G}-\{A,B\}$ trennen, nicht aber durch $n-1$ viele Ecken aus $\mathbf{G}-\{A,B\}$, so gibt es n keuzungsfreie Wege von A nach B.

Der vorauf gegangene Satz handelt von kreuzungsfreien Wegen, also ecken-disjunkten Wegen von A nach B. Wir zeigen jetzt noch, dass gleiches für kanten-disjunkte Wege gilt. Ist dabei n die Minimalzahl A,B trennender Kanten, so bezeichnen wir n mit $\tau^*(A,B)$.

3. 2. 2 Der Mengersche Satz in seiner Dualform. *Es seien A und B verschiedene Ecken (Knoten) eines Graphen, Mehrfach-Kanten und Schlingen zugelassen. Dann ist sie Maximalzahl $\omega^*(A,B)$ kanten-disjunkter Wege von A nach B gleich der Minimalzahl $\tau^*(A,B)$ A und B trennender Kanten von $\mathcal{G}$.*

BEWEIS. Offenbar haben die Schlingen keinen Einfluss auf die Aussage, weshalb wir von einem schlingenfreien Graphen ausgehen dürfen. Wir betrachten nun den Interchange-Graphen $\mathcal{G}^*$ zu $\mathcal{G}$. Man beachte, dass $\mathcal{G}^*$ keine Mehrfachkanten enthält, selbst dann nicht, wenn $\mathcal{G}$ Mehrfachkanten enthält. Hiernach adjungieren wir zwei Zusatzecken A^* und B^* zu $\mathcal{G}^*$ und verbinden A^* und entsprechend B^* mit denjenigen Ecken von $\mathcal{G}^*$, die, aufgefasst als Kanten von $\mathcal{G}$, mit der Ecke von A bzw. B inzidieren. Dann liefert uns die Anwendung des obigen Satzes von Menger auf diesen Graphen und eine Übertragung des Ergebnisses auf $\mathcal{G}$ die Behauptung des Satzes. □

3.3 Zum Satz von Ford und Fulkerson

In memoriam Klaus Wagner (1910–2000)

Dieser Abschnitt sei Klaus Wagner gewidmet. Ohne ihn wäre die Homepage des Autors möglicherweise blütenweiß. Dabei ist anzunehmen, dass Klaus Wagner die Dissertation des Autors nach echt Hilbert'scher Art gelesen hat,[3)] was das sei (?) frag' nach bei (HEINRICH) BEHNKE („Das ist es doch, mein lieber Herr Bosbach, wovon die Universität lebt, das Gespür für Substanz"), und obwohl der Autor nicht eine Arbeit von Klaus Wagner gelesen hat – immer wieder „kam

[3)] Die erste Arbeit des Autors wurde angeregt durch die von K. Wagner angeregte Dissertation von Josef Hintzen, während ihrer Verfertigung erkrankte K. Wagner schwer und fand erst zurück zu seiner großen Schaffenskraft, als die Arbeit des Autors abgeschlossen war.

die Algebra dazwischen", hat ein wunderbarer persönlicher Kontakt von 1958 bis zum Tode Klaus Wagners bestanden.

Die wissenschaftliche Wirkung von Klaus Wagner ist nachzulesen in „The Mathematics Genealogy", als seine Abkommen in der Graphentheorie von internationalem Rang seien in chronologischer Reihenfolge erwähnt die Kommilitonen des Autors ADOLF JUNG, RUDOLF HALIN, WOLFGANG MADER und Wagners langjähriger hoch engagierter Co-Autor REINER BODENDIEK, der von der Zahlentheorie zur Graphentheorie „konvertierte", zwar nicht als Doktorand, wohl aber als Wagners Mitarbeiter und Habilitand. Nicht zuletzt die Begründung einer hoch angesehenen (deutschen) Schule für Graphenthorie führte spät, aber nicht zu spät, zur Ehrendoktorwürde der Mercator-Universität Duisburg, auf die KLAUS WAGNER sehr stolz war, was denn sonst? Die entsprechende Urkunde zierte zuletzt die Wand in K. Wagners Wohn-Raum des Konrad-Adenauer-Seniorenheims, in dem der 90-jährige immer noch nachdachte über Graphen, insbesondere über das Vierfarbenproblem.

Dies alles scheint Grund genug, die nachfolgende Passage zum *Satz von Ford und Fulkerson* dem Buch „Graphentheorie" von Klaus Wagner (B.I. Verlag) – mit marginalen Abänderungen, insbesondere drucktechnischer Art, als ein Stück KLAUS WAGNER im Original zu seinem 100. Geburtstag als eine Spur „hin zum Meister" zu übernehmen.

Inhaltlich wird es um einen Satz von FORD UND FULKERSON aus der Transporttheorie gehen, den DIRAC aus dem Satz von Menger für gerichtete Graphen hergeleitet hatte, bevor K. WAGNER zeigen konnte, dass auch umgekehrt der Satz von FORD UND FULKERSON auf kurzem Wege zu dem Satz von Menger für gerichtete Graphen führt.

Doch wenngleich wir Wagner im Original präsentieren wollen, so soll doch eine Abbildung dem Leser Gelegenheit geben, die einzelnen Schritte zu konkretisieren.

Trennende Kantenmengen sind hier jeweils in gleicher Farbe gehalten.

Man beachte, dass sich durch eine vertikale Verschiebung einer Kante der gerichtete Graph nicht ändert und auch nicht durch Verlängerung oder Verkürzung. Daher können wir Rohre, die nicht von Q auslaufen stets als Rohre gleicher Länge auf gleicher Höhe annehmen. In unserer Abbildung sind drei verschiedene Dicken gewählt, die wären im Beweis aufzulösen in Einfach-, Zweifach- und Dreifachkanten.

O-TON WAGNER:

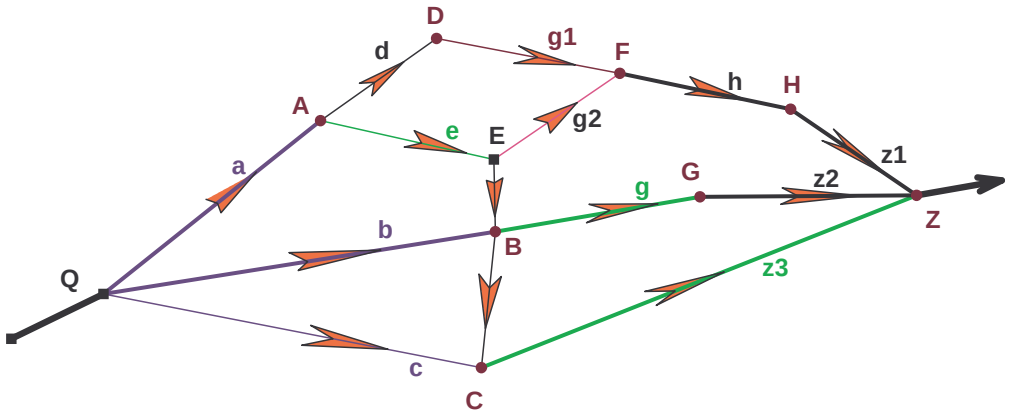


Abbildung 3.1: Ecken zu Kanten

Der Satz von *Ford–Fulkerson* handelt von *Transportnetzen*. Man versteht unter einem Transportnetz $(\vec{\mathcal{G}}, \Phi)$ einen gerichteten, endlichen Graphen $\vec{\mathcal{G}}$ mit einer nicht negativen reellen Funktion Φ, die über der Kantenmenge K von $\vec{\mathcal{G}}$ definiert ist $(\Phi(k) \geq 0, k \in K)$. Die Funktion Φ heißt die *Kapazität* des Transportnetzes $(\vec{\mathcal{G}}, \Phi)$. Für jede Kante k von $\vec{\mathcal{G}}$ heißt der Wert $\Phi(k)$ die *Kapazität von* k. Um ein praktisches Beispiel vor Augen zu haben, vergleiche man $(\vec{\mathcal{G}}, \Phi)$ mit dem Rohrsystems eines Wasserwerks, wobei die Rohre k von unterschiedlicher Stärke (Durchmesser) $\Phi(k)$ seien. Weiter stelle man sich vor, dass in jedem Rohr k etwa vermöge eines Ventils das Wasser nur in einer Richtung in k (gemäß der Orientierung von k) fließen kann. Man habe nun zwei Knotenpunkte Q und Z in $(\vec{\mathcal{G}}, \Phi)$. Die Ventile sollen so gestellt werden, dass in jedem von Q und Z verschiedenen Knotenpunkt von $(\vec{\mathcal{G}}, \Phi)$ die einfließende gleich der ausfließenden Wassermenge ist. Im folgenden handelt es sich um die Frage: Wie groß ist die *maximale* Wassermenge die bei Q oder Z ein- bzw. [ausströmen kann]? Wir präzisieren die eben erläuterten Begriffe.

Man habe ein Transportnetz $(\vec{\mathcal{G}}, \Phi)$. Weiter habe man eine nicht negative reelle Funktion φ, die über der Kantenmenge K von $\vec{\mathcal{G}}$ definiert ist. Es sei X_0 eine Ecke von $\vec{\mathcal{G}}$. Dann versteht man unter der Ergiebigkeit von φ in X_0 oder auch unter dem *Fluss von* φ *in* X_0, in Zeichen[4)] $\varphi'(X_0)$:

$$\varphi'(X_0) = \sum_{k \in K^-(X_0)} \varphi(k) - \sum_{k \in K^+(X_0)} \varphi(k)\,.$$

[4)] Anm. d. Autors: W. definiert zuvor: Ist X eine Eckenmenge aus $\vec{\mathcal{G}}$, so sei $K^-(X)$ die Menge derjenigen Kanten, deren Startpunkt außerhalb von X liegt und deren Zielpunkt in X liegt, also die Menge der Kanten, die „von draußen nach X laufen", und analog $K^+(X)$ die Menge der Kanten, die von X nach draußen laufen.

Es seien [nun] Q und Z zwei verschiedene Ecken aus $\vec{\mathcal{G}}$. Eine Funktion $\varphi(k)$, $k \in K$ heißt ein Fluss in $(\vec{\mathcal{G}}, \Phi)$ zwischen Q und Z oder auch Z und Q, wenn 1. $0 \leq \varphi(k) \leq \Phi(k)$ für jede Kante k von $\vec{\mathcal{G}}$ und 2. $\varphi'(X_0) = 0$ für jede Ecke $X_0 \neq Q, Z$ von $\vec{\mathcal{G}}$ gilt. Ist φ ein Fluss in $(\vec{\mathcal{G}}, \Phi)$ zwischen Q und Z, so folgt aus $\sum_{X_0 \neq Q,Z} \varphi'(X_0) = 0$ leicht $\varphi'(Z) = -\varphi'(Q)$. Man kann die beiden Bedingungen für φ [natürlich] auch so deuten, dass 1. der Fluss in jeder Kante k des Transportnetzes $(\vec{\mathcal{G}}, \Phi)$ nicht größer als die Kapazität von k sein darf, 2. bei jedem Knotenpunkt $X_0 \neq Q, Z$ von $(\vec{\mathcal{G}}, \Phi)$ die gleiche Menge ein- wie ausströmen soll. Das Transportproblem lautet nun: *Wie groß ist das Maximum von φ' für alle möglichen Flüsse φ'*? Hierbei sollen die Flüsse wohlgemerkt immer auf das feste Q und Z bezogen sein. Dieses Maximum heißt der *Maximalfluss* von $(\vec{\mathcal{G}}, \Phi)$. Wir bezeichnen ihn mit

$$\max_{\varphi} \varphi'(Z).$$

Auf der anderen Seite betrachten wir trennende Kantenmengen von $\vec{\mathcal{G}}$ in dem Sinne, dass jede Bahn von Q nach Z in $\vec{\mathcal{G}}$ mindestens eine Kante der betrachteten Kantenmenge enthält. Im folgenden bedeute $\mathbf{B}$ immer eine Eckenmenge von $\vec{\mathcal{G}}$ mit $Z \in \mathbf{B}$ und $Q \notin \mathbf{B}$. Dann ist $K^-(\mathbf{B})$, wie man leicht sieht, immer eine trennende Eckenmenge. Diese (speziellen) trennenden Kantenmengen heißen *Schnitte*. Aber auch umgekehrt stellt man leicht fest, dass es zu jeder trennenden Kantenmenge K' stets ein $\mathbf{B}$ (mit $b \in B$ und $a \notin \mathbf{B}$) gibt, mit $K^-(\mathbf{B}) \subseteq K'$. Denn ein solches $\mathbf{B}$ ist [ja etwa] die Menge aller Ecken von $\vec{\mathcal{G}}$, von denen aus eine Bahn nach Z existiert, die keine Kante von K' enthält. Hieraus folgt unmittelbar, dass die Funktion:

$$\Phi(K^-(\mathbf{B})) = \sum_{k \in K^-(\mathbf{B})} \Phi(k)\,, \tag{3.1}$$

genommen für alle Schnitte $K^-(\mathbf{B})$ von $\vec{\mathcal{G}}$ zwischen Q und Z das gleich Minimum besitzt wie die Funktion:

$$\Phi(K') = \sum k \in K' \Phi(k), \tag{3.2}$$

genommen für alle Q und Z trennenden K'. Dieses Minimum heißt die *Minimalkapazität* der Schnitte von $\vec{\mathcal{G}}$ zwischen Q und Z. Wir bezeichnen sie mit:

$$\min_{\mathbf{B}} \Phi(K^-(\mathbf{B})).$$

In den praktischen Fällen sind alle „transportierten Mengen" in Transportnetzen immer ein ganzzahliges Vielfaches einer bestimmten Zahl (Norm) $q > 0$. Daher

setzen wir voraus, dass alle Werte der betrachteten Flüsse in einem Transportnetz (nicht negative) ganzzahlige Vielfache eines solchen $q > 0$ [sind].

Dann lautet der

3. 3. 1 Satz von Ford und Fulkerson. *Ist $(\vec{\mathcal{G}}, \Phi)$ ein Transportnetz, so ist für je zwei verschiedene Ecken Q und Z von $(\vec{\mathcal{G}}, \Phi)$ der Maximalfluss von $(\vec{\mathcal{G}}, \Phi)$ in Z gleich der Minimalkapazität der Schnitte von $\vec{\mathcal{G}}$ zwischen Q und Z, in Zeichen:*

$$\max_{\varphi} \varphi'(b) = \min_{\mathbf{B}} \Phi(K^-(\mathbf{B}))$$

Beweis (DIRAC). Zunächst stellt man vermöge einer Division aller beteiligten Funktionen durch q leicht fest, dass es genügt, den Satz für $q = 1$ zu beweisen. Setzen wir also voraus, dass die Werte von Φ und die Werte der beteiligten Flüsse ganze Zahlen ≥ 0 sind. Wir betrachten den Graphen $\vec{\mathcal{G}}_\Phi$, der aus $\vec{\mathcal{G}}$ gemäß $\Phi(k) \geq 0$ durch jeweils $\Phi(k)$-madige Vervielfältigung der Kanten k von $\vec{\mathcal{G}}$ entsteht. Anschaulich gesprochen soll jede Kante k von $\vec{\mathcal{G}}$ durch ein Bündel von $\Phi(k)$ solcher Kanten ersetzt werden. Für $\Phi(k) = 0$ lösche man die Kante k. Analog sei $\vec{\mathcal{G}}_\varphi$ definiert. Wegen $0 \leq \varphi(k) \leq \Phi(k)\,(k \in K)$ ist $\vec{\mathcal{G}}_\varphi$ stets ein Teilgraph von $\vec{\mathcal{G}}_\Phi$. Mittels der obigen Beziehungen (3.1), (3.2) sowie 3.2.2 folgt sofort

$$\omega^*_{\vec{\mathcal{G}}_\varphi}(Q, Z) = \min_{\Phi}(K^-(\mathbf{B}))\,. \tag{3.3}$$

Wir bezeichnen die Kantenmenge von $\vec{\mathcal{G}}_\varphi$ mit $\vec{K}_\varphi$. Dann folgt andererseits:

$$\varphi'(b) + |K^+{}_{\varphi(\mathbf{B})}| = |K^-{}_{\varphi(\mathbf{B})}| \tag{3.4}$$

für jede Teilmenge $\mathbf{B}$ der Eckenmenge E von $\vec{\mathcal{G}}$ mit $Z \in \mathbf{B}$ und $Q \notin \mathbf{B}$. Man braucht ja nur $\varphi'(X_0)$ über alle Ecken von $\mathbf{B} - \{Z\}$ zu summieren. Übrigens benutzen wir an dieser Stelle des Beweises (und nur hier) die Voraussetzung, dass $\vec{\mathcal{G}}$ endlich ist. Aus (3.4) folgt [dann]:

$$\varphi'(Z) \leq |K^-_\varphi(\mathbf{B})|\,. \tag{3.5}$$

Betrachtet man (3.5) bei einem festen φ und allen $\mathbf{B}\,, (Z \in \mathbf{B}, Q \notin \mathbf{B})$, so ergibt sich $\varphi'(Z) \leq \tau^*_{\vec{\mathcal{G}}_\varphi}(Q, Z)$, da (3.1) und (3.2) entsprechend für φ [gelten], also nach 3.2.2 auch $\varphi'(Z) \leq \omega^*_{\vec{\mathcal{G}}_\varphi}(Q, Z)$ [erfüllt ist]. Umgekehrt ist $\max_\varphi \varphi'(Z)$ größer oder gleich $\omega^*_{\vec{\mathcal{G}}_\varphi}(Q, Z)$, da die Vereinigung der $\omega^*_{\vec{\mathcal{G}}_\varphi}(Q, Z)$ [vielen] kantendisjunkten Q, Z-Bahnen von $\vec{\mathcal{G}}_\Phi$ ein $\vec{\mathcal{G}}_\varphi$ bilden mit $\varphi'(Z) = \omega^*_{\vec{\mathcal{G}}_\varphi}(Q, Z)$. Also

gilt:

$$\max_{\varphi} \varphi'(Z) = \omega^*_{\vec{\mathcal{G}}_\varphi}(Q, Z)\,. \tag{3.6}$$

Mit (3.3) und (3.6) ist der Satz 3.3.1 bewiesen.

.....

Wir wollen zum Schluss [noch] zeigen, dass aus dem Satz von *Ford-Fulkerson* auch umgekehrt [wie von WAGNER bewiesen] der Mengersche Satz 3.2.2 für gerichtete endliche Graphen folgt.

[Hierzu seien] $\vec{\mathcal{G}}$ ein gerichteter endlicher Graph und Q und Z [] zwei verschiedene Ecken von $\vec{\mathcal{G}}$. Man wähle die konstante Kapazität $\Phi = 1$ in $\vec{\mathcal{G}}$. Dann folgt nach Satz 3.3.1 $\max_\varphi \varphi'(Z) = \tau^*_{\vec{\mathcal{G}}_\varphi}(Q, Z)$ für $q = 1$. Nun gilt aber immer $\omega^*_{\vec{\mathcal{G}}_\varphi}(Q, Z) \geq \varphi'(Z)$ für jeden Fluss φ. Denn $\vec{\mathcal{G}}_\varphi$ sei der Graph, der aus $\vec{\mathcal{G}}$ durch Streichung aller Kanten mit $\varphi(k) = 0$ entsteht. [Dann] gilt offenbar $\omega^*_{\vec{\mathcal{G}}}(Q, Z) \geq \omega^*_{\vec{\mathcal{G}}_\varphi}(Q, Z)$. Streicht man in $\vec{\mathcal{G}}_\varphi$ die $\omega^*_{\vec{\mathcal{G}}_\varphi}(Q, Z)$ kanten-disjunkten Q, Z-Bahnen, so erhält man ein $\vec{\mathcal{G}}_{\varphi_0}$. Da φ_0 wieder ein Fluss ist und $\vec{\mathcal{G}}_{\varphi_0}$ keine Q, Z-Bahn enthält, folgt leicht $\varphi_0(Z) \leq 0$ und daher $\omega^*_{\vec{\mathcal{G}}}(Q, Z) \geq \varphi'(Z)$. Also gilt auch $\omega^*_{\vec{\mathcal{G}}}(Q, Z) \geq \max_\varphi \varphi'(Z)$. Daraus folgt: $\omega^*_{\vec{\mathcal{G}}}(Q, Z) \geq \tau^*_{\vec{\mathcal{G}}}(Q, Z)$ und wegen $\omega^*_{\vec{\mathcal{G}}}(Q, Z) \leq \tau^*_{\vec{\mathcal{G}}}(Q, Z)$ [dann] die Behauptung $\omega^*_{\vec{\mathcal{G}}}(Q, Z) = \tau^*_{\vec{\mathcal{G}}}(Q, Z)$.

Man kann also sagen, dass der Satz von *Ford-Fulkerson* mit dem Satz [...] von Menger für gerichtete Graphen [in dem Sinne] äquivalent ist, [dass man von jedem der beiden Sätze auf kurzem Wege zu dem jeweils anderen gelangt].

Literaturverzeichnis

[1] Bodendiek, Rainer & Rainer Lang: *Lehrbuch der Graphentheorie.* Spektrum, Akademischer Verlag, Heidelberg-Berlin-Oxford, Band 1 1995, Band 2 1996.

[2] König, Dénes: *Theorie der endlichen und unendlichen Graphen.* (Leipzig 1936). Chelsea Publishing Company, New York, New Yersey 1950.

[3] Wagner, Klaus: *Graphentheorie.* Bibliographisches Institut AG, Mannheim 1970.

Stichwortverzeichnis