Fourier-Matrizen und Ringe mit Basis

Dissertation
zur
Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften (Dr. rer. nat.)

im Fachbereich Mathematik/Informatik
der Universität Kassel

vorgelegt von
Michael Cuntz
aus
Berlin

Kassel im Juni 2005

Inhaltsverzeichnis

Einleitung

Bei der Bestimmung der irreduziblen Charaktere einer Gruppe vom Lie-Typ entwickelte Lusztig eine Theorie, in der eine sogenannte Fourier-Transformation auftaucht. Dies ist eine Matrix, die nur von der Weylgruppe der Gruppe vom Lie-Typ abhängt. Anhand der Eigenschaften, die eine solche Fourier-Matrix erfüllen muß, haben Geck und Malle in [12] ein Axiomensystem aufgestellt. Dieses ermöglicht es Broué, Malle und Michel, zu gewissen komplexen Spiegelungsgruppen Fourier-Matrizen zu bestimmen, insbesondere auch für die Spetses (siehe [21]), über die noch vieles unbekannt ist.

Das Ziel dieser Arbeit ist eine Untersuchung und neue Interpretation dieser Fourier-Matrizen (Kapitel 8), die hoffentlich weitere Informationen zu den Spetses liefert. Die Werkzeuge, die dabei entstehen, sind sehr vielseitig verwendbar, denn diese Matrizen entsprechen gewissen $\mathbb{Z}$-Algebren, die im Wesentlichen die Eigenschaften einer Tafelalgebra besitzen. Tafelalgebren spielen in der Charaktertheorie eine wichtige Rolle, weil z.B. der Charakterring einer endlichen Gruppe und das Zentrum einer Gruppenalgebra Tafelalgebren sind. Außerdem finden wir sie in der Quantenfeldtheorie (in Form von Darstellungsringen). In der Theorie der Kac-Moody-Algebren gibt es die sogenannte Kac-Peterson-Matrix, die auch die Eigenschaften unserer Fourier-Matrizen besitzt.

Ein wichtiges Resultat dieser Arbeit (Sätze 5.1.4, 5.1.5, Bemerkung 5.2.1 und Korollar 5.2.3) ist, daß die Fourier-Matrizen, die G. Malle zu den komplexen imprimitiven Spiegelungsgruppen in [20] definiert, tatsächlich die Eigenschaft besitzen, daß die Strukturkonstanten der zugehörigen Algebren ganze Zahlen sind. Dazu müssen äußere Produkte von Gruppenringen von zyklischen Gruppen untersucht werden. Außerdem gibt es einen Zusammenhang zu den Kac-Peterson-Matrizen: Wir beweisen (Satz 6.2.1), daß wir durch Bildung äußerer Produkte von den Matrizen vom Typ $A_1^{(1)}$ zu denen vom Typ $C_l^{(1)}$ gelangen.

Lusztig erkannte in [16], daß manche seiner Fourier-Matrizen zum Darstellungsring des Quantendoppels einer endlichen Gruppe gehören. Deswegen ist es naheliegend zu versuchen, die noch ungeklärten Matrizen als solche zu identifizieren. Coste, Gannon und Ruelle untersuchen diesen Darstellungsring in [6]. Er heißt dort modulares Datum, weil die Fourier-Matrix zusammen mit einer weiteren Matrix eine Darstellung der Gruppe $\mathrm{SL}_2(\mathbb{Z})$ definiert. In [6] wird eine Reihe von wichtigen Fragen gestellt. Eine dieser Fragen beantworten wir in

7.3, nämlich inwieweit rekonstruiert werden kann, zu welcher endlichen Gruppe gegebene Matrizen gehören.

In [8], [9] und [6] wird ein getwistetes Quantendoppel eingeführt. Den Darstellungsring dieser Algebra berechnen wir hier für viele Beispiele am Computer. Dazu müssen unter anderem Elemente aus der dritten Kohomologie-Gruppe $H^3(G, \mathbb{C}^\times)$ explizit berechnet werden. Dieses wurde bisher anscheinend in keinem Computeralgebra-System implementiert. Leider ergibt sich hierbei kein Zusammenhang zu den von Spetses herrührenden Matrizen.

Wir beschreiben nun den Aufbau der Arbeit.

Im ersten Kapitel wird die zentrale Struktur der Arbeit definiert, die eine Variante des Ringes mit Basis von Lusztig (siehe [16]) ist und deshalb hier A-Ring mit Basis genannt wird. Ein $\mathbb{Z}$-Ring mit Basis ($A = \mathbb{Z}$) ist im Wesentlichen eine Tafelalgebra, die auch negative Strukturkonstanten haben kann. Das zweite Kapitel erklärt den Zusammenhang zwischen diesen Ringen und den Fourier-Matrizen. Anschließend wird untersucht, welche Ringe aus Tensorprodukten und symmetrischen Potenzen von Fouriermatrizen entstehen.

Die wichtigsten Werkzeuge der Arbeit, die es in dieser Form noch nicht gab, werden im dritten und vierten Kapitel definiert: Sie ermöglichen eine strukturelle Zerlegung der $\mathbb{Z}$-Ringe mit Basis in bekannte Anteile. Wichtig sind hier die Teilringe zu Teilmengen der Basis eines $\mathbb{Z}$-Ringes mit Basis. Es wird bewiesen (Proposition 3.1.4), daß sie wieder $\mathbb{Z}$-Ringe mit Basis sind. Außerdem wird gezeigt (Korollar 3.1.7), wie sie bei Charakterringen von endlichen Gruppen aussehen. Die meisten der Ringe, die uns interessieren, besitzen solche Teilringe und eine Graduierung, die auch im dritten Kapitel eingeführt wird.

Im fünften Kapitel wird beschrieben, wie äußere Produkte von Matrizen neue Ringe liefern. Diese sind im Spezialfall der Matrizen zu den Gruppenringen von zyklischen Gruppen die Fourier-Matrizen zu den imprimitiven komplexen Spiegelungsgruppen. Es wird gezeigt, daß die Strukturkonstanten ganzzahlig sind. Der Zusammenhang zu den Kac-Moody-Algebren wird im darauf folgenden Kapitel erklärt.

Im siebten Kapitel wird der Darstellungsring des Quantendoppels einer endlichen Gruppe untersucht. Es wird zunächst bewiesen (dies ist zum Beispiel in [2] zu finden), daß die Kategorie der endlichdimensionalen komplexen Darstellungen eine modulare Tensorkategorie ist. Die zugehörige Fusionsalgebra $K(\mathcal{C})$ (der Grothendieck-Ring dieser Kategorie) ist ein Ring mit Basis, dessen Teilringstruktur beschrieben wird. Wir geben ein Ideal I in $K(\mathcal{C})$ an, so daß der Faktorring $K(\mathcal{C})/I$ torsionsfrei ist. Dieses Ideal spielt im letzten Kapitel wieder eine Rolle.
Die durch einen 3-Kozykel getwistete Version des Darstellungsrings des Quantendoppels wurde bisher noch nicht explizit berechnet. Wir können damit die Klassifikation aus [6] aller Matrizen mit bis zu 20 Zeilen und Spalten erweitern und präzisieren.

Im letzten Kapitel wenden wir schließlich die bisher gewonnenen Werkzeuge an, um die Ma-

trizen der Spetses zu klassifizieren. Die zugehörigen $\mathbb{Z}$-Algebren sind Faktorringe von Tensorprodukten von affinen Ringen, Charakterringen und von Darstellungsringen von Quantendoppeln.
Es bleiben nur 3 der 274 Matrizen übrig, die etwas zu groß für Berechnungen am Computer sind, und deshalb nicht leicht beschrieben werden können. Auch die Fourier-Matrix zur Ree-Gruppe ${}^2F_4(q^2)$ bleibt unerklärt. Der zugehörige Ring wird dennoch sehr genau im letzten Abschnitt untersucht. Er hat eine auffällige Ähnlichkeit mit dem Darstellungsring des Quantendoppels der symmetrischen Gruppe S_4.
Die meisten Konstruktionen laufen darauf hinaus, daß ein Ring R und ein Ideal $I \trianglelefteq R$ gefunden werden müssen, so daß der Faktorring R/I zusammen mit einer „kanonischen" Basis der gesuchte Ring ist.
Es stellt sich heraus (siehe 8.2.3), daß für bestimmte Familien der Gruppen G_{25}, G_8 und G_{32} (Numerierung von Shephard und Todd [26]) ähnliche Ideale gewählt werden können.
Einige Familien bei den Gruppen G_4, G_6, G_{14} und G_{24} haben Fourier-Matrizen, die aus affinen Ringen durch eine Art von „Twist" entstehen (siehe 8.2.1).

Ich danke Herrn Gunter Malle für die ausgezeichnete Zusammenarbeit und für seine Unterstützung während der Anfertigung der Arbeit. Ferner danke ich Herrn David Green für verschiedene Gespräche über Gruppenkohomologie. Für das Korrekturlesen der Rohfassung bedanke ich mich bei Herrn Malle und bei Britta Späth. Nicht zuletzt danke ich meiner Freundin Ana Borwitzky für eine letzte Durchsicht der Arbeit und für ihre moralische Unterstützung.

Kapitel 1

A-Ringe mit Basis

Auf der Menge der Isomorphieklassen von Darstellungen einer endlichen Gruppe G haben wir zwei Operationen: Die direkte Summe und das Tensorprodukt. Diese Operationen erfüllen die Assoziativ- und Distributivgesetze, so daß diese Menge ein Ring wäre, wenn sie noch inverse Elemente bezüglich der direkten Summe hätte. Gehen wir zur Grothendieckgruppe über (wir nehmen „negative" Elemente hinzu), so erhalten wir den sogenannten Darstellungsring $R(G)$ von G.

Eine endliche Gruppe hat bekanntlich bis auf Isomorphie endlich viele irreduzible Darstellungen über $\mathbb{C}$, und alle Darstellungen zerlegen sich in eine direkte Summe von irreduziblen Darstellungen. So ist insbesondere das Tensorprodukt von zwei irreduziblen Darstellungen eine direkte Summe von irreduziblen Darstellungen mit gewissen nicht negativen ganzen Vielfachheiten, die Strukturkonstanten des Darstellungsrings genannt werden: Sind $V_1, \ldots, V_n$ Vertreter der irreduziblen Darstellungen von G (bis auf Isomorphie), so gilt im Darstellungsring

$$V_i \otimes V_j = \bigoplus_k N_{ij}^k V_k$$

mit natürlichen Zahlen N_{ij}^k, wobei mit $N_{ij}^k V_k$ die N_{ij}^k-fache direkte Summe von V_k gemeint ist. Dieser Ring hat viele schöne Eigenschaften, die daraus folgen, daß er mit $\mathbb{C}$ über $\mathbb{Z}$ tensoriert halbeinfach ist.

Der Darstellungsring einer Gruppe oder Algebra und der Gruppenring sind zwei unter vielen Beispielen für endlichdimensionale freie $\mathbb{Z}$-Algebren mit ähnlichen Eigenschaften. Es ist daher sinnvoll eine Struktur zu definieren, die die wichtigsten dieser Eigenschaften hat. Dieses wurde von vielen Mathematikern aus unterschiedlichen Richtungen getan. Ein Grund dafür könnte sein, daß über solche Ringe viele Aussagen gemacht werden können.

In der Physik werden diese im allgemeinen Fusionsalgebren oder Algebren mit Fusionsregeln genannt. Diese wurden in der Kategorientheorie zu modularen Tensorkategorien (siehe

zum Beispiel [2]) verallgemeinert.
Lusztig definiert 1987 in [16] im Kontext der Theorie der Heckealgebren den Begriff eines „based ring“ (wir schreiben „Ring mit Basis“). Er zeigt auch einen Zusammenhang zu den Algebren aus der Physik, insbesondere zum Darstellungsring des Quantendoppels einer endlichen Gruppe. Außerdem definiert er später (1994) in [17] das sogenannten Fusionsdatum, das ähnliche Daten wie die modulare Tensorkategorie beinhaltet und auch einen Ring mit Basis definiert.
In der Charaktertheorie gibt es noch eine weitere Struktur, die Tafelalgebra, die 1987 von Arad und Blau definiert wurde. Die Bose-Mesner-Algebra eines Assoziationsschemas ist eines der motivierenden Beispiele. Für Fusionsalgebren gibt es bei Lusztig und bei Blau und Zieschang [3] allerdings völlig unterschiedliche Definitionen.

Alle genannten Strukturen haben gemeinsam, daß die Strukturkonstanten positive Zahlen (aus $\mathbb{N}_0$ oder $\mathbb{R}_{\geq 0}$) sind. Weil wir aber auch an Ringen mit negativen Strukturkonstanten interessiert sind, ist keine von diesen Strukturen für unsere Zwecke geeignet. Wir werden eine Variante des Ringes mit Basis verwenden.

1.1 Ringe mit Basis

1.1.1 Definition

Wir beginnen mit Lusztigs Definition eines Ringes mit Basis (vergleiche mit [16]).
Es sei R ein assoziativer (nicht notwendig kommutativer) Ring mit 1, der ein freier endlich erzeugter $\mathbb{Z}$-Modul mit der Basis $B = \{b_i \mid i \in I\}$ ist. Für die Multiplikation gelte:

$$b_i b_j = \sum_{k \in I} N_{ij}^k \, b_k, \quad N_{ij}^k \in \mathbb{N}_0. \tag{1.1}$$

Die Zahlen N_{ij}^k heißen **Strukturkonstanten** von R. Wir setzen voraus, daß es eine Teilmenge I_0 von I gibt, so daß

$$1 = \sum_{i \in I_0} b_i.$$

(Anders als in [16] behauptet wird, folgt dies nicht aus (1.1), wie man am Beispiel $B = \{a, b\}, a^2 = b, ab = ba = a + b, b^2 = a + 2b, 1 = b - a$ sieht.)

Bemerkung 1.1.1. *Die b_i, $i \in I_0$, sind paarweise orthogonale Idempotente von R.*

Beweis. Es sei $a := b_i$ für ein $i \in I_0$. Mit $b := 1 - a$ haben wir $a^2 + ab = a(a + b) = a \cdot 1$, d.h. $a^2 = 0$ oder $ab = 0$, weil a^2 und ab in der Darstellung mittels B nur nicht-negative Koeffizienten haben. Andererseits ist auch $a^2 + ba = a$, also $ab = ba$. Demnach ist

$$1 = (a + 1 - a)^2 = (a + b)^2 = a^2 + 2ab + b^2,$$

und somit $ab = 0$, weil alle Koeffizienten in der Zerlegung der 1 kleiner als 2 sind. Wir haben also $b_i^2 = b_i$. Daraus folgt

$$b_i = b_i \cdot 1 = \sum_{j \in I_0} b_i b_j = b_i^2 + \sum_{j \in I_0, j \neq i} b_i b_j = b_i + \sum_{j \in I_0, j \neq i} b_i b_j.$$

Damit ist $\sum_{j \in I_0, j \neq i} b_i b_j = 0$ und daraus folgt $N_{ij}^k = 0$ für alle $k \in I$, $i, j \in I_0$ mit $i \neq j$. $\square$

In einem Gruppenring sind Elemente der zugrunde liegenden Gruppe invertierbar. Im Darstellungsring einer endlichen Gruppe hat jede irreduzible Darstellung V eine zugehörige irreduzible Darstellung $\tilde{V}$, so daß $V \otimes \tilde{V}$ einen Anteil an der Eins hat, nämlich die kontragrediente Darstellung. Invertierbar ist sie jedoch im allgemeinen nicht. Dennoch können wir daraus folgern, daß der Darstellungsring mit $\mathbb{C}$ tensoriert halbeinfach ist. Wir benötigen eine Abschwächung der Existenz eines inversen Elements, aus der diese Eigenschaft immer noch folgt. Der Anteil an der Eins ist durch den $\mathbb{Z}$-Modulhomomorphismus

$$\tau : R \to \mathbb{Z}, \quad b_i \mapsto \delta_{i \in I_0},$$

gegeben ($\delta_{i \in I_0}$ ist 1 für $i \in I_0$ und 0 sonst). Dann fordern wir die Existenz einer Involution $\sim: R \to R$, die $\mathbb{Z}$-linear ist und die Eigenschaften

$$\widetilde{r \cdot r'} = \tilde{r}' \cdot \tilde{r}, \quad r, r' \in R,$$

$$b \in B \Rightarrow \tilde{b} \in B,$$

$$\tau(bb') = \delta_{b', \tilde{b}}, \quad b, b' \in B,$$

erfüllt. Daraus folgt sofort $\tilde{b}_i = b_i$ für $i \in I_0$, d.h.

$$\tau(\tilde{r}) = \tau(\sum_{i \in I} \lambda_i \tilde{b}_i) = \tau(\sum_{i \in I_0} \lambda_i \tilde{b}_i) = \tau(\sum_{i \in I_0} \lambda_i b_i) = \tau(r)$$

für alle $r = \sum_{i \in I} \lambda_i b_i \in R$.
Sind alle obigen Bedingungen erfüllt, so heißt $(R, B, \sim)$ ein **Ring mit Basis**. Für $i \in I$ schreiben wir $\tilde{i}$ für den Index mit $b_{\tilde{i}} = \tilde{b}_i$. Für die Strukturkonstanten schreiben wir manchmal auch $N_{b_i b_j}^{b_k}$ statt N_{ij}^k.

Der Prototyp eines Ringes mit Basis ist der Grothendieck-Ring der Darstellungen einer endlichdimensionalen Algebra über einen Körper k mit den irreduziblen Darstellungen als Basis. Die Menge I_0 besteht aus einem Element, der trivialen Darstellung k. Die Abbildung $\sim$ bildet ein V auf den dualen Raum V^* ab.

Anmerkung 1.1.2. Obwohl wir an keiner Stelle Tafelalgebren verwenden werden, ist es wichtig begleitend zu erwähnen, daß es sie gibt, und inwiefern die Definitionen in der zugehörigen Theorie (siehe [3]) von den unseren abweichen.
Eine **Tafelalgebra** (A, B) ist eine endlich dimensionale Algebra A über den komplexen Zahlen $\mathbb{C}$, und eine ausgezeichnete Basis $B = \{b_0 = 1_A, b_1, b_2, \ldots, b_m\}$ von A mit

(a) Für alle $a, b \in B$ ist $ab = \sum_{c \in B} N_{a,b}^c c$ für geeignete $N_{a,b}^c \in \mathbb{R}^+ \cup \{0\}$.

(b) Es gibt einen Algebrenantiautomorphismus $\sim$ von A mit $\tilde{\tilde{a}} = a$ für alle $a \in A$, $\tilde{B} = B$ und für alle $a, b \in B$

$$N_{a,b}^1 = 0 \text{ für } b \neq \tilde{a}, \quad N_{a,\tilde{a}}^1 = N_{\tilde{a},a}^1 > 0.$$

Die Tafelalgebra unterscheidet sich vom Ring mit Basis im Wesentlichen darin, daß die Strukturkonstanten in $\mathbb{R}^+ \cup \{0\}$ liegen dürfen, und daß $N_{a,\tilde{a}}^1$ ungleich 1 sein darf. Außerdem beachte man, daß sie eine $\mathbb{C}$-Algebra und nicht eine $\mathbb{Z}$-Algebra ist. Das heißt: Ist (R, B) ein Ring mit Basis mit $1 \in B$, so ist $R \otimes_{\mathbb{Z}} \mathbb{C}$ mit der Basis $\{b \otimes 1 \mid b \in B\}$ eine Tafelalgebra.

Wie bereits angekündigt, ist ein Ring mit Basis mit $\mathbb{C}$ tensoriert als $\mathbb{C}$-Algebra halbeinfach (Lusztig zeigt in [16], daß der Ring mit $\mathbb{Q}$ tensoriert als $\mathbb{Q}$-Algebra halbeinfach ist):

Bemerkung 1.1.3. *Es sei R ein Ring mit Basis. Dann ist die Algebra $R_{\mathbb{C}} := R \otimes_{\mathbb{Z}} \mathbb{C}$ halbeinfach.*

Beweis. Wir setzen die Abbildung $\sim$ auf $R \otimes_{\mathbb{Z}} \mathbb{C}$ fort: $\widetilde{r \otimes z} := \tilde{r} \otimes \bar{z}$. Die obige Abbildung τ definiert eine Sesquilinearform auf $R_{\mathbb{C}}$,

$$\langle r, r' \rangle := \tau'(\tilde{r} r'),$$

wobei $\tau' : R_{\mathbb{C}} \to \mathbb{C}$, $r \otimes z \mapsto z\tau(r)$. Für $r = \sum_k b_k \otimes \lambda_k \in R_{\mathbb{C}}$ ist

$$\langle r, r \rangle = \tau'(\tilde{r} r) = \sum_{k,j} \bar{\lambda}_k \lambda_j \tau(\tilde{b}_k b_j) = \sum_k \bar{\lambda}_k \lambda_k,$$

$\langle\ ,\ \rangle$ ist also positiv definit, symmetrisch wegen $\widetilde{r \cdot r'} = \tilde{r}' \cdot \tilde{r}$ und $\tau(\tilde{r}) = \tau(r)$.
Ist $\mathfrak{I}$ ein Linksideal in $R_{\mathbb{C}}$, so ist das orthogonale Komplement

$$\mathfrak{I}^{\perp} := \{r \in R_{\mathbb{C}} \mid \langle r, r' \rangle = 0 \quad \forall r' \in \mathfrak{I}\}$$

auch ein Linksideal:

$$\langle tr, r' \rangle = \tau'(\widetilde{tr} r') = \tau'(\tilde{r} \tilde{t} r') = \langle r, \tilde{t} r' \rangle = 0$$

für alle $r \in \mathfrak{I}^{\perp}$, $t \in R_{\mathbb{C}}$ und $r' \in \mathfrak{I}$. Jedes Linksideal hat also ein Komplement, d.h. $R_{\mathbb{C}}$ ist halbeinfach. □

1.1.2 Orthogonalitätsrelation für $R_{\mathbb{C}}$-Moduln

Die irreduziblen Darstellungen von $R_{\mathbb{C}} := R \otimes_{\mathbb{Z}} \mathbb{C}$ erfüllen wie bei den endlichen Gruppen eine Orthogonalitätsrelation bezüglich eines Skalarprodukts, das auf den zugehörigen „Charakteren“ definiert ist (die Spur der Endomorphismen). Wir benötigen dafür die folgende Bemerkung:

Bemerkung 1.1.4. *Es seien E_1, E_2 zwei $R_{\mathbb{C}}$-Moduln und $h : E_1 \to E_2$ eine $\mathbb{C}$-lineare Abbildung. Die Abbildung $h_0 : E_1 \to E_2, e \mapsto \sum_{i \in I} b_i h(\tilde{b}_i e)$ ist $R_{\mathbb{C}}$-linear.*

Beweis. Für $j, k, m \in I$ ist

$$\tau(\tilde{b}_m \sum_i N^i_{jk} b_i) = \sum_i N^i_{jk} \tau(\tilde{b}_m b_i) = N^m_{jk},$$

also $\tau(b_i b_j b_k) = N^{\tilde{i}}_{jk}$.Wegen $\tau(\tilde{r}) = \tau(r)$ haben wir

$$N^i_{\tilde{j}k} = \tau(\tilde{b}_i \tilde{b}_j b_k) = \tau(\tilde{b}_k b_j b_i) = N^k_{ji}.$$

Hieraus folgt, daß h_0 ein $R_{\mathbb{C}}$-Modulhomomorphismus ist:

$$\begin{aligned} h_0(r \cdot e) = \sum_i b_i h(\tilde{b}_i \sum_k \lambda_k \tilde{b}_k e) &\overset{(*)}{=} \sum_i b_i h(\sum_k \lambda_k \sum_j N^j_{ki} \tilde{b}_j e) \\ = \sum_k \lambda_k \sum_{j,i} N^j_{ki} b_i h(\tilde{b}_j e) &= \sum_k \lambda_k \sum_{j,i} N^i_{\tilde{k}j} b_i h(\tilde{b}_j e) \\ &= \sum_k \lambda_k \tilde{b}_k \sum_j b_j h(\tilde{b}_j e) = r \cdot h_0(e), \end{aligned}$$

für $r = \sum_k \lambda_k \tilde{b}_k \in R_{\mathbb{C}}$ und $e \in E_1$, wobei die Gleichheit $(*)$ aus

$$\tilde{b}_i \tilde{b}_k = \widetilde{b_k b_i} = \widetilde{\sum_j N^j_{ki} b_j} = \sum_j N^j_{ki} \tilde{b}_j$$

folgt. □

Bemerkung 1.1.4 liefert die Orthogonalitätsrelation (siehe zum Beispiel [25] oder [16]; für die uns wichtigeren Ringe aus dem nächsten Abschnitt werden wir dies ausführen): Für zwei einfache $R_{\mathbb{C}}$-Moduln E_1, E_2 gilt

$$\sum_i \operatorname{tr}(b_i, E_1) \operatorname{tr}(\tilde{b}_i, E_2) = \begin{cases} \dim(E_1) f_{E_1} & E_1 \cong E_2 \\ 0 & E_1 \not\cong E_2 \end{cases} \tag{1.2}$$

mit passendem $f_{E_1} \in \mathbb{C}$. Dabei bezeichnet $\operatorname{tr}(b_i, E_1)$ die Spur der Operation von b_i auf E_1.

Die Zahlen f_E stehen in Beziehung mit Zahlen f'_E (siehe [16]): Die Abbildungen $R_{\mathbb{C}} \to \mathbb{C}, r \mapsto \operatorname{tr}(r, E)$ für einfache $R_{\mathbb{C}}$-Moduln E bilden eine Basis des $\mathbb{C}$-Vektorraums der $\mathbb{C}$-linearen Funktionen von $R_{\mathbb{C}}$ nach $\mathbb{C}$, die auf allen $rr' - r'r$ verschwinden. Da τ eine solche Abbildung ist, zerlegt es sich in eine Linearkombination

$$\tau(r) = \sum_E f'_E \operatorname{tr}(r, E) \tag{1.3}$$

mit passenden $f'_E \in \mathbb{C}$.

Für einen einfachen $R_{\mathbb{C}}$-Modul E haben wir dann: $f_E f'_E = 1$. (Dies folgt aus (1.3) und (1.2) für $r = b$.)

1.2 A-Ringe mit Basis

1.2.1 Definition

Einerseits ist die Definition von Lusztig etwas zu allgemein, da in allen Beispielen, die wir betrachten, die Eins ein Element der Basis ist, und alle Ringe kommutativ sind. Andererseits gibt es viele Situationen, in denen die Strukturkonstanten auch negativ sind; es ist sogar sinnvoll, zum Beispiel $\mathbb{Z}[\zeta]$ oder allgemeiner irgendeinen Unterring A von $\mathbb{C}$ als Wertebereich für die Strukturkonstanten zuzulassen. Dies motiviert die nächste Definition, die eine Variante der Definition des Ringes mit Basis ist.

In diesem Kapitel sei A immer ein Unterring der komplexen Zahlen $\mathbb{C}$. Alle Aussagen gelten zwar auch für beliebige Ringe, zusammen mit einem Homomorphismus nach $\mathbb{C}$. Damit aber die Notation nicht zu unübersichtlich wird, beschränken wir uns auf Unterringe von $\mathbb{C}$, die insbesondere kommutativ sind. In fast allen Beispielen ist $A = \mathbb{Z}$, deswegen sollte sich der Leser immer die ganzen Zahlen vorstellen.

Es sei R ein kommutativer Ring mit 1, der ein freier endlich erzeugter A-Modul mit Basis $B = \{b_0, \ldots, b_{n-1}\}$ ist. Die Eins sei in der Basis, $1 = b_0$. Für die Multiplikation gelte:

$$b_i b_j = \sum_k N_{ij}^k \, b_k, \quad N_{ij}^k \in A. \tag{1.4}$$

Wie in 1.1 haben wir eine A-lineare Abbildung

$$\tau : R \to \mathbb{C}, \quad ab_i \mapsto a\delta_{i,0}$$

für $a \in A$. Wir fordern wieder die Existenz einer Involution $\sim$ auf R mit den Eigenschaften

$$\widetilde{r_1 \cdot r_2} = \tilde{r}_2 \cdot \tilde{r}_1, \quad \widetilde{r_1 + r_2} = \tilde{r}_1 + \tilde{r}_2, \quad r_1, r_2 \in R,$$

$$b \in B \Rightarrow \tilde{b} \in B,$$

$$\tau(bb') = \delta_{b',\tilde{b}}, \quad b, b' \in B,$$

$$\widetilde{ab} = \bar{a}\tilde{b} \quad \text{für } a \in A,\ b \in B.$$

Sind alle obigen Bedingungen erfüllt, so heißt $(R, B, \sim)$ ein **A-Ring mit Basis**.

Ist $A = \mathbb{Z}$ und sind keine der Strukturkonstanten negativ, so ist $(R, B, \sim)$ ein Ring mit Basis.

Bemerkung 1.2.1. *Die Algebra $R_{\mathbb{C}} := R \otimes_A \mathbb{C}$ ist halbeinfach.*

Beweis. Die Abbildungen $\sim$ und τ setzen sich wie in Bemerkung 1.1.3 auf $R \otimes_A \mathbb{C}$ fort:

$$\widetilde{r \otimes z} := \tilde{r} \otimes \bar{z}, \quad \tau' : r \otimes z \mapsto z\tau(r).$$

Wie in Bemerkung 1.1.3 haben wir eine Sesquilinearform auf $R_{\mathbb{C}}$,

$$\langle r, r' \rangle := \tau'(\tilde{r} r').$$

Es ist leicht nachzurechnen, daß diese hermitesch und positiv definit ist. Zu einem gegebenen Ideal liefert sie ein orthogonales Komplement. Daß dieses wieder ein Ideal ist, zeigt man genau wie in Bemerkung 1.1.3. □

Die Tatsache, daß $R_{\mathbb{C}}$ halbeinfach ist, werden wir später verwenden, um jedem solchen Ring eine Matrix zuzuordnen. Nach dem Satz von Wedderburn-Artin ist nämlich $R_{\mathbb{C}}$ als Ring isomorph zu $\mathbb{C}^n$ mit komponentenweiser Multiplikation (weil R kommutativ ist). Bezüglich der kanonischen Basen wird dieser Isomorphismus durch eine Matrix beschrieben, die alle Informationen über die Struktur des Ringes beinhaltet.

Da R kommutativ ist, sind irreduzible $R_{\mathbb{C}}$-Moduln eindimensional. Wir identifizieren sie deswegen mit ihren „Charakteren“ (die Spur der Endomorphismen). Wie oben haben wir eine Orthogonalitätsrelation für irreduzible Charaktere. Diese folgt aus der folgenden Bemerkung:

Bemerkung 1.2.2. *Es seien E_1, E_2 zwei $R_{\mathbb{C}}$-Moduln und $h : E_1 \to E_2$ eine $\mathbb{C}$-lineare Abbildung. Die Abbildung $h_0 : E_1 \to E_2, e \mapsto \sum_{i \in I} b_i h(\tilde{b}_i e)$ ist $R_{\mathbb{C}}$-linear.*

Beweis. Wörtlich wie in Bemerkung 1.1.4. □

Zusammen mit dem Lemma von Schur folgt daraus:

Bemerkung 1.2.3. *Für zwei irreduzible Charaktere χ_1, χ_2 von $R_{\mathbb{C}}$ gilt die Orthogonalitätsrelation*

$$\sum_{b \in B} \chi_1(b)\chi_2(\tilde{b}) = \delta_{\chi_1,\chi_2} f_{\chi_1} \tag{1.5}$$

mit passendem $f_{\chi_1} \in \mathbb{C}^\times$.

Beweis. Es seien E_1, E_2 zu χ_1, χ_2 gehörige $R_{\mathbb{C}}$-Moduln. Ein $b \in B$ operiert auf E_1 bzw. E_2 als Skalar $\chi_1(b)$ bzw. $\chi_2(b)$. Für irgendeine $\mathbb{C}$-lineare Abbildung $h : E_2 \to E_1$ besagt Bemerkung 1.2.2, daß

$$h_0(e) = \sum_{b \in B} \chi_1(b) h(\chi_2(\tilde{b})e) = \Big(\sum_{b \in B} \chi_1(b)\chi_2(\tilde{b})\Big) h(e)$$

ein $R_{\mathbb{C}}$-Modulhomomorphismus von E_2 nach E_1 ist. Nach dem Lemma von Schur ist h_0 entweder ein Isomorphismus oder die Nullabbildung. Dieses gilt für alle $\mathbb{C}$-linearen Abbildungen h, so daß die Summe (1.5) Null ist, falls $E_1 \ncong E_2$, d.h. $\chi_1 \neq \chi_2$. Falls dagegen h_0 ein Isomorphismus ist, kann (1.5) nicht Null sein, da es mindestens ein Element aus E_2 gibt, das nicht auf Null abgebildet wird. Damit ist $f_{\chi_1} \in \mathbb{C}^\times$. □

Die Abbildungen $\tau, \sim$ kann man auch folgendermaßen interpretieren. Die Basis B verhält sich wie eine „Orthonormalbasis“ und

$$\langle r, r' \rangle := \tau(\tilde{r} r')$$

wie ein „Skalarprodukt“, denn es gilt:

Bemerkung 1.2.4. *Es sei $(R, B, \sim)$ ein A-Ring mit Basis und $r \in R$. Dann ist*

$$r = \sum_{b \in B} \tau(\tilde{b} r) b = \sum_{b \in B} \langle b, r \rangle \, b.$$

Beweis. Sind $r = \sum_{b'} c_{b'} b' \in R$, $b \in B$, so ist $\tau(br) = \tau(\sum_{b'} c_{b'} bb') = \sum_{b'} c_{b'} \tau(bb') = c_{\tilde{b}}$. □

Anders als in Ringen mit Basis gilt in A-Ringen mit Basis R für ein $r \in R$ nicht $\tau(\tilde{r}) = \tau(r)$ sondern $\tau(\tilde{r}) = \overline{\tau(r)}$. Daraus gewinnen wir wichtige Relationen zwischen den Strukturkonstanten:

Bemerkung 1.2.5. *Es sei $(R, B, \sim)$ ein A-Ring mit Basis mit Strukturkonstanten N_{ij}^k. Dann gelten für alle $0 \leq i, j, k < n$:*

$$N_{ij}^k = N_{i\tilde{k}}^{\tilde{j}} = N_{\tilde{k}j}^{\tilde{i}}, \quad N_{ij}^k = \overline{N_{\tilde{i}\tilde{j}}^{\tilde{k}}}.$$

Beweis. Wie in Bemerkung 1.1.4 können wir auch für A-Ringe mit Basis zeigen, daß $\tau(\tilde{b}_k b_i b_j) = N_{ij}^k$. Da R kommutativ ist, gilt

$$N_{ij}^k = \tau(\tilde{b}_k b_i b_j) = \tau(b_j b_i \tilde{b}_k) = N_{i\tilde{k}}^{\tilde{j}},$$

und demnach $N_{ij}^k = N_{i\tilde{k}}^{\tilde{j}} = N_{\tilde{k}i}^{\tilde{j}} = N_{\tilde{k}j}^{\tilde{i}}$. Außerdem ist $N_{ij}^k = \tau(\tilde{b}_k b_i b_j) = \overline{\tau(b_k \tilde{b}_i \tilde{b}_j)} = \overline{N_{\tilde{i}\tilde{j}}^{\tilde{k}}}$. □

In den nächsten Abschnitten wollen wir die Struktur von A-Ringen mit Basis etwas genauer untersuchen. Wir sind besonders an $\mathbb{Z}$-Ringen mit Basis ($A = \mathbb{Z}$) interessiert. Deswegen führen wir für diese einen Isomorphiebegriff ein.

1.2.2 Isomorphie von $\mathbb{Z}$-Ringen mit Basis

In vielen Fällen kommen $\mathbb{Z}$-Ringe mit Basis von Matrizen (siehe 2.1.3), die in der entsprechenden Theorie bis auf Permutationen der Spalten und Multiplikation mit Vorzeichen eindeutig bestimmt sind.

Wir wollen deshalb isomorphe Ringe, bei denen es keinen Isomorphismus bzgl. der beiden Basen gibt, der eine monomiale Matrix mit Einträgen 1 oder -1 ist, als nicht isomorph ansehen. Dies motiviert die folgende Definition:

Definition 1.2.6. Es seien R_1, R_2 $\mathbb{Z}$-Ringe mit den Basen $B_1 = \{b_1, \ldots, b_{n_1}\}$ und $B_2 = \{b'_1, \ldots, b'_{n_2}\}$. Sie heißen **isomorph**, falls $n_1 = n_2$ ist, und es eine Permutation $\sigma \in S_{n_1}$ und eine Abbildung $\nu : B_1 \to \{-1, 1\}$ gibt, so daß der durch

$$R_1 \to R_2, \quad b_i \mapsto \nu(b_i) b'_{\sigma(i)}$$

definierte $\mathbb{Z}$-Modulhomomorphismus ein Ringisomorphismus ist.

Anmerkung 1.2.7. Ist (R, B) ein $\mathbb{Z}$-Ring mit Basis und $\nu : B \to \{-1, 1\}$ eine Abbildung, so wird R als $\mathbb{Z}$-Algebra auch von der Menge

$$B' := \{\nu(b)b \mid b \in B\}$$

erzeugt. Im Allgemeinen ist (R, B') aber kein $\mathbb{Z}$-Ring mit Basis (siehe 5.1 für ein Beispiel).

Kapitel 2

Matrizen zu $\mathbb{Z}$-Algebren

Wie schon im letzten Kapitel angesprochen wurde, können wir jedem $\mathbb{Z}$-Ring mit Basis eine Matrix zuordnen. Ist dagegen eine Matrix mit bestimmten Eigenschaften gegeben, so erhalten wir aus ihr über die Formel von Verlinde die Strukturkonstanten eines Ringes. Im Falle eines $\mathbb{Z}$-Ringes mit Basis können wir sogar die Abbildung $\sim$ an den Spalten dieser Matrix ablesen. Damit beinhaltet die Matrix alle Daten des Ringes.

2.1 Definition

2.1.1 Beispiel

Zur Motivation betrachten wir zuerst ein Beispiel, und zwar die Matrix

$$s := \begin{pmatrix} 1 & 1 & 2 \\ 1 & 1 & -1 \\ 1 & -1 & 0 \end{pmatrix} \in \mathbb{C}^{3\times 3}$$

mit den Spalten v_1, v_2, v_3, die eine Basis B (von $\mathbb{C}^3$) bilden. Die Zeilen dieser Matrix sind orthogonal bezüglich des üblichen Skalarprodukts. Multiplizieren wir zwei Spaltenvektoren komponentenweise und zerlegen wir das Resultat bezüglich B, so ergeben sich immer ganze Zahlen als Koeffizienten, etwa:

$$\begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} + \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix},$$

d.h. $v_3 \cdot v_3 = v_1 + v_2 + v_3$. Das in $\mathbb{C}^3$ von v_1, v_2, v_3 erzeugte Gitter ist also multiplikativ abgeschlossen und ist eine endlich erzeugte $\mathbb{Z}$-Algebra, die hier sogar ein $\mathbb{Z}$-Ring mit Basis ist. (Dem aufmerksamen Leser wird aufgefallen sein, daß s die transponierte Charaktertafel der symmetrischen Gruppe S_3 ist).

2.1.2 Vom Ring zur Matrix

Es sei R eine endlich erzeugte kommutative $\mathbb{Z}$-Algebra mit Eins, die ein freier $\mathbb{Z}$-Modul mit den Erzeugern $b_0, \ldots, b_{n-1}$ ist. Die Multiplikation zweier Erzeuger definiert die Strukturkonstanten:

$$b_i b_j = \sum_k N_{ij}^k \, b_k, \quad N_{ij}^k \in \mathbb{Z}. \tag{2.1}$$

Ist die $\mathbb{C}$-Algebra $R \otimes_{\mathbb{Z}} \mathbb{C}$ halbeinfach, so ist sie nach dem Satz von Wedderburn-Artin (siehe zum Beispiel Theorem 2.4.1 in [10]) isomorph zur $\mathbb{C}$-Algebra $\mathbb{C}^n$ (mit komponentenweiser Multiplikation). Es sei φ ein $\mathbb{C}$-Algebrenisomorphismus

$$\varphi : R \otimes_{\mathbb{Z}} \mathbb{C} \to \mathbb{C}^n.$$

Dieser Ringisomorphismus kann bezüglich der Basis $\{b_0, \ldots, b_{n-1}\}$ von $R \otimes \mathbb{C}$ und der kanonischen Basis $\{e_1, \ldots, e_n\}$ von $\mathbb{C}^n$ als Matrix $s \in \mathbb{C}^{n \times n}$ dargestellt werden, $\varphi(b_i) = \sum_k s_{ki} e_k$. Wegen $\varphi(b_i b_j) = \varphi(b_i)\varphi(b_j)$, folgt daraus für alle k, i, j:

$$\sum_l N_{ij}^l s_{kl} = s_{ki} s_{kj}, \tag{2.2}$$

d.h. für festes k ist $b_i \mapsto s_{ki}$ eine eindimensionale Darstellung von R über $\mathbb{C}$. Sind die Zeilen von s orthogonal zueinander, so können wir diese normieren und erhalten eine Matrix $S \in \mathbb{C}^{n \times n}$ mit $S\bar{S}^T = 1$.

Ist eines der Basiselemente das Einselement der Algebra, etwa b_0, so sind alle Einträge in der entsprechenden Spalte in s gleich 1, weil b_0 auf $\sum_i e_i$ abgebildet wird. Die zugehörigen Einträge in der S-Matrix sind deshalb positive reelle Zahlen ungleich Null.

Definition 2.1.1. Wir nennen die Matrix S die zum Ring R gehörige S-**Matrix** und s die zum Ring R gehörige s-**Matrix**.

Anmerkung 2.1.2. Die S-Matrix ist abhängig von der Wahl von φ. Ein anderer Ringisomorphismus unterscheidet sich von φ um einen Automorphismus von $\mathbb{C}^n$. Die andere S-Matrix (oder s-Matrix) entsteht deshalb aus der ersten durch Permutation der Zeilen. Das bedeutet, daß die S-Matrix nur bis auf Permutation der Zeilen eindeutig bestimmt ist.

Anmerkung 2.1.3. Zu einem explizit gegebenen Ring läßt sich die s-Matrix als Lösung eines quadratischen Gleichungssystems mit $n-1$ Variablen leicht am Computer bestimmen.

Ein $\mathbb{Z}$-Ring mit Basis hat eine zugehörige S-Matrix, da er nach Bemerkung 1.2.1 mit $\mathbb{C}$ tensoriert halbeinfach ist, und die irreduziblen Darstellungen nach Bemerkung 1.2.3 die Orthogonalitätsrelation erfüllen.

2.1.3 Von der Matrix zum Ring

Ist umgekehrt eine Matrix $S \in \mathbb{C}^{n\times n}$ mit $S\bar{S}^T = 1$ gegeben, so können wir daraus unter Umständen wieder einen Ring gewinnen.

Sind alle Einträge der i_0-ten Spalte von S invertierbar, so dürfen wir

$$s_{ij} := \frac{S_{ij}}{S_{ii_0}}, \quad 1 \leq i, j \leq n,$$

setzen. Die Matrix s definiert nach der Wahl zweier Basen einen Vektorraumisomorphismus $\varphi : \mathbb{C}^n \to \mathbb{C}^n$. Wir schreiben $\tilde{R} := \mathbb{C}^n$ für den linken Raum und wählen für diesen eine Basis $\{b_i\}_i$. Der rechte Raum sei wie oben mit der Basis $\{e_i\}_i$ eine $\mathbb{C}$-Algebra mit der Multiplikation $e_i e_j = \delta_{ij} e_i$. Wir fassen φ als Ringisomorphismus auf, d.h. wir transportieren die Multiplikation vom Zielraum in den Raum $\tilde{R}$:

$$b_i b_j = \varphi^{-1}(\varphi(b_i)\varphi(b_j)).$$

So haben wir eine Ring-Struktur auf $\tilde{R} = \mathbb{C}^n$. Das Basiselement b_{i_0} wird auf $\sum_i e_i$ abgebildet, ist also die Eins in $\tilde{R}$. Wegen $\varphi(b_i) = \sum_k s_{ki} e_k$ gilt

$$b_i b_j = \varphi^{-1}(\sum_k \sum_l s_{ki} s_{lj} e_k e_l) = \sum_k s_{ki} s_{kj} \varphi^{-1}(e_k) = \sum_l \sum_k s_{ki} s_{kj} s'_{lk} b_l,$$

wobei $s' = (s'_{lk})_{l,k}$ die zu s inverse Matrix ist. Die Strukturkonstanten von $\tilde{R}$ sind

$$N_{ij}^l = \sum_k s_{ki} s_{kj} s'_{lk}, \tag{2.3}$$

oder auch (Formel von Verlinde)

$$N_{ij}^l = \sum_k \frac{S_{ki} S_{kj} \overline{S_{kl}}}{S_{ki_0}}, \tag{2.4}$$

da (wegen $S\bar{S}^T = 1$) $s'_{lk} = S_{ki_0}\overline{S_{kl}}$ gilt. Die Algebra $\tilde{R}$ ist per Definition halbeinfach. Dagegen wissen wir a priori nicht, wann die Strukturkonstanten ganze Zahlen sind, d.h. ob es eine $\mathbb{Z}$-Algebra R mit Strukturkonstanten N_{ij}^l und mit $R \otimes_{\mathbb{Z}} \mathbb{C} \cong \tilde{R}$ gibt.

Definition 2.1.4. Es sei S wie oben und es gelte $N_{ij}^l \in \mathbb{Z}$ für alle i, j, l. Dann sagen wir, die Matrix S definiert eine $\mathbb{Z}$-Algebra mit der Eins i_0.

Falls i_0 nicht aus dem Kontext gegeben ist, schreiben wir ${}_{i_0}N_{ij}^l := N_{ij}^l$ für die von der Wahl von i_0 abhängigen Strukturkonstanten. Es besteht folgender Zusammenhang zwischen verschiedenen Wahlen der Eins:

Bemerkung 2.1.5. *Es seien m_1, m_2 zwei Indizes mit $S_{lm_1}, S_{lm_2} \neq 0$ für alle l. Dann erfüllen die oben definierten Strukturkonstanten die Relation*

$$\sum_k {}_{m_2}N^k_{m_1 i}\, {}_{m_1}N^j_{m_2 k} = \delta_{ij}$$

für alle i, j. Es ist also $({}_{m_1}N^j_{m_2 i})_{i,j}$ die inverse Matrix zu $({}_{m_2}N^j_{m_1 i})_{i,j}$.

Beweis. Wegen $\sum_k S_{i_1,k}\overline{S_{i_2,k}} = \delta_{i_1,i_2}$ gilt

$$\sum_k \sum_{i_1} \frac{S_{i_1,i} S_{i_1,m_1} \overline{S_{i_1,k}}}{S_{i_1,m_2}} \sum_{i_2} \frac{S_{i_2,k} S_{i_2,m_2} \overline{S_{i_2,j}}}{S_{i_2,m_1}} = \sum_{i_1} S_{i_1,i}\overline{S_{i_1,j}} = \delta_{i,j}.$$

Dies ist nach der Formel 2.4 die gewünschte Aussage. □

2.2 S-Matrix eines $\mathbb{Z}$-Ringes mit Basis

Bemerkung 2.2.1. *Es sei $(R, B, \sim)$ ein $\mathbb{Z}$-Ring mit Basis. Dann hat R eine S-Matrix. Die Involution $\sim$ operiert auf B wie die komplexe Konjugation auf den entsprechenden Spalten von S.*

Beweis. Wie oben schon angemerkt wurde, hat ein $\mathbb{Z}$-Ring mit Basis eine S-Matrix mit orthogonalen normierten Spalten. Die Spalte zum Basiselement b_0 hat nur positive reelle Einträge $S_{k0} = \overline{S_{k0}}$.
Es sei v_i die Spalte zu $b \in B$ in S und es bezeichne $\bar{v}_i$ den zu v_i komplex konjugierten Vektor. Außerdem bezeichne $\langle\ ,\ \rangle$ das Standardskalarprodukt auf $\mathbb{C}^n$. Dann ist

$$\delta_{\tilde{i},j} = N^0_{i,j} = \sum_k \frac{S_{ki} S_{kj} \overline{S_{k0}}}{S_{k0}} = \sum_k S_{ki} S_{kj} = \langle v_i, \bar{v}_j \rangle = \langle \bar{v}_i, v_j \rangle,$$

da $\delta_{\tilde{i},j} \in \mathbb{R}$. Damit gilt

$$\bar{v}_{\tilde{i}} = \sum_j \langle \bar{v}_{\tilde{i}}, v_j \rangle v_j = \sum_j \delta_{\tilde{\tilde{i}},j} v_j = v_i,$$

da die Spalten von S eine Orthonormalbasis bilden. □

Insbesondere ist bei $\mathbb{Z}$-Ringen mit Basis die Menge der Spalten von S unter komplexer Konjugation abgeschlossen, was im allgemeinen nicht gilt. Zum Beispiel ist $R = \mathbb{Z}[\mathrm{i}]$ mit Basis $B = \{1, \mathrm{i}\}$ und $\mathrm{i}^2 = -1$ kein $\mathbb{Z}$-Ring mit Basis, da es keine geeignete Involution $\sim$ gibt. Dennoch gibt es eine zugehörige Matrix s:

$$s = \begin{pmatrix} 1 & \mathrm{i} \\ 1 & -\mathrm{i} \end{pmatrix}.$$

Die komplex konjugierte zweite Spalte ist nicht Spalte von s.

Mit Hilfe der S-Matrix können wir zeigen, daß keine Basiselemente eines $\mathbb{Z}$-Ringes mit Basis (bis auf die 1) idempotent sein können.

Proposition 2.2.2. *Es sei $(R, B, \sim)$ ein $\mathbb{Z}$-Ring mit Basis und $1 \neq b \in B$. Dann gilt $b^2 \neq b$.*

Beweis. Es seien s, S die Matrizen zu R (Notation wie oben). Angenommen ein Element $b \neq 1$ aus der Basis sei idempotent. Dann entspricht diesem Element eine Spalte v von s. Diese kann nur Einträge 0 oder 1 haben, da mit komponentenweiser Multiplikation $v \cdot v = v$ gelten soll.
Die entsprechende Spalte w in S entsteht aus v, indem wir den i-ten Eintrag durch eine positive reelle Zahl a_i teilen (die Norm der i-ten Zeile von s). Die der 1 entsprechende Spalte w_0 von S hat an der i-ten Stelle den Wert a_i^{-1}. Die Spalten von S sind aber orthogonal, d.h. $\langle w_0, w \rangle = 0$, woraus $w = 0$ folgt, da alle Einträge von w_0 positive reelle Zahlen ungleich Null sind. Es kann aber keine Spalte von S gleich dem Nullvektor sein, weil S einen Isomorphismus beschreibt. □

2.3 Fusionsdaten

Motiviert durch verschiedene von ihm als „nicht-abelsche Fourier-Transformationen" bezeichnete Matrizen sammelt Lusztig in [17] die Axiome für ein sogenanntes Fusionsdatum. Dieses beinhaltet eine solche Fouriermatrix und charakterisiert ihre Eigenschaften. Insbesondere definiert diese Matrix einen Ring mit Basis, der von Lusztig Fusionsalgebra genannt wird.

2.3.1 Definition

Es sei X eine endliche Menge mit einem ausgezeichnetem Element x_0 und mit kommutierenden Involutionen $^\sharp : X \to X$ und $^\flat : X \to X$ so, daß $x_0^\sharp = x_0^\flat = x_0$. Es seien $S = (S_{x,y})_{x,y \in X}$ eine Matrix mit komplexen Einträgen und $t = (t_x)_{x \in X}$ ein Vektor mit komplexen Einträgen ungleich Null, die durch X indiziert werden.

Wir nennen $(X, x_0, ^\sharp, ^\flat, S, t)$ ein **Fusionsdatum**, falls die folgenden Bedingungen erfüllt sind:

(a) $S_{x,y} = S_{x^\sharp,y^\flat} = S_{x^\flat,y^\sharp} = S_{x^\sharp,y^\sharp} = S_{x^\flat,y^\flat} = \overline{S}_{y,x}$, für alle $x, y \in X$;

(b) $t_{x^\flat} = t_{x^\sharp} = t_x^{-1} = \bar{t}_x$, für alle $x \in X$;

(c) $S_{x,x_0} \in \mathbb{R}_{>0}$ für alle $x \in X$, $\quad t_{x_0} = 1$;

(d) $\sum_{z\in X} S_{x,z}S_{z,y} = \delta_{x,y}$ für alle $x, y \in X$;

(e) $\sum_{u\in X} \frac{S_{x,u}S_{y,u}S_{z,u}}{S_{x_0,u}} \in \mathbb{N}$, für alle $x, y, z \in X$;

(f) $\sum_{x,y\in X} S_{u,x^\flat}S_{x,y^\flat}S_{y,z^\flat}t_x^{-1}t_y^{-1}t_z^{-1} = \delta_{u,z}$, für alle $u, z \in X$.

Anmerkung 2.3.1. Bei vielen sehr wichtigen Beispielen ist die Eigenschaft $t_{x_0} = 1$ nicht erfüllt. Es ist sinnvoll, die Definition deshalb leicht zu verallgemeinern. Wir werden, wenn es um Fusionsdaten geht, immer angeben, ob $t_{x_0} = 1$ gilt oder nicht.

Es sei $T = (t_{x,y})_{x,y\in X}$ die Matrix mit $t_{x,y} := \delta_{x,y^\flat}t_y^{-1}$. Dann erfüllen die Matrizen S und T wegen der Bedingungen (d) und (f) die Gleichungen $S^2 = 1$ und $(ST)^3 = 1$, und definieren damit eine Matrixdarstellung der Gruppe $\mathrm{PSL}_2(\mathbb{Z})$.

Wegen (a),(c),(d) und (e) ist S die S-Matrix eines Ringes mit Basis. Die durch S eindeutig bestimmte Involution $\sim$ setzt sich zusammen aus $\sharp$ und $\flat$: $\tilde{x} = x^{\sharp\flat}$.

In der Physik werden die Matrizen S, T ein **modulares Datum** genannt; allerdings erfüllen diese nicht exakt die Eigenschaften (a)-(f), sondern

(a) $S\overline{S}^T = T\overline{T}^T = 1$,

(b) T ist diagonal, S ist symmetrisch,

(c) $(ST)^3 = S^2 = C$,

wobei C eine Permutationsmatrix der Ordnung 2 ist, die mit S und T kommutiert (sie heißt „charge conjugation“). Die Matrizen S, T definieren dann eine Matrixdarstellung der Gruppe $\mathrm{SL}_2(\mathbb{Z})$ (siehe z.B. [6]).

Durch eine Substitution $T \mapsto CT$ bilden wir (grob gesprochen) ein modulares Datum auf ein Fusionsdatum ab. Es ist nämlich $(S(CT))^3 = (ST)^3C^3 = C^2 = I$. Die Matrix CT ist nicht diagonal. Hier entspricht die Permutation C der Abbildung $\flat$ von oben.

Beispiel 1. Der Darstellungsring des Quantendoppels einer endlichen Gruppe hat eine S-Matrix, die zusammen mit einer passenden T-Matrix ein Fusionsdatum definiert. Die Kategorie dieser Darstellungen ist sogar eine modulare Tensorkategorie (siehe Kapitel 7). Es ist aber nicht klar, ob wir aus einem Fusionsdatum eine Tensorkategorie gewinnen können, weil die Morphismen zwischen den einfachen Objekten (das wäre die Menge X) nicht vorgegeben sind.

2.3.2 Wess-Zumino-Witten-Verlinde-Ringe

Definition 2.3.2. Es sei $p \in \mathbb{N}$, $e = 2p$ und ζ die e-te Einheitswurzel $\exp(\pi\sqrt{-1}/p) \in \mathbb{C}$. Die Matrix

$$S := \left(\frac{(\zeta^{ij} - \zeta^{-ij})}{\sqrt{-2p}}\right)_{1\leq i,j\leq p-1}$$

bildet zusammen mit

$$t := (-\kappa^{-1}\zeta^{-\frac{j^2}{2}})_{1\leq j\leq p-1},$$

$\kappa := \exp(\frac{2\pi\sqrt{-1}}{24})$ ein modulares Datum, das sogenannte **Wess-Zumino-Witten-Verlinde-Fusionsdatum** (WZWV-Fusionsdatum) zu p, wie Verlinde es in [28] beweist. Die Interpretation als Fusionsdatum stammt von Lusztig ([17]). Hier hat Lusztig übersehen, daß es nur fast ein Fusionsdatum ist, weil die Eigenschaft $t_1 = 1$ fehlt.

Man rechnet leicht nach, daß die zugehörige Fusionsalgebra ganze Zahlen als Strukturkonstanten hat, es kommen sogar nur die Zahlen 0 und 1 vor. Die Matrix S ist ein Spezialfall einer Kac-Peterson-Matrix, die wir in Kapitel 6 genauer untersuchen werden.

2.3.3 Das Fusionsdatum $\mathrm{Dih}(p)$

In [17], Abschnitt 3 definiert Lusztig eine Reihe von Fusionsdaten, die er „dihedral fusion data" nennt. Diese werden durch eine ganze Zahl $p \geq 3$ parametrisiert. Sowohl die Definition als auch der Beweis, daß es sich um Fusionsdaten handelt, sind sehr technisch. Wir werden diese Fusionsdaten hier nicht mehr explizit gebrauchen und verzichten deshalb darauf, sie zu definieren. Für die Tabellen in Kapitel 8 führen wir die Bezeichnung $\mathrm{Dih}(p)$ für den Ring ein, der von der zugehörigen S-Matrix definiert wird.

In [17], Abschnitt 3.8 wird beschrieben, wie wir diese Ringe als Tensorkategorien ansehen können. Diese Interpretation liefert folgende Konstruktion (vergleiche 8.5.2): Es sei R der WZWV-Ring zu p (siehe Definition 2.3.2). Dann gibt es einen Teilring R' von $R \otimes R$ und ein Ideal $I \trianglelefteq R'$, so daß R'/I als $\mathbb{Z}$-Ring mit Basis isomorph zu $\mathrm{Dih}(p)$ ist (bei geeigneter Wahl der Basis).

2.4 Tensorprodukte von S-Matrizen

Es seien R, R' die gemäß der Konstruktion in 2.1.3 zu den Matrizen S, S' gehörigen $\mathbb{Z}$-Algebren. Dann sind $R \otimes \mathbb{C} \cong \mathbb{C}^{m_1}$ und $R' \otimes \mathbb{C} \cong \mathbb{C}^{m_2}$ für passende $m_1, m_2 \in \mathbb{N}$. Auf der Basis $\{e_{i_1} \otimes e_{i_2} \mid 1 \leq i_1 \leq m_1, 1 \leq i_2 \leq m_2\}$ von $\mathbb{C}^{m_1} \otimes \mathbb{C}^{m_2}$ operiert $S \otimes S'$ folgendermaßen:

$$(S \otimes S')(e_{i_1} \otimes e_{i_2}) = (\sum_{j_1} S_{j_1,i_1} e_{j_1}) \otimes (\sum_{j_2} S'_{j_2,i_2} e_{j_2}) = \sum_{j_1,j_2} S_{j_1,i_1} S'_{j_2,i_2} e_{j_1} \otimes e_{j_2}.$$

Bemerkung 2.4.1. *Die zur Matrix* $S'' := (S_{i_1,j_1} S'_{i_2,j_2})_{(i_1,i_2),(j_1,j_2)}$ *gehörige* $\mathbb{Z}$*-Algebra mit der Eins* $(1,1)$ *ist isomorph zu* $R \otimes_{\mathbb{Z}} R'$*.*

Beweis. Wir bestimmen die Strukturkonstanten ${N''}^{*}_{*,*}$ zu S'' nach der Formel von Verlinde:

$${N''}^{(k_1,k_2)}_{(i_1,i_2),(j_1,j_2)} = \sum_{(l_1,l_2)} \frac{S_{i_1,l_1} S'_{i_2,l_2} S_{j_1,l_1} S'_{j_2,l_2} \overline{S_{k_1,l_1} S'_{k_2,l_2}}}{S_{0,l_1} S'_{0,l_2}} =$$

$$= \sum_{l_1} \frac{S_{i_1,l_1} S_{j_1,l_1} \overline{S_{k_1,l_1}}}{S_{0,l_1}} \sum_{l_2} \frac{S'_{i_2,l_2} S'_{j_2,l_2} \overline{S'_{k_2,l_2}}}{S'_{0,l_2}} = N^{k_1}_{i_1,j_1} {N'}^{k_2}_{i_2,j_2},$$

wenn $N^*_{*,*}$, ${N'}^*_{*,*}$ die Strukturkonstanten von S,S' sind. Andererseits ist

$$(b_{i_1} \otimes b'_{i_2})(b_{j_1} \otimes b'_{j_2}) = (\sum_{k_1} N^{k_1}_{i_1,j_1} b_{k_1} \otimes \sum_{k_2} {N'}^{k_2}_{i_2,j_2} b'_{k_2}) = \sum_{(k_1,k_2)} N^{k_1}_{i_1,j_1} {N'}^{k_2}_{i_2,j_2} (b_{k_1} \otimes b'_{k_2}),$$

was offenbar dieselben Strukturkonstanten liefert. □

Die gleiche Aussage gilt, falls wir statt der S-Matrizen die s-Matrizen (die Darstellungsmatrix des Ringisomorphismus) verwenden. Der Ringisomorphismus $s \otimes s'$ definiert auch den Ring $R \otimes R'$.

2.5 Symmetrische Potenzen

Es sei R ein $\mathbb{Z}$-Ring mit Basis und s die zugehörige s-Matrix. Das n-fache Tensorprodukt von R über $\mathbb{Z}$ hat nach Bemerkung 2.4.1 die s-Matrix $\bigotimes^n s$. Schränken wir diese Matrix auf den symmetrischen Anteil von $\bigotimes^n (R \otimes_{\mathbb{Z}} \mathbb{C})$ ein, so ist dies eine s-Matrix zu einem Unterring von $\bigotimes^n R$ (dieser ist kein Teilring zu einer Teilmenge der Basis (siehe Abschnitt 3.1)).

Das symmetrische Produkt $\Sigma^n\mathbb{C}^e$ ist der Teilraum von $\bigotimes^n \mathbb{C}^e$, der von

$$C := \Big\{ \sum_{\sigma\in S_n} e_{i_{\sigma(1)}} \otimes \ldots \otimes e_{i_{\sigma(n)}} \mid 1 \le i_1 \le \ldots \le i_n \le e \Big\}$$

aufgespannt wird. Die Menge C ist eine Basis und hat $\binom{e+n-1}{n}$ Elemente, die durch Tupel $\bar{i} = (i_1, \ldots, i_n)$ mit $1 \le i_1 \le \ldots \le i_n \le e$ indiziert werden. Die Einschränkung $\Sigma^n s$ von $\bigotimes^n s$ auf $\Sigma^n\mathbb{C}^e$ hat bezüglich C die Darstellungsmatrix

$$(\Sigma^n s)_{\bar{i},\bar{j}} = \chi_{\bar{i}}^{-1} \sum_{\sigma\in S_n} \prod_{\nu=1}^{n} s_{i_\nu j_{\sigma(\nu)}},$$

wobei $\chi_{\bar{i}} := |\{\sigma \in S_n \mid \bar{i}^\sigma = \bar{i}\}|$ und $\bar{i}^\sigma := (i_{\sigma(1)}, \ldots, i_{\sigma(n)})$ sind. Die Matrix $\Sigma^n s$ definiert einen Ring mit ganzen Strukturkonstanten, der aber kein $\mathbb{Z}$-Ring mit Basis ist, da komplexe Konjugation auf den Spalten von $\Sigma^n s$ eine Involution $\sim$ definiert, die nicht mehr die geforderten Eigenschaften hat (siehe Beispiel 2).

Proposition 2.5.1. *Ist s die s-Matrix eines Ringes mit den Strukturkonstanten $N_{i,j}^k$, so definiert die Matrix $\Sigma^n s$ einen Ring mit den Strukturkonstanten*

$${}_\Sigma N_{\bar{i},\bar{j}}^{\bar{k}} = \sum_{\sigma_1,\sigma_2\in S_n} \chi_{\bar{i}}^{-1}\chi_{\bar{j}}^{-1} \prod_{\nu=1}^{n} N_{i_{\sigma_1(\nu)},j_{\sigma_2(\nu)}}^{k_\nu}.$$

Liegen alle $N_{i,j}^k$ in $\mathbb{N}$ bzw. $\mathbb{Z}$, so sind auch alle ${}_\Sigma N_{\bar{i},\bar{j}}^{\bar{k}}$ in $\mathbb{N}$ bzw. $\mathbb{Z}$.

Beweis. Ist s' die zu s inverse Matrix, so ist $\bigotimes^n s'$ die zu $\bigotimes^n s$ inverse Matrix. Die Einschränkung auf $\Sigma^n\mathbb{C}^e$ ändert daran nichts, d.h. $\Sigma^n s'$ ist die Inverse von $\Sigma^n s$. Damit ist

$$\begin{aligned}
{}_\Sigma N_{\bar{i},\bar{j}}^{\bar{k}} &= \sum_{\bar{m}\in C} (\Sigma^n s)_{\bar{m},\bar{i}} (\Sigma^n s)_{\bar{m},\bar{j}} (\Sigma^n s')_{\bar{k},\bar{m}} \\
&= \sum_{\bar{m}\in C} \sum_{\sigma_1,\sigma_2,\sigma_3\in S_n} \chi_{\bar{i}}^{-1}\chi_{\bar{j}}^{-1}\chi_{\bar{m}}^{-1} \prod_{\nu=1}^{n} s_{m_\nu,i_{\sigma_1(\nu)}} s_{m_\nu,j_{\sigma_2(\nu)}} s'_{k_\nu,m_{\sigma_3(\nu)}} \\
&= \sum_{m_1,\ldots,m_n=1}^{e} \sum_{\sigma_1,\sigma_2,\sigma_3\in S_n} \frac{\chi_{\bar{i}}^{-1}\chi_{\bar{j}}^{-1}}{n!} \prod_{\nu=1}^{n} s_{m_\nu,i_{\sigma_1(\nu)}} s_{m_\nu,j_{\sigma_2(\nu)}} s'_{k_\nu,m_{\sigma_3(\nu)}} \\
&= \sum_{m_1,\ldots,m_n=1}^{e} \frac{1}{n!} \sum_{\sigma_3\in S_n} \sum_{\sigma_1,\sigma_2\in S_n} \chi_{\bar{i}}^{-1}\chi_{\bar{j}}^{-1} \prod_{\nu=1}^{n} s_{m_\nu,i_{\sigma_1\sigma_3^{-1}(\nu)}} s_{m_\nu,j_{\sigma_2\sigma_3^{-1}(\nu)}} s'_{k_\nu,m_\nu} \\
&= \sum_{\sigma_1,\sigma_2\in S_n} \chi_{\bar{i}}^{-1}\chi_{\bar{j}}^{-1} \sum_{m_1,\ldots,m_n=1}^{e} \prod_{\nu=1}^{n} s_{m_\nu,i_{\sigma_1(\nu)}} s_{m_\nu,j_{\sigma_2(\nu)}} s'_{k_\nu,m_\nu},
\end{aligned}$$

was nach der Formel (2.3) die gewünschte Gleichung ist. Es gibt genau $\chi_{\bar{i}}$ Elemente σ_1 in S_n, die $\bar{i}$ invariant lassen, also auch an der hinteren Summe nichts ändern; das gleiche gilt für $\chi_{\bar{j}}$. Damit bleiben die Strukturkonstanten beim Übergang zum symmetrischen Produkt in $\mathbb{N}$ bzw. $\mathbb{Z}$. □

Beispiel 2. Es sei R der Ring $\mathbb{Z}[\mathbb{Z}/3\mathbb{Z}]$ mit s-Matrix s und $n=2$. Dann definiert $\Sigma^n s$ den Ring mit der Multiplikationstafel (siehe 3.3 für die Definition)

$$\begin{bmatrix} 1 & . & . & . & . & . \\ . & 1 & . & . & . & . \\ . & . & 1 & . & . & . \\ . & . & . & 1 & . & . \\ . & . & . & . & 1 & . \\ . & . & . & . & . & 1 \end{bmatrix}, \begin{bmatrix} . & 1 & . & . & . & . \\ . & . & 1 & 2 & . & . \\ 2 & . & . & . & 1 & . \\ . & . & . & . & 1 & . \\ . & 1 & . & . & . & 2 \\ . & . & 1 & . & . & . \end{bmatrix}, \begin{bmatrix} . & . & 1 & . & . & . \\ 2 & . & . & . & 1 & . \\ . & 1 & . & . & . & 2 \\ . & 1 & . & . & . & . \\ . & . & 1 & 2 & . & . \\ . & . & . & . & 1 & . \end{bmatrix},$$

$$\begin{bmatrix} . & . & . & 1 & . & . \\ . & . & . & . & 1 & . \\ . & 1 & . & . & . & . \\ . & . & . & . & . & 1 \\ . & . & 1 & . & . & . \\ 1 & . & . & . & . & . \end{bmatrix}, \begin{bmatrix} . & . & . & . & 1 & . \\ . & 1 & . & . & . & 2 \\ . & . & 1 & 2 & . & . \\ . & . & 1 & . & . & . \\ 2 & . & . & . & 1 & . \\ . & 1 & . & . & . & . \end{bmatrix}, \begin{bmatrix} . & . & . & . & . & 1 \\ . & . & 1 & . & . & . \\ . & . & . & . & 1 & . \\ 1 & . & . & . & . & . \\ . & 1 & . & . & . & . \\ . & . & . & 1 & . & . \end{bmatrix}.$$

Wir können durch einen passenden Basiswechsel erreichen, daß es die Involution $\sim$ gibt, nur ist dieser Basiswechsel kein $\mathbb{Z}$-Algebrenhomomorphismus.

Experimentell stellen wir fest:

Vermutung 2.5.2. *Es seien $e=2$, $n \in \mathbb{N}$ und $\tilde{N}_{i,j}^k$ die Strukturkonstanten des WZWV-Ringes zu $n+2$, wobei wir die Basis wie in Definition 2.3.2 sortieren und durch $0,\dots,n$ indizieren. Dann gilt*

$$_{\Sigma}N_{i,j}^k = \tilde{N}_{i,j}^k \binom{n-k}{(i+j-k)/2}\binom{k}{(-i+j+k)/2},$$

wobei $_{\Sigma}N_{i,j}^k$ die Strukturkonstanten zu $\Sigma^n s$ sind, wenn s die s-Matrix zu $\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$ ist (die Tupel $(i_1,\dots,i_n)$, die die Basis indizieren, haben Einträge $1 \le i_1 \le \ldots \le i_n \le 2$, werden also durch die Anzahl der Einsen im Tupel indiziert). Man beachte, daß $\tilde{N}_{i,j}^k$ immer Null ist, falls $i+j+k$ ungerade ist.

Kapitel 3

Teilringe und Graduierung in $\mathbb{Z}$-Ringen mit Basis

3.1 Teilringe zu Teilmengen der Basis

Betrachten wir zuerst den Gruppenring einer endlichen Gruppe. Wählen wir eine Untergruppe, so ist der zugehörige Gruppenring ein Unterring des gesamten Ringes. Schauen wir uns allgemeiner bei beliebigen $\mathbb{Z}$-Ringen mit Basis die Unterringe an, die als $\mathbb{Z}$-Modul von einer Teilmenge von B erzeugt werden, so stellt sich heraus, daß es im Allgemeinen nicht sehr viele sind, aber noch genug, um Aussagen über die Struktur des Ringes zu gewinnen.

Betrachten wir einen noch unbekannten Ring R, so finden wir häufig bekannte Unterringe. Manchmal können wir dann ausschließen, daß R isomorph zu einem uns schon bekannten Ring ist, da die Unterringstruktur nicht übereinstimmt. Außerdem ist R zusammen mit dem Unterring eine Ringerweiterung mit besonderen Eigenschaften, die wir im nächsten Kapitel untersuchen werden.

3.1.1 Definition

Es sei R ein $\mathbb{Z}$-Ring mit Basis B.

Definition 3.1.1. Es sei $1 \in B' \subseteq B$ eine Teilmenge der Basis, so daß das Produkt zweier Elemente aus B' eine Kombination von Elementen aus B' ist:

$$b_i b_j = \sum_{b_k \in B'} N_{ij}^k b_k \quad \text{für} \quad b_i, b_j \in B'.$$

Dann heißt die von B' erzeugte $\mathbb{Z}$-Algebra in R ein **Teilring zur Teilmenge** B'.

Beispiel 3. Der Gruppenring $\mathbb{Z}[G]$ einer endlichen Gruppe G hat als Teilringe zu Teilmengen von G genau die Ringe $\mathbb{Z}[H]$ zu den Untergruppen H von G.

Beispiel 4. Der WZWV-Ring zu $p = 6$ hat als Teilring den Charakterring der Symmetrischen Gruppe S_3.

Für die nachfolgenden Propositionen benötigen wir folgendes Lemma:

Lemma 3.1.2. *Ist R ein $\mathbb{Z}$-Ring mit Basis B, so gibt es zu jedem $b \in B$ ein $m \in \mathbb{N}$ mit $\tau(b^m) \neq 0$.*

Beweis. Es sei v die zu b gehörige Spalte der s-Matrix von R. Ist $v^m = \sum_i \lambda_i x_i$, wobei x_i die Spalten von s sind, so ist $\tau(b^m) = \lambda_0$ gleich dem Koeffizienten vor der Eins x_0.
Die zur Eins gehörige Spalte w der S-Matrix hat als Einträge die Normen der Zeilen von s, also positive reelle Zahlen. Damit ist $wv^m = \sum_i \lambda_i w x_i = \sum_i \lambda_i X_i$, wenn X_i die Spalten von S sind ($w = X_0$). Diese bilden aber eine Orthonormalbasis, d.h.

$$\tau(b^m) = \lambda_0 = \langle wv^m, w \rangle,$$

($w = \bar{w}$). Da die Multiplikation komponentenweise ist, können wir deshalb ohne Einschränkung annehmen, daß alle Einträge von v ungleich 0 sind.
Wenn die Basis n Elemente hat, so sind die Potenzen $v^0, \ldots, v^n$ von v linear abhängig. Es sei ein minimales k gewählt, so daß $v^0, \ldots, v^k$ linear abhängig sind. Dann gibt es $c_0, \ldots, c_{k-1}$ mit

$$v^k + c_{k-1}v^{k-1} + \cdots + c_0 v^0 = 0.$$

Angenommen $\tau(b^m) = 0$ für alle $m > 0$. Dann ist $\langle wv^m, w \rangle = 0$ für alle $m > 0$. Insbesondere ist auch

$$0 = \langle w(v^k + c_{k-1}v^{k-1} + \cdots + c_0 v^0), w \rangle = \langle wc_0 v^0, w \rangle = c_0 \langle w, w \rangle,$$

d.h. $c_0 = 0$. Da aber alle Einträge von v ungleich Null sind, ist v invertierbar, und es gilt $v^{k-1} + c_{k-1}v^{k-2} + \cdots + c_1 v^0 = 0$, was ein Widerspruch zur minimalen Wahl von k ist. □

Anmerkung 3.1.3. Aus dem letzten Beweis ergibt sich auch, daß die Einträge der s-Matrix eines Ringes mit Basis ganz algebraisch über $\mathbb{Z}$ sind, weil die Potenzen einer Spalte linear abhängig sind.

Wahrscheinlich gilt sogar, daß es ein m gibt mit $\tau(b^m) > 0$. Es genügt aber nicht ein m mit $\tau(b^m) \neq 0$ zu wählen und b^m zu quadrieren, denn das Quadrat eines Elements kann im Allgemeinen auch einen negativen Anteil an der Eins haben. Ist zum Beispiel $R := \mathbb{Z}[\mathbb{Z}/3\mathbb{Z}]$ mit der Basis $\{b_0, b_1, b_2\}$, so ist $\tilde{b}_1 = b_2$ und $b_1 b_2 = 1$. Dann ist $\tau(-b_0 - b_1 + b_2) = -1$ und $\tau((-b_0 - b_1 + b_2)^2) = \tau(-b_0 + 3b_1 - b_2) = -1$. Dennoch ist $\tau((-b_0 - b_1 + b_2)^3) = 5 > 0$.

Teilringe zu Teilmengen der Basis sind $\mathbb{Z}$-Ringe mit Basis:

Proposition 3.1.4. *Es sei R ein $\mathbb{Z}$-Ring mit Basis B und R' ein Teilring zur Teilmenge $B' \subseteq B$. Dann ist $\sim (R') \subseteq R'$, d.h. $(R', B', \sim_{|R'})$ ist ein $\mathbb{Z}$-Ring mit Basis.*

Beweis. Es genügt zu zeigen, daß $\tilde{b} \in B'$ für alle $b \in B'$. Seien dazu $b \in B'$ und $m \in \mathbb{N}$ mit $\tau(b^m) \neq 0$ (Lemma 3.1.2). Ist $b^{m-1} = \sum_{b'} c_{b'} b'$ für geeignete $c_{b'} \in \mathbb{Z}$, so ist

$$0 \neq \tau(b^m) = \tau(\sum_{b'} b c_{b'} b') = \sum_{b'} c_{b'} \tau(bb') = c_{\tilde{b}},$$

d.h. $\tilde{b} \in B'$ und somit $\sim (R') \subseteq R'$. □

Eine wichtige Tatsache, die wir später noch brauchen werden, ist, daß der vom Komplement der Basis B' eines Teilringes R' erzeugte $\mathbb{Z}$-Modul ein R'-Modul ist:

Proposition 3.1.5. *Ist R ein $\mathbb{Z}$-Ring mit Basis B und R' ein Teilring zur Teilmenge $B' \subseteq B$, so ist der von $B \backslash B'$ erzeugte $\mathbb{Z}$-Untermodul ein R'-Modul bzgl. der Multiplikation aus R.*

Beweis. Es sei $B'' := B \backslash B'$ und $b \in B', m \in B''$. Ist $bm = ca + r$ mit $a \in B'$, $c \in \mathbb{Z}$ und $r \in \langle B \backslash \{a\} \rangle$ (ohne a-Anteil), so ist

$$\tau(\tilde{a}bm) = \tau(\tilde{a}(ca + r)) = \tau(c\tilde{a}a) + \tau(\tilde{a}r) = c,$$

($\tau(\tilde{a}r) = 0$, da r keinen Anteil an a hat). Daraus folgt mit Bemerkung 1.2.4 $\tilde{a}b = c\tilde{m} + r'$ für ein geeignetes r' ohne $\tilde{m}$-Anteil. Da aber $\tilde{a}, b$ in B' und $\tilde{m}$ in B'' liegen (Proposition 3.1.4), muß $c = 0$ gelten. Dieses gilt für alle $a \in B'$ und somit ist bm im Erzeugnis von B''. □

Für beliebige endlich erzeugte $\mathbb{Z}$-Algebren gilt Proposition 3.1.5 nicht. Ein Gegenbeispiel ist: $B = \{1, a, b\}$ und $b^2 = 1$, $ab = ba = a$, $a^2 = a$. Das Erzeugnis $R' = \langle 1, a \rangle$ ist ein Teilring zur Teilmenge $\{1, a\}$. Der von b erzeugte $\mathbb{Z}$-Modul ist kein R'-Modul. In diesem Beispiel ist ein Basiselement ungleich 1 idempotent, was nach Proposition 2.2.2 in $\mathbb{Z}$-Ringen mit Basis nicht möglich ist.

3.1.2 Teilringe zu Teilmengen bei Charakterringen

Die Teilringe zu Teilmengen von Charakterringen von endlichen Gruppen sind leicht zu beschreiben. Wir benötigen dazu den Satz von Burnside-Brauer (siehe zum Beispiel [13], Theorem 4.3):

Satz 3.1.6 (Burnside, Brauer). *Es sei χ ein treuer Charakter der endlichen Gruppe G, χ nehme genau m verschiedene Werte auf G an. Dann ist jeder irreduzible Charakter von G Komponente eines der Charaktere $\chi^0, \ldots, \chi^{m-1}$.*

Korollar 3.1.7. *Es sei G eine endliche Gruppe. Der Charakterring von G hat als Teilringe zu Teilmengen der Basis genau die Charakterringe von Faktorgruppen von G.*

Beweis. Die irreduziblen Charaktere einer Faktorgruppe von G können wir kanonisch als Charaktere von G ansehen (konstant auf die Nebenklassen fortsetzen). Somit liefert jede Faktorgruppe einen Teilring zur Teilmenge.

Umgekehrt definiere die Teilmenge $B' := \{\chi_1, \ldots, \chi_n\}$ von B einen Teilring. Es sei N der Kern des Charakters $\theta := \sum_i \chi_i$. Dieser ist gleich dem Schnitt der Kerne der Elemente von B':

$$N = \ker\theta = \bigcap_i \ker\chi_i = \{g \in G \mid \chi_i(g) = \chi_i(1) \text{ für alle } 1 \leq i \leq n\}.$$

Da $N \subseteq \ker\chi_i$ für alle i gilt, kann jedes χ_i als irreduzibler Charakter der Faktorgruppe G/N angesehen werden. Damit ist der Teilring R' zu B' ein Unterring des Charakterrings A von G/N. Andererseits ist θ ein treuer Charakter von G/N. Nach Satz 3.1.6 finden wir jeden irreduziblen Charakter von G/N als Komponente einer Potenz von θ, d.h. $A = R'$. □

In Kapitel 7 werden wir die Teilringe zu Teilmengen der Basis im Darstellungsring des Quantendoppels einer endlichen Gruppe untersuchen.

3.1.3 Einfache ℤ-Ringe mit Basis

Für Tafelalgebren (Definition siehe 1.1.2) gibt es auch ausgezeichnete Unterstrukturen. Teilmengen C von B mit der Eigenschaft $\tilde{C}C \subseteq C$ heißen **abgeschlossene Teilmengen** (dies ist äquivalent zu $CC \subseteq C$ und $\tilde{C} = C$, siehe [3]). Die von abgeschlossenen Teilmengen erzeugten Algebren entsprechen nicht den Teilringen zu Teilmengen der Basis. Wegen $CC \subseteq C$ ist die von C erzeugte Algebra eine Halbgruppenalgebra. Eine Tafelalgebra heißt einfach, falls sie außer den trivialen keine abgeschlossenen Teilmengen hat.

Wir nennen einen ℤ-Ring mit Basis **einfach**, falls es außer den trivialen Unterringen keine Teilringe zu Teilmengen der Basis gibt. Einfach sind zum Beispiel die Gruppenringe und Charakterringe von einfachen Gruppen. Eine ganze Reihe von Fusionsalgebren zu affinen Algebren (siehe Kapitel 6) sind auch einfach.

3.1.4 Isomorphietests, Invarianten

Will man für zwei ℤ-Ringe mit Basis bestimmen, ob sie isomorph sind, so kann man verschiedene Invarianten berechnen:

Bemerkung 3.1.8. *Es seien R_1, R_2 ℤ-Ringe mit Basen B_1, B_2, die zueinander isomorph sind. Dann gilt:*

(i) $\{\{|N_{ij}^k| \mid b_j, b_k \in B_1\} \mid b_i \in B_1\} = \{\{|N_{ij}^k| \mid b_j, b_k \in B_2\} \mid b_i \in B_2\}$ *(als Multisets)*

(ii) $\{|B'| \mid \langle B' \rangle = R'$ *Teilring zu einer Teilmenge* B' *von* $B_1\} =$
$\{|B'| \mid \langle B' \rangle = R'$ *Teilring zu einer Teilmenge* B' *von* $B_2\}$ *(mit Vielfachheiten)*

(iii) Die Anzahl der Idempotente in den Ringen $R_1 \otimes \mathbb{Q}$, $R_2 \otimes \mathbb{Q}$ *ist gleich.*

Andererseits weiß man, daß zwei Ringe isomorph sind, wenn man aus den zugehörigen s-Matrizen direkt einen Isomorphismus erhält: Sind R_1, R_2 $\mathbb{Z}$-Ringe mit Basis und den s-Matrizen s_1, s_2, so sind diese als $\mathbb{Z}$-Algebren isomorph, falls $s_1 s_2^{-1}$ oder $s_2 s_1^{-1}$ eine Matrix mit ganzen Einträgen ist. Wenn eine dieser Matrizen eine monomiale Matrix mit Einträgen ± 1 ist, so sind die Ringe als $\mathbb{Z}$-Ringe mit Basis isomorph (siehe 1.2.6).

Umgekehrt haben isomorphe $\mathbb{Z}$-Ringe mit Basis nicht unbedingt diese Eigenschaft: Es sei R der $\mathbb{Z}$-Ring mit Basis $\{1, a, b\}$ und

$$a \cdot a = 1 - a - b, \quad a \cdot b = -a, \quad b \cdot b = 1.$$

Dieser Ring ist isomorph zum Charakterring R' der symmetrischen Gruppe S_3. Sind s_1, s_2 die s-Matrizen zu R, R', so haben weder $s_1 s_2^{-1}$ noch $s_2 s_1^{-1}$ nur ganze Einträge.

3.2 Graduierte $\mathbb{Z}$-Ringe mit Basis

Es sei $n \in \mathbb{N}$. Ab jetzt bezeichnen wir die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ mit n Elementen mit C_n und den Gruppenring $\mathbb{Z}[\mathbb{Z}/n\mathbb{Z}]$ mit Z_n.

In vielen Fällen kann man die Basis B eines $\mathbb{Z}$-Ringes mit Basis so partitionieren

$$B = M_1 \cup M_2 \cup \ldots \cup M_r, \quad M_i \cap M_j = \emptyset \text{ für } i \neq j,$$

daß es für alle $1 \leq i, j \leq r$ genau ein $1 \leq k \leq r$ gibt mit $M_i M_j \subseteq \langle M_k \rangle$. Es sei $J := \{1, \ldots, r\}$ und

$$\mu : J \times J \to J, \quad (i, j) \mapsto k.$$

Falls μ auf J eine assoziative Operation definiert, d.h.

$$\mu(\mu(i, j), k) = \mu(i, \mu(j, k)),$$

so ist (J, μ) ein Monoid, denn dasjenige i mit $1 \in M_i$ ist neutrales Element der Halbgruppe (J, μ).

Definition 3.2.1. Es sei J' ein Monoid. Ein $\mathbb{Z}$-Ring mit Basis R, für den es eine Partition der Basis gibt, so daß das zugehörige (J, μ) ein Monoid bildet, das isomorph zu J' ist, heißt ein **J'-graduierter $\mathbb{Z}$-Ring mit Basis**.

Wir schreiben dann: Der Ring R ist graduiert über dem Teilring R', der von den Basiselementen vom Grad 0_J erzeugt wird.

Beispiel 5. Ist A eine abelsche Gruppe, so ist $\mathbb{Z}[A]$ für jeden Normalteiler N von A ein A/N-graduierter $\mathbb{Z}$-Ring mit Basis. Die Elemente vom Grad 0 (neutrales Element in A/N) bilden einen Teilring, der isomorph zu $\mathbb{Z}[N]$ ist.

Es sei $M_1 \subseteq B$ die Teilmenge, die die Eins enthält. Diese definiert einen Teilring R', und die von M_i erzeugten $\mathbb{Z}$-Untermoduln $\langle M_i \rangle$ von R sind sogar R'-Moduln (mit der Multiplikation aus R als Operation). Die Umkehrung gilt nicht: Wenn wir einen Teilring R' wählen und die Basis so partitionieren, daß Elemente, die durch Multiplikation mit Elementen aus R' ineinander übergeführt werden können, zusammengelegt werden, so erhalten wir im Allgemeinen keine Graduierung (siehe zum Beispiel den Darstellungsring der symmetrischen Gruppe S_4 im nächsten Abschnitt).

Anmerkung 3.2.2. Meistens haben die Mengen M_i unterschiedlich viele Elemente. Wir haben dann nicht die Situation aus Beispiel 5, bei dem sozusagen R mit der „Basis“ $M_1, \ldots, M_r$ wieder ein Ring wird. Ein typisches Beispiel ist der $WZWV$-Ring (siehe 8.2.1).

Bei Tafelalgebren (Definition in 1.1.2) gibt es ein ähnliches Konzept. Die Graduierung ist dort eine Partition der Basis derart, daß das Produkt der Teilmengen assoziativ ist. Diese Definition stimmt nicht mit der obigen überein.

3.3 Multiplikationstafeln und Beispiele

Wir stellen die Multiplikation in einem $\mathbb{Z}$-Ring mit Basis als Tafel folgendermaßen dar: Jedes Basiselement b_i operiert auf R wie eine lineare Abbildung, die wir bezüglich B als Matrix $A(i)$ darstellen (reguläre Darstellung). Diese Matrizen bilden die Multiplikationstafel, denn

$$A(i)_{j,k} = N_{i,j}^k.$$

Betrachten wir zwei Beispiele für $\mathbb{Z}$-Ringe mit Basis. Es sei S_4 die symmetrische Gruppe auf 4 Punkten und R der Darstellungsring von S_4 mit der Basis B bestehend aus den Isomorphieklassen von irreduziblen Darstellungen.

Sind χ_0 der 1-Charakter, ε der Signum-Charakter, θ der irreduzible Charakter vom Grad 2 und $\psi, \varepsilon\psi$ die irreduziblen Charaktere vom Grad 3, so sieht die Tafel zu R bezüglich der Basis $\chi_0, \varepsilon, \theta, \psi, \varepsilon\psi$ (in dieser Reihenfolge) so aus („.“ bedeutet „0“):

$$\begin{bmatrix} 1 & . & . & . & . \\ . & 1 & . & . & . \\ . & . & 1 & . & . \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{bmatrix}, \begin{bmatrix} . & 1 & . & . & . \\ 1 & . & . & . & . \\ . & . & 1 & . & . \\ . & . & . & . & 1 \\ . & . & . & 1 & . \end{bmatrix}, \begin{bmatrix} . & . & 1 & . & . \\ . & . & 1 & . & . \\ 1 & 1 & 1 & . & . \\ . & . & . & 1 & 1 \\ . & . & . & 1 & 1 \end{bmatrix}, \begin{bmatrix} . & . & . & 1 & . \\ . & . & . & . & 1 \\ . & . & . & 1 & 1 \\ 1 & . & 1 & 1 & 1 \\ . & 1 & 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} . & . & . & . & 1 \\ . & . & . & 1 & . \\ . & . & . & 1 & 1 \\ . & 1 & 1 & 1 & 1 \\ 1 & . & 1 & 1 & 1 \end{bmatrix}.$$

Jeweils die erste Spalte jeder Matrix definiert die Involution $\sim$, die hier offenbar die Identität ist. Außerdem erkennen wir zwei Teilringe zu Teilmengen der Basis: Die ersten beiden

Elemente definieren einen Teilring Z_2; die ersten drei erzeugen den Darstellungsring der Gruppe S_3. Der gesamte Ring ist über keinem der beiden graduiert. Dennoch ist der von $\{\psi, \varepsilon\psi\}$ erzeugte $\mathbb{Z}$-Modul ein Modul über dem Teilring zu $\{\chi_0, \varepsilon, \theta\}$.

Die Multiplikationstafel des Darstellungsrings des Quantendoppels von S_3 (siehe Kapitel 7) sieht folgendermaßen aus:

$$\begin{bmatrix} 1&.&.&.&.&.&.&. \\ .&1&.&.&.&.&.&. \\ .&.&1&.&.&.&.&. \\ .&.&.&1&.&.&.&. \\ .&.&.&.&1&.&.&. \\ .&.&.&.&.&1&.&. \\ .&.&.&.&.&.&1&. \\ .&.&.&.&.&.&.&1 \end{bmatrix}, \begin{bmatrix} .&1&.&.&.&.&.&. \\ 1&.&.&.&.&.&.&. \\ .&.&1&.&.&.&.&. \\ .&.&.&1&.&.&.&. \\ .&.&.&.&1&.&.&. \\ .&.&.&.&.&1&.&. \\ .&.&.&.&.&.&.&1 \\ .&.&.&.&.&.&1&. \end{bmatrix}, \begin{bmatrix} .&.&1&.&.&.&.&. \\ .&.&1&.&.&.&.&. \\ 1&1&1&.&.&.&.&. \\ .&.&.&.&1&1&.&. \\ .&.&.&1&.&1&.&. \\ .&.&.&1&1&.&.&. \\ .&.&.&.&.&.&1&1 \\ .&.&.&.&.&.&1&1 \end{bmatrix}, \begin{bmatrix} .&.&.&1&.&.&.&. \\ .&.&.&1&.&.&.&. \\ .&.&.&.&1&1&.&. \\ 1&1&.&1&.&.&.&. \\ .&.&1&.&.&1&.&. \\ .&.&1&.&1&.&.&. \\ .&.&.&.&.&.&1&1 \\ .&.&.&.&.&.&1&1 \end{bmatrix},$$

$$\begin{bmatrix} .&.&.&.&1&.&.&. \\ .&.&.&.&1&.&.&. \\ .&.&.&1&.&1&.&. \\ .&.&1&.&.&1&.&. \\ 1&1&.&.&1&.&.&. \\ .&.&1&1&.&.&.&. \\ .&.&.&.&.&.&1&1 \\ .&.&.&.&.&.&1&1 \end{bmatrix}, \begin{bmatrix} .&.&.&.&.&1&.&. \\ .&.&.&.&.&1&.&. \\ .&.&.&1&1&.&.&. \\ .&.&1&.&1&.&.&. \\ .&.&1&1&.&.&.&. \\ 1&1&.&.&.&1&.&. \\ .&.&.&.&.&.&1&1 \\ .&.&.&.&.&.&1&1 \end{bmatrix}, \begin{bmatrix} .&.&.&.&.&.&1&. \\ .&.&.&.&.&.&.&1 \\ .&.&.&.&.&.&1&1 \\ .&.&.&.&.&.&1&1 \\ .&.&.&.&.&.&1&1 \\ .&.&.&.&.&.&1&1 \\ 1&.&1&1&1&1&.&. \\ .&1&1&1&1&1&.&. \end{bmatrix}, \begin{bmatrix} .&.&.&.&.&.&.&1 \\ .&.&.&.&.&.&1&. \\ .&.&.&.&.&.&1&1 \\ .&.&.&.&.&.&1&1 \\ .&.&.&.&.&.&1&1 \\ .&.&.&.&.&.&1&1 \\ .&1&1&1&1&1&.&. \\ 1&.&1&1&1&1&.&. \end{bmatrix}.$$

(Die Indizierung der Basiselemente ist nicht die kanonische aus Kapitel 7, weil die Graduierung dann schlechter zu sehen ist.) Auch hier ist $\sim$ trivial. Die Teilmengen

$$\{b_1, b_2, b_3\}, \{b_1, b_2, b_5\}, \{b_1, b_2, b_6\}, \{b_1, b_2, b_4\}$$

erzeugen jeweils einen Ring, der isomorph zum Darstellungsring von S_3 ist. Der gesamte Ring ist C_2-graduiert über dem Teilring zur Teilmenge $\{b_1, b_2, b_3, b_4, b_5, b_6\}$. Dieser ist isomorph als $\mathbb{Z}$-Ring mit Basis zum Darstellungsring der 4. Gruppe der Ordnung 18 (in der Numerierung von GAP oder Magma), welche ein semidirektes Produkt $C_3 \rtimes S_3$ ist.

Kapitel 4

Erweiterungen von $\mathbb{Z}$-Ringen mit Basis

Wenn Teilmengen der Basis von R unter Umständen Teilringe von R definieren, so ist es naheliegend die andere Richtung zu untersuchen: Welche Bedingungen müssen Elemente erfüllen, die man zur Basis hinzufügt, damit dabei ein $\mathbb{Z}$-Ring mit Basis und Teilring R entsteht?

Ist (R, B) ein $\mathbb{Z}$-Ring mit Basis und R' ein Teilring zur Teilmenge B', so haben wir schon in Proposition 3.1.5 gesehen, daß das Komplement $M := \langle B \backslash B' \rangle$ ein R'-Modul ist, also eine Darstellung von R'. Die irreduziblen Darstellungen von R' sind aber genau die Zeilen der zugehörigen s-Matrix (sie sind eindimensional, da R kommutativ ist). Wir wissen also, wie sich Elemente aus B' und $B \backslash B'$ multiplizieren: Sind $B = \{b_0, \ldots, b_{n-1}, m_1, \ldots, m_r\}$ und $B' = \{b_0, \ldots, b_{n-1}\}$, so sind folgende Strukturkonstanten durch die Darstellung M gegeben:

$$N_{b_i m_j}^{m_k} = N_{m_j b_i}^{m_k} = N_{m_j \tilde{m}_k}^{\tilde{b}_i}, \quad 1 \leq j, k \leq r, \quad 0 \leq i < n.$$

Nur die Strukturkonstanten $N_{m_i m_j}^{m_k}$ sind durch die Vorgabe von M nicht festgelegt. Falls M eindimensional ist, etwa $M = \langle m \rangle$, so ist N_{mm}^{m} frei wählbar. Ist es zweidimensional, so werden die einschränkenden Gleichungen, die durch die Assoziativität gegeben sind, etwas komplizierter.

4.1 Erweiterung durch ein Element

Es sei R' ein $\mathbb{Z}$-Ring mit Basis B'. Wir wollen ein Element m zur Basis hinzufügen. Da R' ein Teilring des neuen Rings sein sollte, müssen wir nur die Produkte $b \cdot m$, $b \in B'$ und $m \cdot m$ definieren.

Proposition 4.1.1. *Es sei R' ein $\mathbb{Z}$-Ring mit Basis $B' = \{b_0, \ldots, b_{n-1}\}$ und R ein freier $\mathbb{Z}$-Modul über $B' \cup \{m\}$, $m \notin R'$. Dann gelten:*

(a) Ist R ein $\mathbb{Z}$-Ring mit Basis und Teilring R' zur Teilmenge B', so gibt es eine Zeile $(a_0, \ldots, a_{n-1})$ der s-Matrix von R' mit $a_i \in \mathbb{Z}$ und $b_i \cdot m = a_i m$ für $0 \leq i < n$.

(b) Ist $(a_0, \ldots, a_{n-1})$ eine Zeile der s-Matrix von R', so wird R mit

$$b_i \cdot m = a_i m, \quad m \cdot m = \sum_i a_i b_i$$

und der Multiplikation von R' auf B' ein $\mathbb{Z}$-Ring mit Basis, der $\mathbb{Z}/2\mathbb{Z}$-graduiert über R' ist.

Beweis. Es sei R ein $\mathbb{Z}$-Ring mit Basis und Teilring R' zur Teilmenge B'. Nach Proposition 3.1.5 ist der von m erzeugte $\mathbb{Z}$-Untermodul von R ein R'-Modul, also eine eindimensionale Darstellung des Ringes R' über $\mathbb{Z}$ und somit eine Zeile $(a_0, \ldots, a_{n-1})$ der s-Matrix mit $a_i \in \mathbb{Z}$. Es gilt $b_i \cdot m = a_i m$.

Es sei jetzt $m \cdot m := \sum_i a_i b_i$. Wir zeigen, daß diese Multiplikation assoziativ ist. Da R kommutativ sein soll, reicht es $(mm)b_j = m(mb_j)$ für alle j zu zeigen. Diese Gleichung ist äquivalent zu

$$\sum_i \sum_k N_{ij}^k a_i b_k = \sum_k a_j a_k b_k.$$

Da $(a_0, \ldots, a_{n-1})$ eine Zeile der s-Matrix ist gilt nach Bemerkung 2.2.1 $\bar{a}_i = a_{\tilde{i}}$. Daher ist die linke Seite wegen

$$\sum_i N_{ij}^k a_i = \sum_i N_{\tilde{k}j}^{\tilde{i}} a_{\tilde{i}} = \sum_i N_{\tilde{k}j}^i a_i = a_{\tilde{k}} a_j$$

gleich $\sum_k a_{\tilde{k}} a_j b_k = \sum_k \bar{a}_k a_j b_k$, was wiederum wegen $\bar{a}_k = a_k$ $(a_k \in \mathbb{Z})$ gleich der rechten Seite ist.
Wir müssen noch zeigen, daß der neue Ring eine entsprechende Involution $\sim$ besitzt: Wir definieren $\tilde{m} := m$. Dann ist $\tau(b_i m) = 0$ und $\tau(\tilde{m} m) = a_0 = 1$. Es bleibt nachzuprüfen, ob $\widetilde{b_i m} = \tilde{m} \tilde{b}_i$ für alle i gilt. Dies folgt aber sofort aus $a_i = \bar{a}_{\tilde{i}} = a_{\tilde{i}}$.
Die $\mathbb{Z}/2\mathbb{Z}$-Graduierung ist trivialerweise vorhanden. □

Beispiel 6. Es seien R' der Charakterring der endlichen Gruppe G und $\{\chi_1, \ldots, \chi_n\}$ die irreduziblen Charaktere von G. Wählen wir $(a_1, \ldots, a_n) = (\chi_1(1), \ldots, \chi_n(1))$ die Charaktergrade als neue Strukturkonstanten, d.h. $\chi_i \cdot m = \chi_i(1)m$ und $m \cdot m = \sum_i \chi_i(1)\chi_i$, so erhalten wir wieder einen $\mathbb{Z}$-Ring mit Basis, eine „Wurzel der regulären Darstellung“ (sogar einen Ring mit Basis).

Beispiel 7. In [27] wird zu jeder endlichen abelschen Gruppe A eine Tensorkategorie definiert: Die einfachen Objekte sind $A \cup \{m\}$ und das Tensorprodukt ist

$$a \otimes b \cong ab, \quad a \otimes m \cong m \cong m \otimes a, \quad m \otimes m \cong \bigoplus_{a \in A} a,$$

für $a, b \in A$. Bei einer abelschen Gruppe sind alle Charaktergrade 1; der Grothendieck-Ring dieser Tensorkategorie ist demnach der Spezialfall des Rings aus Beispiel 6 für $G = A$.

Wir können den Koeffizienten vor m im Produkt $m \cdot m$ ungleich Null wählen. Das liefert auch einen $\mathbb{Z}$-Ring mit Basis, aber die Graduierung geht dabei verloren.

4.2 Erweiterung durch mehrere Elemente

Schauen wir uns zunächst den allgemeinen Fall an. Es seien alle Bezeichnungen wie am Anfang des Kapitels, d.h. $B = \{b_0, \ldots, b_{n-1}, m_1, \ldots, m_r\}$ usw. und $B'' := \{m_1, \ldots, m_r\}$. Insbesondere sei $M := \langle m_1, \ldots, m_r \rangle$ ein R'-Modul. Wir berechnen die Gleichungen, die die Strukturkonstanten $N_{m_i m_j}^{m_k}$ erfüllen müssen:

Proposition 4.2.1. *Es seien $C_i := (N_{m_i m_j}^{m_k})_{1 \le j,k \le r}$, $A_i := (N_{b_i m_j}^{m_k})_{1 \le j,k \le r}$. Angenommen es gelte $\tilde{m} = m$ für alle $m \in M$. Dann ist R assoziativ genau dann, wenn R' assoziativ ist und*

$$(*) \quad C_q C_p - C_p C_q = \Big(\sum_k N_{m_p m_j}^{b_k} N_{m_q \tilde{m}_l}^{\tilde{b}_k} - N_{m_q m_j}^{b_k} N_{m_p \tilde{m}_l}^{\tilde{b}_k} \Big)_{1 \le j,l \le r},$$
$$(**) \quad C_q A_p - A_q C_p = 0$$

für alle $1 \le p, q \le r$ gelten.

Beweis. Da R kommutativ ist, ist es assoziativ genau dann, wenn

$$(b_i m_p) m_q = b_i (m_p m_q) \quad \text{und} \quad (m_p m_q) m_l = m_p (m_q m_l)$$

für alle $0 \le i < n$, $1 \le p, q, l \le r$ gilt. (Die Gleichung $(b_i b_j) m_p = b_i (b_j m_p)$ gilt, da M ein R'-Modul ist, $(b_i b_j) b_k = b_i (b_j b_k)$ gilt, weil R' ein assoziativer Ring ist.) Die linke Gleichung ist äquivalent dazu, daß $(**)$ gilt, und daß M ein R'-Modul ist. Die rechte Gleichung führt zu $(*)$ und $(**)$. □

4.3 Erweiterung durch zwei Elemente

Ist speziell $r = 2$ so wird $(*)$ zu einer einzigen Gleichung:

Proposition 4.3.1. *Es gelten die Voraussetzungen aus Proposition 4.2.1. Ist $r = 2$, so wird die Gleichung $(*)$ zu*

$$\Big(C_1C_2 - C_2C_1\Big)_{1,2} = \delta_{\chi_1,\chi_2}|\chi_1|,$$

wenn sich die Darstellung M von R' über $\mathbb{C}$ in die eindimensionalen Darstellungen (Zeilen der s-Matrix) χ_1 und χ_2 zerlegt, d.h. $M \otimes_{\mathbb{Z}} \mathbb{C} \cong \chi_1 \oplus \chi_2$ (es bezeichne χ_i sowohl den Modul als auch den Homomorphismus).

Beweis. Gleichung $(*)$ ist nur dann interessant, wenn $p \neq q$ und $j \neq l$. In diesem Fall wird die rechte Seite zu $\sum_k \det(A_k)$. Da aber $M \otimes_{\mathbb{Z}} \mathbb{C} \cong \chi_1 \oplus \chi_2$ ist, gibt es eine Basis, in der alle A_k diagonal sind. Dann ist $\det(A_k) = \chi_1(b_k)\chi_2(b_k)$ und die Orthogonalitätsrelation (Bemerkung 1.2.3) liefert die gewünschte Gleichung. □

Korollar 4.3.2. *Ist M die direkte Summe von zwei unterschiedlichen eindimensionalen Darstellungen, so liefert $N_{m_im_j}^{m_k} := 0$ eine Erweiterung von R'. Diese ist $\mathbb{Z}/2\mathbb{Z}$-graduiert.*

Ist allerdings M direkte Summe von einer Darstellung mit sich selbst, so wird R mit $N_{m_im_j}^{m_k} := 0$ nicht assoziativ, insbesondere gibt es keine $\mathbb{Z}/2\mathbb{Z}$-graduierte Erweiterung von R' durch M.

4.4 Auswirkung auf die s-Matrizen

Es sei $R' < R$ eine Ringerweiterung durch ein Element, wie sie oben definiert wurde. Ist s' die s-Matrix von R', so entsteht die s-Matrix s von R, indem wir eine Zeile von s' verdoppeln und eine Spalte hinzufügen, die nur in den verdoppelten Zeilen ungleich Null ist und dort die Norm dieser Zeile als Einträge hat.

Etwas allgemeiner gilt: Es sei (R, B) ein $\mathbb{Z}$-Ring mit Basis und $R' \leq R$ ein Teilring zur Teilmenge $B' \subseteq B$. Die s-Matrix s von R hat als Zeilen die irreduziblen Darstellungen von R. Da R' auch ein $\mathbb{Z}$-Ring mit Basis ist (siehe Proposition 3.1.4), hat er auch eine s-Matrix s' (Bemerkung 2.2.1).

Ist $\rho : R \to \mathbb{C}$ eine irreduzible Darstellung von R, so ist $\rho_{|_{R'}}$ natürlich auch eine Darstellung von R'. Ist $\tilde{s}$ die $|B| \times |B'|$ Matrix, die aus s entsteht, indem nur die zu Elementen aus B' gehörigen Spalten beibehalten werden, so sind ihre Zeilen irreduzible Darstellungen von R'. Es gibt aber nur $|B'|$ nicht isomorphe irreduzible Darstellungen von R' (Satz von

Wedderburn-Artin). Daraus folgt, daß es in $\tilde{s}$ höchstens $|B'|$ verschiedene Zeilen gibt, die sich bei einer Erweiterung auf ein R vervielfachen.

Kapitel 5

Äußere Produkte

In [20] führt G. Malle für bestimmte imprimitive komplexe Spiegelungsgruppen (die Gruppen $G(e,1,n)$, Definition in 8.1) sogenannte unipotente Grade ein, die im Fall der Weylgruppe einer endlichen Gruppe vom Lie-Typ mit den Graden unipotenter Charaktere übereinstimmen. Die Übergangsmatrix von den sogenannten Scheingraden (fake degrees) zu den unipotenten Graden definiert eine Fourier-Transformation, die wir als S-Matrix einer $\mathbb{Z}$-Algebra ansehen können. Daß die Strukturkonstanten dieses Ringes ganze Zahlen sind, wird in [20] nicht gezeigt. Um das zu beweisen, müssen wir äußere Produkte untersuchen.

Wir haben in 2.5 bereits gesehen, daß symmetrische Potenzen einer S-Matrix $\mathbb{Z}$-Ringe mit Basis liefern. Hat diese Matrix e Spalten und Zeilen, so ist auch der Vektorraum $\bigwedge^n \mathbb{C}^e$ invariant unter $\bigotimes^n S$. Der Automorphismus $\bigotimes^n S|_{\bigwedge^n \mathbb{C}^e}$ hat bzgl. der kanonischen Basis die Eigenschaften einer S-Matrix und definiert für bestimmte S einen $\mathbb{Z}$-Ring mit Basis.

Wir werden zuerst zeigen, daß dieses bei der S-Matrix des Gruppenrings einer zyklischen Gruppe für beliebige e und n funktioniert. Daraus werden wir folgern, daß auch die oben erwähnte Fourier-Transformation $\mathbb{Z}$-Ringe mit Basis definiert.

Interessanterweise können wir diese Konstruktion auch auf die S-Matrix des WZWV-Fusionsdatums anwenden. Im nächsten Kapitel werden wir sehen, daß dieses eine Fourier-Matrix einer Kac-Moody-Algebra vom Typ $C_l^{(1)}$ ist. Daraus ergibt sich, daß die Strukturkonstanten des zugehörigen Ringes nicht negative ganze Zahlen sind, wofür wir keinen direkten Beweis finden konnten.

Die Charakterringe von Diedergruppen der Ordnung $2n$, n ungerade liefern im äußeren Produkt vermutlich $\mathbb{Z}$-Ringe mit Basis. Wie diese mit affinen Algebren zusammenhängen, muß noch untersucht werden. Andere S-Matrizen, wie etwa die des Darstellungsringes des Quantendoppels einer endlichen Gruppe, definieren im äußeren Produkt keinen Ring, da es meistens keine Zeile (oder Spalte) ohne 0 gibt, und somit keine geeignete Eins gewählt werden kann.

5.1 Äußeres Produkt von zyklischen Gruppenringen

5.1.1 Notation

Es sei $e \in \mathbb{N}$ und $\zeta = \exp(\frac{2\pi i}{e}) \in \mathbb{C}$. Dann ist $s = (\zeta^{ij})_{0 \le i,j \le e-1} \in \mathbb{C}^{e \times e}$ die s-Matrix und $S = (\frac{\zeta^{ij}}{\sqrt{e}})_{0 \le i,j \le e-1} \in \mathbb{C}^{e \times e}$ die S-Matrix von $Z_e (= \mathbb{Z}[\mathbb{Z}/e\mathbb{Z}])$. Wir betrachten den Vektorraum $\bigwedge^n \mathbb{C}^e$, $n \le e$. Dieser hat als Unterraum von $\bigotimes_{i=1}^n \mathbb{C}^e$ die Basis

$$C := \Big\{ \sum_{\sigma \in S_n} \varepsilon_\sigma e_{i_{\sigma(1)}} \otimes \ldots \otimes e_{i_{\sigma(n)}} \mid 0 \le i_1 < \ldots < i_n \le e-1 \Big\},$$

wobei ε_σ das Vorzeichen der Permutation σ und $e_0, \ldots, e_{e-1}$ die kanonische Basis von $\mathbb{C}^e$ ist (e mit Index ist ein Basiselement, ohne Index ist es das $e \in \mathbb{N}$ von oben). Diese Basis wird durch die n-Tupel $(i_1, \ldots, i_n)$ mit $0 \le i_1 < \ldots < i_n \le e-1$ indiziert; es bezeichne also $(i_1, \ldots, i_n)$ das entsprechende Basiselement.

Die Einschränkung von $\bigotimes_{i=1}^n S$ auf $\bigwedge^n \mathbb{C}^e$ definiert einen Automorphismus $\bigwedge^n S$. Wegen

$$\begin{aligned}
&(\bigotimes_{i=1}^n S) \sum_{\sigma \in S_n} \varepsilon_\sigma e_{i_{\sigma(1)}} \otimes \ldots \otimes e_{i_{\sigma(n)}} \\
&= \sum_{\sigma \in S_n} \varepsilon_\sigma (\sum_{j_1=1}^e S_{j_1, i_{\sigma(1)}} e_{j_1}) \otimes \ldots \otimes (\sum_{j_n=1}^e S_{j_n, i_{\sigma(n)}} e_{j_n}) \\
&= \sum_{j_1, \ldots, j_n} \left(\sum_{\sigma \in S_n} \varepsilon_\sigma \prod_{\nu=1}^n S_{j_\nu, i_{\sigma(\nu)}} \right) e_{j_1} \otimes \ldots \otimes e_{j_n} \\
&= \sum_{0 \le j_1 < \ldots < j_n \le e-1} \sum_{\tau \in S_n} \varepsilon_\tau \left(\sum_{\sigma \in S_n} \varepsilon_\sigma \prod_{\nu=1}^n S_{j_{\tau(\nu)}, i_{\sigma(\nu)}} \right) e_{j_{\tau(1)}} \otimes \ldots \otimes e_{j_{\tau(n)}} \\
&= \sum_{0 \le j_1 < \ldots < j_n \le e-1} \left(\sum_{\sigma \in S_n} \varepsilon_\sigma \prod_{\nu=1}^n S_{j_\nu, i_{\sigma(\nu)}} \right) \sum_{\tau \in S_n} \varepsilon_\tau e_{j_{\tau(1)}} \otimes \ldots \otimes e_{j_{\tau(n)}}
\end{aligned}$$

hat $\bigwedge^n S$ bezüglich der Basis C die Darstellungsmatrix

$$(\bigwedge^n S)_{\bar{i}, \bar{j}} = \sum_{\sigma \in S_n} \varepsilon_\sigma \prod_{\nu=1}^n S_{i_\nu, j_{\sigma(\nu)}} = \det((S_{i_\nu, j_{\nu'}})_{1 \le \nu, \nu' \le n}),$$

wobei $\bar{i} = (i_1, \ldots, i_n)$, $\bar{j} = (j_1, \ldots, j_n)$.

Wir wählen in C das Element $\bar{i}_0 := (0, \ldots, n-1)$ aus. Bis auf einen Normierungsfaktor ist $(\bigwedge^n S)_{\bar{i},\bar{i}_0}$ eine Vandermondesche Determinante $\prod_{1 \leq \lambda_1 < \lambda_2 \leq n} (\zeta^{i_{\lambda_2}} - \zeta^{i_{\lambda_1}})$ und deshalb ungleich 0. Wir definieren eine Matrix $\hat{s} \in \mathbb{C}^{|C| \times |C|}$ durch

$$\hat{s}_{\bar{i},\bar{j}} := \frac{(\bigwedge^n S)_{\bar{i},\bar{j}}}{(\bigwedge^n S)_{\bar{i},\bar{i}_0}},$$

die wir als Algebrenisomorphismus auffassen können (siehe 2.1.3). Das Bild der Algebra $\bigwedge^n \mathbb{C}^e$ mit komponentenweiser Multiplikation unter $\hat{s}$ ist dann ein Ring mit den Strukturkonstanten

$$N_{\bar{j},\bar{k}}^{\bar{l}} = \sum_{\bar{i} \in C} \frac{(\bigwedge^n S)_{\bar{i},\bar{j}} (\bigwedge^n S)_{\bar{i},\bar{k}} \overline{(\bigwedge^n S)_{\bar{i},\bar{l}}}}{(\bigwedge^n S)_{\bar{i},\bar{i}_0}}.$$

5.1.2 Ganzheit und Involution

Wir wollen zeigen, daß die Matrix $\bigwedge^n S$ mit $\bar{i}_0$ einen $\mathbb{Z}$-Ring mit Basis definiert. Dazu müssen wir zunächst nachprüfen, daß $N_{\bar{j},\bar{k}}^{\bar{l}}$ ganze Zahlen sind.

Anmerkung 5.1.1. Der Quotient $\frac{(\bigwedge^n S)_{\bar{i},\bar{j}}}{(\bigwedge^n S)_{\bar{i},\bar{i}_0}}$ in der obigen Summe ist gerade die Schur-Funktion $s_{\bar{j}'}(x_1, \ldots, x_n)$, $\bar{j}' := (j_n - (n-1), \ldots, j_2 - 1, j_1)$ ausgewertet an den Stellen $(\zeta^{i_1}, \ldots, \zeta^{i_n})$ (siehe [18], [24] oder im Anhang S.113). Die beiden nächsten Lemmata können auch durch entsprechende Aussagen über Schur-Funktionen ersetzt werden, die im Anhang S.113 ausgeführt werden.

Die beiden nächsten Lemmata liefern eine für den Beweis passende Darstellung des Quotienten $\frac{(\bigwedge^n S)_{\bar{i},\bar{j}}}{(\bigwedge^n S)_{\bar{i},\bar{i}_0}}$:

Lemma 5.1.2. *Es sei M die Menge der Matrizen $m = (m_{j,k})_{1 \leq j,k \leq n}$ in $\mathbb{N}_0^{n \times n}$ mit $m_{j,k} \leq m_{j+1,k+1}$ für $1 \leq j, k < n$ und $m_{j+1,k} < m_{j,k}$ für $1 \leq j < k \leq n$. Für $\bar{i} = (i_1, \ldots, i_n) \in \mathbb{N}^n$, $i_1 < \ldots < i_n$ sei*

$$M_{\bar{i}} = \{m \in M \mid m_{1,k} = i_k, 1 \leq k \leq n \quad m_{j,k} = 0, 1 \leq k < j \leq n\},$$

und für $j > 1$, $a \in \mathbb{N}$, $m \in M$ seien

$$w_j(m) := \Big(\sum_{k=j-1}^{n} m_{j-1,k} \Big) - \Big(\sum_{k=j}^{n} m_{j,k} \Big) - (n - j + 1),$$

$$z_j(a) := \{m \in M_{\bar{i}} \mid w_j(m) = a\}.$$

Dann gilt für alle $1 < i, j \leq n+1$, $a \in \mathbb{N}$:

$$|z_i(a)| = |z_j(a)|.$$

Beweis. Wir zeigen: $|z_j(a)| = |z_{j+1}(a)|$. Es sei also $m \in M_{\bar{i}}$ mit $w_j(m) = a$. Mit

$$v_k := \{m_{(j+1),k}, m_{(j-1),(k-1)} - 1\} \text{ für } j < k \leq n,$$

$$v_k := \{m_{(j-1),(k-1)} - 1\} \text{ für } k = j, k = n+1$$

gilt wegen der beiden Bedingungen an die Elemente von M

$$(\max v_k) + 1 \leq m_{j,k} \leq \min v_{k+1},$$

und zwar so, daß für $m_{j,k}$ (bei fest vorgegebenen $m_{l,k}$, $l \neq j$) genau die Werte von $(\max v_k)+1$ bis $\min v_{k+1}$ erlaubt sind. Wir definieren ein $\tilde{m} \in M_{\bar{i}}$ mit $m_{l,k} = \tilde{m}_{l,k}$, $l \neq j$ so, daß $a = w_j(m) = w_{j+1}(\tilde{m})$:

$$\tilde{m}_{j,k} := (\max v_k) + (\min v_{k+1}) + 1 - m_{j,k}.$$

Das ergibt

$$\sum_{k=j}^{n} \tilde{m}_{j,k} = \sum_{k=j}^{n} (\max v_k) + (\min v_{k+1}) + 1 - m_{j,k} =$$

$$= (\max v_j) + 1 - m_{j,j} + (\min v_{n+1}) + \sum_{k=j+1}^{n} (\max v_k) + (\min v_k) + 1 - m_{j,k} =$$

$$= m_{(j-1),(j-1)} - m_{j,j} + m_{(j-1),n} - 1 + \sum_{k=j+1}^{n} (\max v_k) + (\min v_k) + 1 - m_{j,k}.$$

Wegen $\max v_k + \min v_k = m_{(j+1),k} + m_{(j-1),(k-1)} - 1$ für $j < k < n+1$ ist

$$\sum_{k=j}^{n} \tilde{m}_{j,k} = \Big(\sum_{k=j}^{n} -m_{j,k}\Big) + \Big(\sum_{k=j-1}^{n} m_{(j-1),k}\Big) + \Big(\sum_{k=j+1}^{n} m_{(j+1),k}\Big) - 1,$$

und daraus folgt sofort die geforderte Eigenschaft. Die Abbildung $m \mapsto \tilde{m}$ ist eine Bijektion, die ein m mit $w_j(m) = a$ auf ein $\tilde{m}$ mit $w_{j+1}(\tilde{m}) = a$ abbildet. □

Lemma 5.1.3. *Es seien $\bar{i}, \bar{j} \in C$. Mit $P_{\bar{i},\bar{j}} := \det(\zeta^{i_\mu j_\nu})_{\mu,\nu}$ und $\bar{i}_0 := (0, \ldots, n-1)$ nimmt die Schur-Funktion $s_{\bar{j}}$ bei $(\zeta^{i_1}, \ldots, \zeta^{i_n})$ den Wert*

$$\frac{P_{\bar{i},\bar{j}}}{P_{\bar{i},\bar{i}_0}} = \sum_{m \in M_{\bar{j}}} \prod_{\nu=1}^{n} \zeta^{i_\nu w_{\nu+1}(m)}$$

an, wobei

$$w_j(m) = \Big(\sum_{k=j-1}^{n} m_{(j-1)k}\Big) - \Big(\sum_{k=j}^{n} m_{jk}\Big) - (n - j + 1).$$

Beweis. Der Nenner $P_{\bar{i},\bar{i}_0}$ ist eine Vandermondesche Determinante

$$V_{\bar{i}} = P_{\bar{i},\bar{i}_0} = \prod_{1\le\lambda_1<\lambda_2\le n} (\zeta^{i_{\lambda_2}} - \zeta^{i_{\lambda_1}}).$$

Für ein $\bar{m} = (m_1, \dots, m_n)$ mit $0 \le m_1 < \dots < m_n \le e-1$ gilt

$$P_{\bar{i},\bar{m}} = \zeta^{i_1 m_1} \det(\zeta^{i_\mu m_\nu} - \zeta^{i_\mu m_1 + (i_1 m_\nu - i_1 m_1)})_{2\le\mu,\nu\le n}$$

$$= \zeta^{-(n-2)i_1 m_1} \det(\zeta^{i_1 m_1 + i_\mu m_\nu} - \zeta^{i_1 m_\nu + i_\mu m_1})_{2\le\mu,\nu\le n}.$$

Wir haben für alle $v_1, v_2, i_1, i_2 \in \mathbb{Z}, i_1 < i_2$ die Gleichung (folgt direkt aus der geometrischen Reihe)

$$\frac{\zeta^{i_1 v_1 + i_1 v_2} - \zeta^{i_1 v_2 + i_2 v_1}}{\zeta^{i_2} - \zeta^{i_1}} = \zeta^{i_1(v_2-1)+i_2 v_1} \sum_{\mu=0}^{v_2-v_1-1} \zeta^{(i_2-i_1)\mu}.$$

Daraus folgt

$$\begin{aligned}
P_{\bar{i},\bar{m}} &= \zeta^{-(n-2)i_1 m_1} \prod_{k=2}^{n} (\zeta^{i_k} - \zeta^{i_1}) \det\left(\zeta^{i_1(m_\nu-1)+i_\mu m_1} \sum_{\eta=0}^{m_\nu-m_1-1} \zeta^{(i_\mu-i_1)\eta}\right)_{2\le\mu,\nu\le n} \\
&= \zeta^{-(n-2)i_1 m_1} \prod_{k=2}^{n} (\zeta^{i_k} - \zeta^{i_1}) \zeta^{i_1(m_k-1)+i_k m_1} \sum_{\eta_2=0}^{m_2-m_1-1} \cdots \sum_{\eta_n=0}^{m_n-m_1-1} \det(\zeta^{(i_\mu-i_1)\eta_\nu})_{2\le\mu,\nu\le n} \\
&= \sum_{\eta_2=m_1}^{m_2-1} \cdots \sum_{\eta_n=m_{(n-1)}}^{m_n-1} \zeta^{i_1 m_1} \prod_{k=2}^{n} (\zeta^{i_k} - \zeta^{i_1}) \zeta^{i_1(m_k-1)-i_1\eta_k} \det(\zeta^{i_\nu \eta_\mu})_{2\le\mu,\nu\le n} \\
&= \sum_{\eta_2=m_1}^{m_2-1} \cdots \sum_{\eta_n=m_{(n-1)}}^{m_n-1} \zeta^{i_1 m_1} \prod_{k=2}^{n} \zeta^{i_1(m_k-1)-i_1\eta_k} P_{(i_2,\dots,i_n),(\eta_2,\dots,\eta_n)} \frac{V_{\bar{i}}}{V_{(i_2,\dots,i_n)}}.
\end{aligned}$$

Mit $m_{1,\nu} := m_\nu$ und Induktion folgt daraus

$$\begin{aligned}
\frac{P_{\bar{i},\bar{m}}}{V_{\bar{i}}} = \sum_{m_{2,2}=m_{1,1}}^{m_{1,2}-1} \cdots \sum_{m_{2,n}=m_{1,(n-1)}}^{m_{1,n}-1} \Bigg(\sum_{m_{3,3}=m_{2,2}}^{m_{2,3}-1} \cdots \sum_{m_{3,n}=m_{2,(n-1)}}^{m_{2,n}-1} \Bigg(\cdots \Bigg(\sum_{m_{n,n}=m_{(n-1),(n-1)}}^{m_{(n-1),n}-1} \\
\zeta^{i_1(m_{1,1}+\sum_{k=2}^n(m_{1,k}-m_{2,k}-1))} \zeta^{i_2(m_{2,2}+\sum_{k=3}^n(m_{2,k}-m_{3,k}-1))} \cdots \\
\zeta^{i_{n-1}(m_{(n-1),(n-1)}+m_{(n-1),n}-m_{n,n}-1)} \zeta^{i_n(m_{n,n})} \Bigg)\Bigg)\Bigg).
\end{aligned}$$

Die Exponenten sind genau die in Lemma 5.1.2 definierten Zahlen. □

Satz 5.1.4. *Die oben definierten Strukturkonstanten $N_{\bar{j},\bar{k}}^{\bar{l}}$ sind ganze Zahlen.*

Beweis. Wegen $s_{ij} = \zeta^{ij}$ hat jede Zeile von s die Norm $\sqrt{e}$. Damit ist $S_{ij} = \frac{\zeta^{ij}}{\sqrt{e}}$ und

$$(\bigwedge^n S)_{\bar{i},\bar{j}} = \frac{1}{\sqrt{e}^n} \sum_{\sigma \in S_n} \varepsilon_\sigma \prod_{\nu=1}^n \zeta^{i_\nu j_{\sigma(\nu)}}.$$

Wir erhalten

$$N_{\bar{j},\bar{m}}^{\bar{k}} = \frac{1}{e^n} \sum_{0 \le i_1 < \ldots < i_n \le e-1} \frac{P_{\bar{i},\bar{j}} \overline{P_{\bar{i},\bar{k}}} P_{\bar{i},\bar{m}}}{P_{\bar{i},(0,\ldots,n-1)}},$$

wenn $P_{\bar{i},\bar{j}} := \det(\zeta^{i_\mu j_\nu})_{\mu,\nu}$. Lemma 5.1.3 liefert für $D_{\bar{i},\bar{m}} := \frac{P_{\bar{i},\bar{m}}}{V_{\bar{i}}}$ die Formel

$$D_{\bar{i},\bar{m}} = \sum_{m \in M_{\bar{m}}} \prod_{\nu=1}^n \zeta^{i_\nu w_{\nu+1}(m)}.$$

Diese ist nun auch für beliebige Tupel $(i_1, \ldots, i_n)$, $0 \le i_1, \ldots, i_n \le e-1$ definiert. Im allgemeinen ist $D_{\bar{i},\bar{m}}$ für ein $\bar{i}$ mit zwei gleichen Einträgen ungleich 0. Der Ausdruck $P_{\bar{i},\bar{j}} \overline{P_{\bar{i},\bar{k}}} D_{\bar{i},\bar{m}}$ ist aber in diesem Fall dennoch 0, da die Determinanten $P_{\bar{i},\bar{j}}, P_{\bar{i},\bar{k}}$ gleich 0 sind. Außerdem wissen wir, daß $D_{\bar{i},\bar{m}}$ unter Permutation der $i_1, \ldots, i_n$ invariant ist, falls $0 \le i_1 < \ldots < i_n \le e-1$ (das gilt vermutlich immer, wir benötigen dies aber nur für paarweise verschiedene $i_1, \ldots, i_n$). Die Determinanten $P_{\bar{i},\bar{j}}, P_{\bar{i},\bar{k}}$ verändern sich dabei nur um Vorzeichen, die sich gegenseitig aufheben. Wir dürfen also folgendermaßen umformen:

$$N_{\bar{j},\bar{m}}^{\bar{k}} = \frac{1}{e^n} \sum_{0 \le i_1 < \ldots < i_n \le e-1} P_{\bar{i},\bar{j}} \overline{P_{\bar{i},\bar{k}}} D_{\bar{i},\bar{m}} = \frac{1}{e^n n!} \sum_{0 \le i_1, \ldots, i_n \le e-1} P_{\bar{i},\bar{j}} \overline{P_{\bar{i},\bar{k}}} D_{\bar{i},\bar{m}}.$$

Wir wollen zeigen, daß $a := \sum_{0 \le i_1, \ldots, i_n \le e-1} P_{\bar{i},\bar{j}} \overline{P_{\bar{i},\bar{k}}} D_{\bar{i},\bar{m}}$ eine ganze Zahl und kongruent 0 modulo $e^n n!$ ist. Wir setzen für $P_{\bar{i},\bar{j}}$ den Ausdruck $\sum_{\sigma \in S_n} \varepsilon_\sigma \prod_{\nu=1}^n \zeta^{i_\nu j_{\sigma(\nu)}}$ ein:

$$a = \sum_{\sigma_1, \sigma_2 \in S_n} \varepsilon_{\sigma_1} \varepsilon_{\sigma_2} \sum_{m \in M_{\bar{m}}} \sum_{0 \le i_1, \ldots, i_n \le e-1} \prod_{\nu=1}^n \zeta^{i_\nu (j_{\sigma_1(\nu)} - k_{\sigma_2(\nu)} + w_{\nu+1}(m))},$$

wobei sich die innere Summe auch so schreibt:

$$\sum_{i_1=0}^{e-1} \zeta^{i_1 (j_{\sigma_1(1)} - k_{\sigma_2(1)} + w_{1+1}(m))} \sum_{i_2=0}^{e-1} \zeta^{i_2 (j_{\sigma_1(2)} - k_{\sigma_2(2)} + w_{2+1}(m))} \cdots \sum_{i_n=0}^{e-1} \zeta^{i_n (j_{\sigma_1(n)} - k_{\sigma_2(n)} + w_{n+1}(m))}.$$

Für ein Paar (σ_1, σ_2) ist dieses genau dann ungleich 0, falls alle Klammern $(j_{\sigma_1(\nu)} - k_{\sigma_2(\nu)} + w_{\nu+1}(m))$ kongruent 0 modulo e sind. Nach Lemma 5.1.2 nehmen die $w_{\nu+1}(m), m \in M_{\bar{m}}$ für alle ν die gleichen Werte mit gleicher Vielfachheit an. Damit ist mit (σ_1, σ_2) auch $(\sigma_1 \tau, \sigma_2 \tau)$, $\tau \in S_n$ ein geeignetes Paar ($\varepsilon_{\sigma_1 \tau} \varepsilon_{\sigma_2 \tau} = \varepsilon_{\sigma_1} \varepsilon_{\sigma_2}$). Jedes geeignete Paar liefert am Ende ein e^n. Damit ist R kongruent 0 modulo $e^n n!$, woraus $N_{\bar{j},\bar{m}}^{\bar{k}} \in \mathbb{Z}$ folgt. $\square$

Wir können übrigens nicht zeigen, daß die Strukturkonstanten natürliche Zahlen sind, weil dies im allgemeinen nicht gilt:

Beispiel 8. Mit $e = 4$, $n = 2$ haben wir 6 Basiselemente. Die Multiplikationstafel sieht folgendermaßen aus:

$$\begin{bmatrix} 1 & . & . & . & . & . \\ . & 1 & . & . & . & . \\ . & . & 1 & . & . & . \\ . & . & . & 1 & . & . \\ . & . & . & . & 1 & . \\ . & . & . & . & . & 1 \end{bmatrix}, \begin{bmatrix} . & 1 & . & . & . & . \\ . & . & 1 & 1 & . & . \\ . & . & . & . & 1 & . \\ . & . & . & . & 1 & . \\ -1 & . & . & . & . & 1 \\ . & -1 & . & . & . & . \end{bmatrix}, \begin{bmatrix} . & . & 1 & . & . & . \\ . & . & . & . & 1 & . \\ . & . & . & . & . & 1 \\ -1 & . & . & . & . & . \\ . & -1 & . & . & . & . \\ . & . & . & -1 & . & . \end{bmatrix},$$

$$\begin{bmatrix} . & . & . & 1 & . & . \\ . & . & . & . & 1 & . \\ -1 & . & . & . & . & . \\ . & . & . & . & . & 1 \\ . & -1 & . & . & . & . \\ . & . & -1 & . & . & . \end{bmatrix}, \begin{bmatrix} . & . & . & . & 1 & . \\ -1 & . & . & . & . & 1 \\ . & -1 & . & . & . & . \\ . & -1 & . & . & . & . \\ . & . & -1 & -1 & . & . \\ . & . & . & . & -1 & .] \end{bmatrix}, \begin{bmatrix} . & . & . & . & . & 1 \\ . & -1 & . & . & . & . \\ . & . & . & -1 & . & . \\ . & . & -1 & . & . & . \\ . & . & . & . & -1 & . \\ 1 & . & . & . & . & . \end{bmatrix}.$$

Dieses ist noch kein $\mathbb{Z}$-Ring mit Basis, da die Involution $\sim$ zum Beispiel das zweite Basiselement auf minus das vierte Basiselement abbildet. Substitutionen der Form $b \mapsto -b$ (die Isomorphismen von $\mathbb{Z}$-Algebren sind) beseitigen dieses Problem. Es ist aber nicht möglich, durch solche Substitutionen einen Ring mit Basis zu erhalten (wir können mit dem Computer leicht alle 2^6 Vorzeichenwechsel ausschließen).

Nach einem geeigneten Vorzeichenwechsel der Basiselemente haben wir einen $\mathbb{Z}$-Ring mit Basis:

Satz 5.1.5. *Die Matrix $\bigwedge^n S$ definiert eine $\mathbb{Z}$-Algebra, die nach einer geeigneten Substitution der Basiselemente der Form $b_{\bar{i}} \mapsto \pm b_{\bar{i}}$ ein $\mathbb{Z}$-Ring mit Basis ist.*

Beweis. Satz 5.1.4 zeigt, daß $\bigwedge^n S$ eine $\mathbb{Z}$-Algebra definiert. Wir definieren eine Abbildung $\sim$, die nach einer Substitution der Basiselemente diese Algebra zu einem $\mathbb{Z}$-Ring mit Basis macht. Ist $\bar{i} = (i_1, \ldots, i_n) \in C$ ein Basiselement, so ergibt

$$\bar{i}' := (n - 1 - i_1, \ldots, n - 1 - i_n)$$

aufsteigend sortiert ein Basiselement $\tilde{\bar{i}}$. Es sei $\sim\colon C \to C$, $\bar{i} \mapsto \tilde{\bar{i}}$ und $\gamma_{\bar{i}} \in \{\pm 1\}$ das Signum der Permutation, die zum Sortieren von $\bar{i}'$ benötigt wird. Wir zeigen für beliebige $\bar{j} \in C$:

$$N_{\bar{i},\bar{j}}^{\bar{i}_0} = \begin{cases} \delta_{\tilde{\bar{i}},\bar{j}} & \text{falls } \bar{i} = \tilde{\bar{i}} \\ \pm\delta_{\tilde{\bar{i}},\bar{j}} & \text{falls } \bar{i} \neq \tilde{\bar{i}}. \end{cases}$$

Daraufhin definieren wir eine Substitution u: Für $N_{\bar{i},\tilde{\bar{i}}}^{\bar{i}_0} = -1$ (dann ist auch $\bar{i} \neq \tilde{\bar{i}}$) sei $u(b_{\bar{i}}) := -b_{\bar{i}}$ und $u(b_{\tilde{\bar{i}}}) := b_{\tilde{\bar{i}}}$, d.h. wir wählen zwischen $b_{\bar{i}}$ und $b_{\tilde{\bar{i}}}$ eines aus, das wir mit einem Minus versehen (dann ist $\tau(u(b_{\bar{i}})u(b_{\tilde{\bar{i}}})) = -N_{\bar{i},\tilde{\bar{i}}}^{\bar{i}_0} = 1$). Für $N_{\bar{i},\tilde{\bar{i}}}^{\bar{i}_0} = 1$ sei $u(b_{\bar{i}}) := b_{\bar{i}}$.

Mit der Notation aus Satz 5.1.4 und $\bar{i}, \bar{i}', \tilde{\bar{i}}$ wie am Anfang des Beweises stellen wir zunächst fest, daß für alle $\bar{k} \in C$

$$(*) \quad \overline{P_{\bar{k},\bar{i}}} = P_{\bar{k},-\bar{i}} = P_{\bar{k},\bar{i}'} \prod_{\nu=1}^{n} \zeta^{-k_\nu(n-1)} = \gamma_{\bar{i}} P_{\bar{k},\tilde{\bar{i}}} \prod_{\nu=1}^{n} \zeta^{-k_\nu(n-1)}$$

gilt. Daraus folgt aber

$$N^{\bar{i}_0}_{\bar{i},\bar{j}} = \frac{1}{e^n} \sum_{0 \le k_1 < \ldots < k_n \le e-1} \frac{P_{\bar{k},\bar{i}} \overline{P_{\bar{k},\bar{i}_0}} P_{\bar{k},\bar{j}}}{P_{\bar{k},\bar{i}_0}} = \gamma_{\bar{i}} \gamma_{\bar{i}_0} \frac{1}{e^n} \sum_{0 \le k_1 < \ldots < k_n \le e-1} \frac{\overline{P_{\bar{k},\tilde{\bar{i}}}} P_{\bar{k},\bar{i}_0} P_{\bar{k},\bar{j}}}{P_{\bar{k},\bar{i}_0}} = \gamma_{\bar{i}} \gamma_{\bar{i}_0} \delta_{\tilde{\bar{i}},\bar{j}},$$

weil die Spalten von $\bigwedge^n S$ orthonormal sind. Wenn $\bar{i} = \tilde{\bar{i}}$ gilt, wird zum Sortieren von $\bar{i}'$ die gleiche Permutation wie zum Sortieren von $\tilde{\bar{i}}_0$ benötigt (weil dann $n-1-i_n = i_1$ gilt, und somit $(n-1-i_1, \ldots, n-1-i_n)$ absteigend sortiert ist). Die Vorzeichen der Permutationen sind also gleich, d.h. $\gamma_{\bar{i}} \gamma_{\bar{i}_0} = 1$.
Wir müssen noch die Multiplikativität von $\sim$ beweisen, d.h. $N^{\bar{m}}_{\tilde{\bar{i}},\tilde{\bar{j}}} = N^{\tilde{\bar{m}}}_{\bar{i},\bar{j}}$ für alle $\bar{i}, \bar{j}, \bar{m} \in C$ (nach der Substitution u). Dazu schauen wir uns an, was mit der obigen Gleichung geschieht, wenn wir sie komplex konjugieren:

$$N^{\bar{m}}_{\tilde{\bar{i}},\tilde{\bar{j}}} = \overline{N^{\bar{m}}_{\tilde{\bar{i}},\tilde{\bar{j}}}} = \frac{1}{e^n} \sum_{0 \le k_1 < \ldots < k_n \le e-1} \frac{\overline{P_{\bar{k},\tilde{\bar{i}}}} P_{\bar{k},\bar{m}} \overline{P_{\bar{k},\tilde{\bar{j}}}}}{\overline{P_{\bar{k},\bar{i}_0}}} \overset{(*)}{=} \gamma_{\bar{i}} \gamma_{\bar{j}} \gamma_{\bar{m}} \gamma_{\bar{i}_0} N^{\tilde{\bar{m}}}_{\bar{i},\bar{j}}.$$

Nach der Substitution u heben sich die Vorzeichen auf: Ein $b_{\bar{i}}$ wird höchstens dann durch $-b_{\bar{i}}$ substituiert, wenn $N^{\bar{i}_0}_{\bar{i},\tilde{\bar{i}}} = -1$, d.h. wenn $\gamma_{\bar{i}} \neq \gamma_{\bar{i}_0}$. Andererseits gilt für die restlichen $\bar{i}$ aus C $\gamma_{\bar{i}} = \gamma_{\bar{i}_0}$. Gilt nun in der obigen Formel etwa $\gamma_{\bar{i}} \neq \gamma_{\bar{i}_0}$, so wird entweder $b_{\bar{i}}$ oder $b_{\tilde{\bar{i}}}$ durch $-b_{\bar{i}}$ bzw. $-b_{\tilde{\bar{i}}}$ substituiert; dabei erhält $N^{\tilde{\bar{m}}}_{\bar{i},\bar{j}}$ bzw. $N^{\bar{m}}_{\tilde{\bar{i}},\tilde{\bar{j}}}$ ein zusätzliches Vorzeichen, das zusammen mit $\gamma_{\bar{i}}$ den Wert $\gamma_{\bar{i}_0}$ liefert. Nach der Substitution bleibt demnach als Vorzeichen $\gamma^4_{\bar{i}_0} = 1$ übrig. □

Satz 5.1.5 und Bemerkung 2.2.1 ergeben, daß die Spalten der s-Matrix $\hat{s}$ bezüglich der komplexen Konjugation abgeschlossen sind. Da die zu $\bar{i}_0$ gehörige Spalte der Matrix $\bigwedge^n S$ nicht nur reelle Einträge hat, ist die Menge ihrer Spalten jedoch nicht abgeschlossen bezüglich komplexer Konjugation. Die S-Matrix des Ringes, wie sie in Kapitel 2 definiert wird, ist deshalb nicht $\bigwedge^n S$. Erst wenn wir $\bigwedge^n S$ in jeder Zeile mit einer Einheitswurzel multiplizieren (so daß die Spalte $\bar{i}_0$ schließlich nur noch reelle Einträge hat) erhalten wir die S-Matrix.

5.1.3 Negative Strukturkonstanten

Beispiel 8 zeigt, daß die Strukturkonstanten auch negativ sein können. Berechnungen am Computer belegen, daß es wahrscheinlich immer einen Ring R' doppelter Dimension gibt, so daß unser Ring R ein Faktorring R'/I für ein geeignetes Ideal $I \trianglelefteq R'$ ist:

Vermutung 5.1.6. *Es sei $C = \{b_1, \ldots, b_q\}$ die obige Basis zu dem obigen Ring R und $\tilde{R}$ der freie $\mathbb{Z}$-Modul erzeugt von $\{b_1, \ldots, b_q, b'_1, \ldots, b'_q\}$. Es sei π der Modul-Epimorphismus $\tilde{R} \to R$, $b_i \mapsto b_i$, $b'_i \mapsto -b_i$ mit Kern $I := \langle b_i + b'_i \mid i = 1, \ldots, q \rangle$. Weiterhin sei $\varphi : R \to \tilde{R}$ durch*

$$\sum_i \lambda_i b_i \mapsto \sum_i \delta_{\lambda_i \ge 0} \lambda_i b_i - \delta_{\lambda_i < 0} \lambda_i b'_i$$

definiert. Dann ist die auf $\tilde{R}$ definierte Multiplikation $c_1 c_2 := \varphi(\pi(c_1)\pi(c_2))$ assoziativ und die Strukturkonstanten von $\tilde{R}$ liegen in $\mathbb{N}$. Das heißt, R ist Faktorring eines Ringes mit positiven Strukturkonstanten doppelter Dimension.

Die Vermutung wurde am Computer für alle Ringe mit höchstens 50 Basiselementen überprüft. Dazu genügt es, alle $3 < e \leq 10$, $1 < n < e-1$ zu durchlaufen. Die restlichen ($n = 1$ oder $n = e-1$) sind Gruppenringe von zyklischen Gruppen.

Bei beliebigen $\mathbb{Z}$-Ringen mit Basis funktioniert diese Methode der Basisverdoppelung nicht (zum Beispiel beim Ring aus Abschnitt 8.5).

5.1.4 Wahl der Eins

Es sei jetzt $\bar{m} = (m_1, \ldots, m_n)$ aus C mit $(\bigwedge^n S)_{\bar{i},\bar{m}} \neq 0$ für alle $\bar{i}$. Mit der Wahl von $\bar{m} = \bar{i}_0$ wurde die 1 im neuen Ring festgelegt. Es stellt sich die Frage, welche anderen Wahlen $\bar{m} \in C$ ganze Strukturkonstanten liefern. Wir fassen die Matrix $\tilde{s} \in \mathbb{C}^{|C|\times|C|}$,

$$\tilde{s}_{\bar{i},\bar{j}} := \frac{(\bigwedge^n S)_{\bar{i},\bar{j}}}{(\bigwedge^n S)_{\bar{i},\bar{m}}},$$

als Algebrenisomorphismus auf. Das Bild von $\bigwedge^n \mathbb{C}^e$ unter $\tilde{s}$ ist dann ein Ring mit den Strukturkonstanten

$${}_{\bar{m}}N_{\bar{j},\bar{k}}^{\bar{l}} := \sum_{\bar{i}\in C} \frac{(\bigwedge^n S)_{\bar{i},\bar{j}}(\bigwedge^n S)_{\bar{i},\bar{k}}\overline{(\bigwedge^n S)_{\bar{i},\bar{l}}}}{(\bigwedge^n S)_{\bar{i},\bar{m}}},$$

und mit der Eins $\bar{m}$. Bemerkung 2.1.5 besagt, daß $({}_{\bar{m}_1}N_{\bar{i}_0,\bar{j}}^{\bar{i}})_{\bar{i},\bar{j}}$ die inverse Matrix zu $(N_{\bar{m}_1,\bar{i}}^{\bar{j}})_{\bar{i},\bar{j}}$ ist. Damit sind alle Strukturkonstanten rationale Zahlen, aber nicht immer ganze Zahlen. Zum Beispiel haben wir bei $e = 7$, $n = 4$ für $\bar{m} = \bar{i}_0 = (0, 1, 2, 3)$ nur Strukturkonstanten aus $\{-2, -1, 0, 1, 2\}$, aber für $\bar{m} = (0, 1, 2, 4)$ die Werte $\{-1, -\frac{1}{2}, 0, \frac{1}{2}, 1\}$. Somit ist nicht jedes Basiselement geeignet. Gewisse $\bar{m}$ sind jedoch geeignet. Zwei Modifikationen an $\bar{i}_0$ liefern eine brauchbare Eins:

Für jedes $f \in \mathbb{Z}$, das teilerfremd zu e ist, sind die Potenzen $1, \zeta^f, \zeta^{f2}, \ldots, \zeta^{f(e-1)}$ unterschiedlich. Alle Argumente im Beweis von Satz 5.1.4 stimmen noch, falls wir ζ durch ζ^f ersetzen. Das Tupel $(0, f, 2f, \ldots, (n-1)f) \in (\mathbb{Z}/e\mathbb{Z})^n$ ist aber nicht immer aufsteigend sortiert. Wird zum Sortieren die Permutation σ benötigt, und ist $\bar{m}_f$ das sortierte Tupel, so ändert sich die Formel für die Strukturkonstanten nur um das Vorzeichen ε_σ, und wir haben ${}_{\bar{m}_f}N_{\bar{i},\bar{j}}^{\bar{k}} \in \mathbb{Z}$.
Für ein $r \in \mathbb{Z}$ können wir im Beweis von Satz 5.1.4 das Tupel $\bar{i}_0$ ersetzen durch $\bar{m}^{+r} := (r, r+1, \ldots, r+n-1)$. Dann ergibt sich in der letzten Formel ein zusätzlicher Faktor $\zeta^{-\sum_\nu i_\nu}$, der aber die Argumentation nicht ändert. Insgesamt erhalten wir

$${}_{\bar{m}_f^{+r}}N_{\bar{i},\bar{j}}^{\bar{k}} \in \mathbb{Z}.$$

Vielleicht liegen die Strukturkonstanten nicht mehr in $\mathbb{Z}$, wenn $\bar{m} \in C$ nicht von der Form $\bar{m}_f^{+r}$ ist. Eine notwendige Bedingung an $\bar{m}$ ist:

Proposition 5.1.7. *Damit die Strukturkonstanten zu $\bar{m}$ ganze Zahlen sind, muß zumindest*

$$|\prod_{\bar{j}\in C} D_{\bar{j},\bar{m}}| = |\prod_{\bar{j}\in C} \frac{S_{\bar{j},\bar{m}}}{S_{\bar{j},\bar{i}_0}}| = 1$$

sein.

Beweis. Wenn die Strukturkonstanten ganze Zahlen sind, dann haben die Matrizen $({}_{\bar{m}}N_{\bar{i},\bar{j}}^{\bar{k}})_{\bar{j},\bar{k}}$ ganze Einträge, und ihre Determinanten sind auch ganz.
Insbesondere ist die Determinante der Matrix $A := ({}_{\bar{m}}N_{\bar{i}_0,\bar{j}}^{\bar{k}})_{\bar{j},\bar{k}}$ ganz. Nach Bemerkung 2.1.5 ist A die inverse Matrix von $({}_{\bar{i}_0}N_{\bar{m},\bar{j}}^{\bar{k}})_{\bar{j},\bar{k}}$. Somit müssen $\det(A)$ und $\det(A^{-1})$ ganze Zahlen sein. Das geht aber nur, falls $|\det(A^{-1})| = 1$. Wir bestimmen $\det(A^{-1})$.
Dazu benötigen wir etwas Notation: Wir schreiben $S_{*,*}$ statt $(\bigwedge^n S)_{*,*}$ und $\mathrm{Sym}(C)$ für die symmetrische Gruppe auf C. Mit $\sum_{\bar{i}_{\bar{p}}\in C,\ \bar{p}\in C}$ sind $|C|$ Summen der Form $\sum_{\bar{i}\in C}$ gemeint, bei denen die Variablen durch $\bar{p} \in C$ indiziert sind. Dann ist:

$$\det(A^{-1}) = \sum_{\sigma\in\mathrm{Sym}(C)} \varepsilon_\sigma \sum_{\bar{i}_{\bar{p}}\in C,\ \bar{p}\in C} \prod_{\bar{j}\in C} \frac{S_{\bar{i}_{\bar{j}},\bar{m}} S_{\bar{i}_{\bar{j}},\bar{j}} \overline{S_{\bar{i}_{\bar{j}},\sigma(\bar{j})}}}{S_{\bar{i}_0,\bar{i}_{\bar{j}}}} =$$

$$= \sum_{\bar{i}_{\bar{p}}\in C,\ \bar{p}\in C} \det\left(\frac{S_{\bar{i}_{\bar{j}},\bar{m}} S_{\bar{i}_{\bar{j}},\bar{j}} \overline{S_{\bar{i}_{\bar{j}},\bar{k}}}}{S_{\bar{i}_0,\bar{i}_{\bar{j}}}}\right)_{\bar{j},\bar{k}} = \sum_{\bar{i}_{\bar{p}}\in C,\ \bar{p}\in C} \left(\prod_{\bar{j}\in C} \frac{S_{\bar{i}_{\bar{j}},\bar{m}} S_{\bar{i}_{\bar{j}},\bar{j}}}{S_{\bar{i}_{\bar{j}},\bar{i}_0}}\right) \det(\overline{S_{\bar{i}_{\bar{j}},\bar{k}}})_{\bar{j},\bar{k}}.$$

Nun ist $\det(\overline{S_{\bar{i}_{\bar{j}},\bar{k}}})_{\bar{j},\bar{k}}$ genau dann ungleich 0, wenn alle $\bar{i}_{\bar{j}}$, $\bar{j} \in C$ unterschiedlich sind, und falls es ungleich 0 ist, ist es gleich $\pm\det(S) = \pm 1$ (das Vorzeichen entsteht durch die Reihenfolge, in der die $\bar{i}_{\bar{j}}$ für $\bar{j}$ in C die Menge C durchlaufen). Die Menge der paarweise verschiedenen $\bar{i}_{\bar{j}}$ wird gerade durch $\mathrm{Sym}(C)$ parametrisiert: Zu $\sigma \in \mathrm{Sym}(C)$ entspricht die Menge der $\bar{i}_{\bar{j}} = \sigma(\bar{j})$. Daraus ergibt sich:

$$\det(A^{-1}) = \sum_{\sigma\in\mathrm{Sym}(C)} \varepsilon_\sigma \prod_{\bar{j}\in C} \frac{S_{\sigma(\bar{j}),\bar{m}} S_{\sigma(\bar{j}),\bar{j}}}{S_{\sigma(\bar{j}),\bar{i}_0}} =$$

$$= \sum_{\sigma\in\mathrm{Sym}(C)} \varepsilon_\sigma \left(\prod_{\bar{j}\in C} \frac{S_{\bar{j},\bar{m}}}{S_{\bar{j},\bar{i}_0}}\right) \prod_{\bar{j}\in C} S_{\sigma(\bar{j}),\bar{j}} = \prod_{\bar{j}} \frac{S_{\bar{j},\bar{m}}}{S_{\bar{j},\bar{i}_0}} \det(S) = \prod_{\bar{j}} \frac{S_{\bar{j},\bar{m}}}{S_{\bar{j},\bar{i}_0}},$$

was per Definition von $D_{*,*}$ gleich $\prod_{\bar{j}\in C} D_{\bar{j},\bar{m}}$ ist. □

5.2 Fourier-Matrizen zu $G(e,1,n)$

Die Fourier-Matrizen zu den imprimitiven komplexen Spiegelungsgruppen $G(e,1,n)$ werden in [20] eingeführt. Die zugehörigen unipotenten Grade werden in Familien zusammengefaßt. Die Fourier-Matrizen zerfallen in Blöcke, die den Familien entsprechen. Die Ergebnisse aus dem letzten Abschnitt ermöglichen es uns zu zeigen, daß jeder dieser Blöcke einen $\mathbb{Z}$-Ring mit Basis definiert.

Wir verwenden die Notation aus [20]: Es seien $m \geq 1, r > 1$ und $e \geq n_y \geq 1$ $(1 \leq y \leq r)$ mit

$$\sum_{y=1}^{r} n_y = em + 1. \tag{5.1}$$

Wie oben haben wir zu dem Raum $\bigwedge^{n_y} \mathbb{C}^e$ die kanonische Basis

$$C_{n_y} = \{(i_1, \ldots, i_{n_y}) \mid 0 \leq i_1 < \ldots < i_{n_y} \leq e-1\},$$

wobei wir das Tupel $(i_1, \ldots, i_{n_y})$ mit $\sum_{\sigma \in S_{n_y}} \varepsilon_\sigma e_{i_{\sigma(1)}} \otimes \ldots \otimes e_{i_{\sigma(n_y)}}$ identifizieren, und auf dem Raum

$$\bigwedge^{n_1} \mathbb{C}^e \otimes \cdots \otimes \bigwedge^{n_r} \mathbb{C}^e$$

haben wir eine Basis

$$E := \{\bar{i}^1 \otimes \ldots \otimes \bar{i}^r \mid \bar{i}^y \in C_{n_y}\}.$$

Darauf operiert der Automorphismus $\tilde{S} := \bigwedge^{n_1} S \otimes \cdots \otimes \bigwedge^{n_r} S$, der wie üblich die Strukturkonstanten eines Ringes definiert, der das Tensorprodukt von Ringen der obigen Form ist (siehe 2.4.1).

Für ein $a \in \mathbb{Z}/e\mathbb{Z}$ sei $E_a := \{\bar{i}^1 \otimes \ldots \otimes \bar{i}^r \in E \mid \sum_{y=1}^{r} \sum_{\nu=1}^{n_y} i_\nu^y \equiv a \pmod{e}\}$. Dann definiert die Teilmatrix $T := (\tilde{S}_{\xi_1,\xi_2})_{\xi_1,\xi_2 \in E_a}$ für ein geeignetes $\xi_0 \in E_a$ einen Ring mit den Strukturkonstanten

$${}^aN_{\xi_1,\xi_2}^{\xi_3} := e \sum_{\xi \in E_a} \frac{T_{\xi,\xi_1} T_{\xi,\xi_2} \overline{T_{\xi,\xi_3}}}{T_{\xi,\xi_0}}.$$

Bemerkung 5.2.1. *Für $a \equiv m\binom{e}{2}$ und*

$$\xi_0 = (a_1, \ldots, a_1 + n_1 - 1) \otimes \ldots \otimes (a_r, \ldots, a_r + n_r - 1)$$

mit $a_y \in \mathbb{Z}$ so, daß $\xi_0 \in E_a$, gilt

$${}^aN_{\xi_1,\xi_2}^{\xi_3} \in \mathbb{Z}$$

für alle $\xi_1, \xi_2, \xi_3 \in E_a$.

Beweis. Mit der Notation aus Satz 5.1.4 gilt mit der gleichen Argumentation für $\xi_1 = \bar{j}^1 \otimes \ldots \otimes \bar{j}^r$, $\xi_2 = \bar{k}^1 \otimes \ldots \otimes \bar{k}^r$, $\xi_3 = \bar{l}^1 \otimes \ldots \otimes \bar{l}^r \in E_a$

$$
{}^aN_{\xi_1,\xi_2}^{\xi_3} = e \sum_{\bar{i}^1\otimes\ldots\otimes\bar{i}^r\in E_a} \prod_{y=1}^{r} \frac{1}{e^{n_y}} P_{\bar{i}^y,\bar{j}^y} \overline{P_{\bar{i}^y,\bar{k}^y}} D_{\bar{i}^y,\bar{l}^y} =
$$

$$
= \frac{e}{(n_r-1)!} \left(\prod_{y=1}^{r-1} \frac{1}{n_y!} \right) \sum_{0\le i_1^1,\ldots,i_{n_1}^1 \le e-1} \cdots \sum_{0\le i_1^{r-1},\ldots,i_{n_{r-1}}^{r-1}\le e-1}
$$

$$
\sum_{\substack{0\le i_2^r,\ldots,i_{n_r}^r\le e-1 \\ (i_1^r = a - i_2^r - \ldots - i_{n_r}^r - \sum_{y=1}^{r-1}\sum_{\nu=1}^{n_y} i_\nu^y)}} \prod_{y=1}^{r} \frac{1}{e^{n_y}} P_{\bar{i}^y,\bar{j}^y} \overline{P_{\bar{i}^y,\bar{k}^y}} D_{\bar{i}^y,\bar{l}^y}.
$$

Ganz im Inneren steht eine Potenz von ζ (siehe Beweis zu Satz 5.1.4). Diese ist von der Form

$$
\zeta^{\sum_{y=1}^{r}\sum_{\nu=1}^{n_y} i_\nu^y \cdot w_{y,\nu}},
$$

wobei der Koeffizient $w := w_{r,1}$ hinter i_1^r gleich

$$
w = (j_{\sigma_1(1)}^r - k_{\sigma_2(1)}^r + m_{01} + \sum_{\nu=2}^{n_r} (m_{0\nu} - m_{1\nu} - 1))
$$

ist. Das i_1^r läßt sich aber bezüglich der anderen ausdrücken, d.h.

$$
i_1^r w = (a - i_2^r - \ldots - i_n^r - \sum_{y=1}^{r-1}\sum_{\nu=1}^{n_y} i_\nu^y) w.
$$

Wir können also zuerst von den Koeffizienten $w_{y,\nu}$ hinter $i_1^1, \ldots, i_{n_{r-1}}^{r-1}, i_2^r, \ldots, i_{n_r}^r$ jeweils ein w abziehen. Dann verläuft der Beweis wieder wie in Satz 5.1.4. Es darf aber ein Paar (σ_1, σ_2) nur um Elemente aus dem Stabilisator von 1 in S_{n_r} variiert werden; wir erhalten also den gewünschten Faktor $(n_r - 1)!$. Weil nicht über i_1^r summiert wird, ergibt dabei die letzte Summe nur ein $e^{n_r - 1}$, das zusammen mit dem vorderen e den Faktor $\frac{1}{e^{n_r}}$ aufhebt. Es bleibt noch der Faktor

$$
\zeta^{aw} = (\zeta^{\binom{e}{2}})^{mw} = (\pm 1)^{mw}
$$

übrig, welcher in $\mathbb{Z}$ liegt, da $2 \cdot \binom{e}{2}$ durch e teilbar ist. □

Die Zeilen der Matrix T sind für ein a wie in Bemerkung 5.2.1 orthogonal. Diese Eigenschaft benötigen wir, um zu zeigen, daß der zugehörige Ring ein $\mathbb{Z}$-Ring mit Basis ist.

Bemerkung 5.2.2. *Mit den Voraussetzungen aus Bemerkung 5.2.1 gilt* $eT\overline{T}^T = I$.

Beweis. Wir wollen zeigen, daß

$$\sum_{\xi\in E_a} \tilde{S}_{\xi_1,\xi}\overline{\tilde{S}_{\xi_2,\xi}} = \frac{1}{e}\delta_{\xi_1,\xi_2}$$

gilt, wobei $\xi = \bar{i}^1 \otimes \ldots \otimes \bar{i}^r$ durch E_a läuft, d.h.

$$(*) \quad \sum_{y=1}^{r}\sum_{\nu=1}^{n_y} i_\nu^y \equiv a \pmod{e}.$$

Wie im Beweis von Bemerkung 5.2.1 dürfen wir auch hier für alle $1 \leq y \leq r$ über $0 \leq i_1^y, \ldots, i_{n_y}^y < e$ statt über $0 \leq i_1^y < \ldots < i_{n_y}^y < e$ summieren. Dadurch kommt der Faktor $\frac{1}{n_y!}$ hinzu. Nun hängen die verschiedenen i_ν^y nur noch über $(*)$ voneinander ab. Wir können deshalb ohne Einschränkung $r = 1$ setzen (das vereinfacht die folgenden Formeln sehr). Dann ist mit $\xi_1 := \bar{k} := (k_1, \ldots, k_n)$, $\xi_2 := \bar{j} := (j_1, \ldots, j_n)$ und $\xi := \bar{i} := (i_1, \ldots, i_n)$

$$\sum_{\xi\in E_a} \tilde{S}_{\xi_1,\xi}\overline{\tilde{S}_{\xi_2,\xi}} = \frac{1}{n!} \sum_{\substack{0\leq i_1,\ldots,i_n\leq e-1 \\ \sum_{\nu=1}^n i_\nu \equiv a}} \sum_{\sigma_1\in S_n}\sum_{\sigma_2\in S_n} \varepsilon_{\sigma_1\sigma_2} \prod_{\nu=1}^{n} \frac{1}{e}\zeta^{k_\nu i_{\sigma_1(\nu)} - j_\nu i_{\sigma_2(\nu)}} =$$

$$= \frac{1}{n!}\sum_{\sigma_1,\sigma_2\in S_n} \varepsilon_{\sigma_1\sigma_2} \sum_{0\leq i_2,\ldots,i_n\leq e-1} \zeta^{a(k_{\sigma_1(1)} - j_{\sigma_2(1)})}\frac{1}{e^n}\prod_{\nu=2}^{n}\zeta^{i_\nu(k_{\sigma_1(\nu)} - j_{\sigma_2(\nu)} - k_{\sigma_1(1)} + j_{\sigma_2(1)})},$$

welches offenbar nur dann ungleich Null ist, wenn

$$(**) \quad k_{\sigma_1(\nu)} - j_{\sigma_2(\nu)} \equiv k_{\sigma_1(1)} - j_{\sigma_2(1)} \pmod{e}$$

für alle $1 \leq \nu \leq n$. Da aber $0 \leq k_1 < \ldots < k_n < e$ und $0 \leq j_1 < \ldots < j_n < e$ gelten, ist das nur erfüllt, falls $\sigma := \sigma_1 = \sigma_2$. Wenn $(**)$ gilt, ist mit $d := k_{\sigma(1)} - j_{\sigma(1)}$ wegen $(*)$

$$nd \equiv \sum_{\nu=1}^{n} k_\nu - j_\nu \equiv a - a \equiv 0 \pmod{e}.$$

Andererseits gilt nach Voraussetzung (Gleichung (5.1)) $n = em + 1 \equiv 1 \pmod{e}$. Es ergibt sich somit, daß die innere Summe im obigen Ausdruck nur Null ist, falls $\sigma_1 = \sigma_2$ und $(**)$ gelten, und in diesem Fall ist $d = k_{\sigma_1(1)} - j_{\sigma_2(1)} \equiv 0$, d.h.

$$\sum_{\xi\in E_a} \tilde{S}_{\xi_1,\xi}\overline{\tilde{S}_{\xi_2,\xi}} = \frac{1}{n!}\sum_{\sigma\in S_n}\zeta^{ad}\frac{1}{e} = \frac{1}{e}.$$

Außerdem folgt aus $(**)$, $d = 0$ und $\sigma_1 = \sigma_2$, daß $\bar{j} = \bar{k}$ gilt. □

Korollar 5.2.3. *Die in [20], Abschnitt 4A, Formel (4.10) definierten Matrizen definieren (nach einem Vorzeichenwechsel der Basiselemente) $\mathbb{Z}$-Ringe mit Basis, also solche mit ganzzahligen Strukturkonstanten.*

Beweis. Die Matrizen und Strukturkonstanten aus Bemerkung 5.2.1 sind genau diejenigen, die in [20] definiert werden, d.h. mit $a \equiv m\binom{e}{2} \pmod{e}$ und

$$\xi_0 = (a_1, \dots, a_1 + n_1 - 1) \otimes \dots \otimes (a_r, \dots, a_r + n_r - 1).$$

Es bleibt zu zeigen, daß es die Involution $\sim$ gibt. Wir gehen genau wie im Beweis von Satz 5.1.5 vor: Zu $\xi = (i_1^1, \dots, i_{n_1}^1) \otimes \dots \otimes (i_1^r, \dots, i_{n_r}^r) \in E_a$ sei

$$\xi' := (w_1 - i_1^1, \dots, w_1 - i_{n_1}^1) \otimes \dots \otimes (w_r - i_1^r, \dots, w_r - i_{n_r}^r),$$

mit $w_y := n_y - 1 + 2a_y$, $y = 1, \dots, r$. Dann sei $\tilde{\xi}$ das Element aus E, das aus ξ' entsteht, indem jede Klammer aufsteigend sortiert wird. Dieses liegt sogar in E_a, da

$$\sum_{y=1}^{r} \sum_{\nu=1}^{n_y} (n_y - 1 + 2a_y) - i_\nu^y = \Big(\sum_y n_y(n_y - 1) + 2n_y a_y \Big) - a =$$

$$= 2\Big(\sum_y (\sum_{\nu=0}^{n_y-1} \nu + a_y) \Big) - a \equiv 2a - a \pmod{e},$$

wobei die letzte Kongruenz aus $\xi_0 \in E_a$ folgt.
Nun zeigen wir (vergleiche 5.1.5) für alle $\xi_1, \xi_2 \in E_a$:

$${}^a N_{\xi_1,\xi_2}^{\xi_0} = \begin{cases} \delta_{\tilde{\xi}_1,\xi_2} & \text{falls } \xi_1 = \tilde{\xi}_1 \\ \pm\delta_{\tilde{\xi}_1,\xi_2} & \text{falls } \xi_1 \neq \tilde{\xi}_1. \end{cases}$$

Man rechnet leicht nach, daß für $\xi := \bar{k}^1 \otimes \dots \otimes \bar{k}^r$, $\xi_1 := \bar{i}^1 \otimes \dots \otimes \bar{i}^r$

$$\overline{T_{\xi,\xi_1}} = T_{\xi,\tilde{\xi}_1} \prod_{y=1}^{r} \gamma_{\bar{i}^y} \prod_{\nu=1}^{n_y} \zeta^{-k_\nu^y(n_y - 1 + 2a_y)},$$

wobei $\gamma_{\bar{i}^y}$ wie in Satz 5.1.5 das Vorzeichen der Permutation ist, die das zu $\bar{i}^y$ gehörige Tupel in ξ_1' aufsteigend sortiert. Mit $\xi_0 = \bar{i}_0^1 \otimes \dots \otimes \bar{i}_0^r$ folgt daraus

$${}^a N_{\xi_1,\xi_2}^{\xi_0} := e \sum_{\xi \in E_a} \frac{T_{\xi,\xi_1} T_{\xi,\xi_2} \overline{T_{\xi,\xi_0}}}{T_{\xi,\xi_0}} = \left(\prod_{y=1}^{r} \gamma_{\bar{i}^y} \gamma_{\bar{i}_0^y} \right) e \sum_{\xi \in E_a} \overline{T_{\xi,\tilde{\xi}_1}} T_{\xi,\xi_2} = \prod_{y=1}^{r} \gamma_{\bar{i}^y} \gamma_{\bar{i}_0^y} \delta_{\tilde{\xi}_1,\xi_2},$$

weil $eT\overline{T}^T = I$ (Bemerkung 5.2.2).

Der Rest des Beweises verläuft analog zum Beweis von Satz 5.1.5. □

Kapitel 6

Ringe zu Kac-Moody-Algebren

Eine ganze Reihe von Fusionsdaten erhalten wir aus den affinen Kac-Moody-Algebren (siehe [14] für die grundlegenden Definitionen).

6.1 Definitionen

Mit den Bezeichnungen aus [14] seien $\mathfrak{g}(A)$ eine affine Kac-Moody-Algebra zu einer $n \times n$-Matrix A vom Rang l, $\mathfrak{h}$ ihre Cartan Unteralgebra und $\langle\ ,\ \rangle : \mathfrak{h} \times \mathfrak{h}^* \to \mathbb{C}$ die zugehörige Paarung. Es seien

$$P := \{\lambda \in \mathfrak{h}^* \mid \langle \lambda, \alpha_i^\vee \rangle \in \mathbb{Z}, \quad i = 0, \ldots, n-1\},$$

$$P_+ := \{\lambda \in P \mid \langle \lambda, \alpha_i^\vee \rangle \geq 0, \quad i = 0, \ldots, n-1\}.$$

Die Menge P heißt das Gitter der Gewichte, Elemente von P bzw. P_+ heißen ganze Gewichte bzw. dominant ganze Gewichte.

Es sei jetzt $\mathfrak{g}(A)$ vom Typ $X_l^{(1)}$ oder $A_{2l}^{(2)}$ (damit ist $n = l+1$). Die fundamentalen Gewichte $\Lambda_i \in P$, $i = 0, \ldots, l$ werden durch die Gleichungen

$$\langle \Lambda_i, \alpha_j^\vee \rangle = \delta_{ij}, \quad \langle \Lambda_i, d \rangle = 0$$

für $j = 0, \ldots, l$ definiert, wobei $d \in \mathfrak{h}^*$ durch $\langle \alpha_i, d \rangle = \delta_{i,0}$ gegeben ist. Es sind $\{\alpha_0^\vee, \ldots, \alpha_l^\vee, d\}$ eine Basis von $\mathfrak{h}$ und $\{\alpha_0, \ldots, \alpha_l, \Lambda_0\}$ eine Basis von $\mathfrak{h}^*$. Für die fundamentalen Gewichte $\overline{\Lambda}_i$ der zugehörigen endlich dimensionalen Lie-Algebra $\mathfrak{g}^\circ$ gilt

$$\Lambda_i = \overline{\Lambda}_i + a_i^\vee \Lambda_0,$$

($\overline{\Lambda}_0 = 0$ da $a_0^\vee = 1$; eine Definition von $a_i^\vee$ findet man in [14], 6.1).

Zu jeder positiven ganzen Zahl k sei $P_+^k \subseteq P_+$ die endliche Menge der ganzen höchsten Gewichte vom Level k:

$$P_+^k := \Big\{ \sum_{j=0}^{l} \lambda_j \Lambda_j \mid \lambda_j \in \mathbb{Z}, \lambda_j \geq 0, \sum_{j=0}^{l} a_j^\vee \lambda_j = k \Big\}.$$

Kac und Peterson haben eine natürliche $\mathbb{C}$-Darstellung der Gruppe $\mathrm{SL}_2(\mathbb{Z})$ auf dem Raum definiert, der von den durch P_+^k indizierten affinen Charakteren von $\mathfrak{g}$ aufgespannt wird. In Kapitel 13, Theorem 13.8 von [14] wird das Bild von $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ unter dieser Darstellung bestimmt, die sogenannte **Kac-Peterson-Matrix**. Für affine Algebren vom Typ $X_l^{(1)}$ oder $A_{2l}^{(2)}$ ist diese Matrix

$$S_{\Lambda,\Lambda'} = c \sum_{w \in W^\circ} \det(w) \mathrm{e}^{-\frac{2\pi \imath (\overline{\Lambda}+\bar{\rho} \mid w(\overline{\Lambda}'+\bar{\rho}))}{k+h^\vee}}, \tag{6.1}$$

wobei Λ, Λ' die Menge P_+^k durchlaufen, $(\cdot \mid \cdot)$ die normierte Bilinearform aus Kapitel 6 in [14] und e die Eulersche Zahl sind. Die Konstante c spielt hier keine Rolle, da wir die Matrix als s-Matrix nutzen wollen und deshalb normieren.

Zu jedem Level gibt es eine solche Matrix, die als S-Matrix einen Ring mit Basis definiert (die obige Darstellung von $\mathrm{SL}_2(\mathbb{Z})$ ergibt sogar ein modulares Datum). Die Isomorphieklassen der Ringe zu den Matrizen vom Typ $X_l^{(1)}$ wurden von Gannon in [11] vollständig beschrieben. Im folgenden nennen wir die Ringe mit Basis, die aus einer Kac-Peterson-Matrix entstehen, **affine Ringe vom Typ $X_l^{(r)}$ und Level k**.

Beispiel 9. Die WZWV-Ringe zu p aus Kapitel 2 sind gerade die affinen Ringe vom Typ $A_1^{(1)}$, Level $(p-2)$.

6.2 Äußere Produkte und affine Algebren

Einige der Ringe, die wir in Kapitel 8 beschreiben wollen, sind affine Ringe oder zusammengesetzt aus affinen Ringen. Um dies zu erkennen, untersuchen wir die Struktur ihrer Teilringe zu Teilmengen der Basis und ihre Graduierung.

Dabei stellen wir zunächst fest, daß die affinen Ringe vom Typ $C_l^{(1)}$ äußere Produkte von affinen Ringen vom Typ $A_1^{(1)}$ sind:

Satz 6.2.1. *Es seien $k, l \in \mathbb{N}$, $k \geq 1, l \geq 2$ und S die Kac-Peterson-Matrix vom Typ $A_1^{(1)}$ und Level $(k+l-1)$. Dann ist die Kac-Peterson-Matrix vom Typ $C_l^{(1)}$ und Level k gleich dem äußeren Produkt $\bigwedge^l S$ der Matrix S.*

Beweis. Es sei A die Cartan-Matrix vom Typ $C_l^{(1)}$. Dann sind $\bar{a}, \bar{a}^\vee$ Elemente aus dem Kern von A bzw. A^T, etwa $\bar{a} := (2, \ldots, 2, 1, 1)$, $\bar{a}^\vee := (1, \ldots, 1)$ (die Indizierung der Matrix sei so, daß α_0 am Ende steht). Weiter sind $\kappa := k + h^\vee = k + \sum_{i=0}^l a_i^\vee = k + l + 1$, $\bar\rho := (1, \dots, 1)$,

$$P_+^k = \{\bar\lambda + \bar\rho \mid \bar\lambda \in \{0, \dots, k\}^l, \sum_{i=1}^l a_i^\vee \lambda_i \le k\}$$

und W° die Weylgruppe zum Typ C_l. Mit der Diagonalmatrix D, die auf der Diagonale die Einträge $\frac{a_1^\vee}{a_1}, \dots, \frac{a_l^\vee}{a_l}$ hat, schreibt sich (6.1) für $\mu, \nu \in P_+^k$:

$$S_{\mu,\nu} = c \sum_{w \in W^\circ} \det(w) \mathrm{e}^{-\frac{1}{\kappa}\mu D w^T A^{-1^T} \nu^T} = c \sum_{w \in W^\circ} \det(w) \mathrm{e}^{-\frac{1}{\kappa}\mu M_w \nu^T}$$

mit $M_w := D w^T A^{-1^T}$. Betrachten wir die Menge

$$\tilde P := \{\tilde\mu := (\mu_1, \mu_1 + \mu_2, \dots, \sum_{i=1}^l \mu_i) \mid \mu \in P_+^k\}.$$

Der Basiswechsel $\mu \mapsto \tilde\mu$ macht aus den M_w, $w \in W^\circ$, monomiale Matrizen mit Einträgen $\pm\frac{1}{2}$ (bis auf einen Faktor ist das der Basiswechsel $\alpha_i \mapsto v_i$, vergleiche [14], 6.7). Die Formel für S wird zu

$$S_{\tilde\mu,\tilde\nu} = c \sum_{\sigma \in S_l} \sum_{f \in \{\pm 1\}^l} (\varepsilon_\sigma \prod_{i=1}^l f_i) \zeta^{-\sum_{i=1}^l f_i \tilde\mu_i \tilde\nu_{\sigma(i)}} = c \sum_{\sigma \in S_l} \sum_{f \in \{\pm 1\}^l} \varepsilon_\sigma \prod_{i=1}^l f_i \zeta^{-f_i \tilde\mu_i \tilde\nu_{\sigma(i)}} =$$

$$= \tilde c \sum_{\sigma \in S_l} \varepsilon_\sigma \prod_{i=1}^l (\zeta^{\tilde\mu_i \tilde\nu_{\sigma(i)}} - \zeta^{-\tilde\mu_i \tilde\nu_{\sigma(i)}}),$$

wobei $\zeta := \mathrm{e}^{\frac{1}{2\kappa}}$. Im letzten Term erkennen wir die Determinanten der Teilmatrizen der Matrix des WZWV-Fusionsdatums, also der Kac-Peterson-Matrix vom Typ $A_1^{(1)}$ zum Level $k + l - 1 = \kappa - 1 - 1 = p - 2$, $e = 2p = 2\kappa$, wenn e, p wie in 2.3.2 definiert sind. □

Korollar 6.2.2. *Äußere Produkte von WZWV-Ringen sind Ringe mit Basis (haben ganze nicht-negative Strukturkonstanten).*

Dabei stellt sich natürlich die Frage, ob wir die äußeren Produkte von zyklischen Gruppenringen in einer ähnlichen Weise beschreiben können. Ganz so einfach wird es aber nicht sein, weil die Strukturkonstanten der affinen Ringe nicht-negative ganze Zahlen sind. Bei den äußeren Produkten hingegen haben wir Ringe wie zum Beispiel den zu $e = 4$ und $n = 2$, die nicht zu einem $\mathbb{Z}$-Ring mit Basis, der keine negativen Strukturkonstanten hat, isomorph sind.

Dennoch gibt es einen noch ungeklärten Zusammenhang:

Satz 6.2.3. *Es sei $\mathfrak{g}(A)$ eine affine Kac-Moody-Algebra vom Typ $C_l^{(1)}$. Dann ist*

$$S'_{\Lambda,\Lambda'} = c \sum_{w \in W'} \varepsilon(w) \mathrm{e}^{-\frac{2\pi\imath(\overline{\Lambda}+\bar{\rho}|w(\overline{\Lambda}'+\bar{\rho}))2}{k+h^\vee-1}}$$

die S-Matrix aus 5.1 zum n-ten äußeren Produkt vom zyklischen Gruppenring Z_e mit $e = k+l$ und $n = l$, wobei W' die symmetrische Gruppe S_l als Untergruppe der Weylgruppe W° von $\mathfrak{g}^\circ$ ist.

Die Matrizen zum äußeren Produkt und zum affinen Ring unterscheiden sich in diesem Fall also dadurch, daß nicht über die gesamte Weylgruppe summiert wird, und daß der Exponent statt $\frac{1}{k+h^\vee}$ den Wert $\frac{2}{k+h^\vee-1}$ als Faktor hat (es entstehen andere Einheitswurzeln).

Beweis. Der Beweis von 6.2.1 liefert die passende Notation. Dadurch, daß wir nur über W' summieren, wird dort der letzte Term zu

$$S_{\tilde{\mu},\tilde{\nu}} = \tilde{c} \sum_{\sigma \in S_l} \varepsilon_\sigma \prod_{i=1}^{l} \zeta^{\tilde{\mu}_i \tilde{\nu}_{\sigma(i)}},$$

und ζ wird durch den Vorfaktor im Exponenten eine $k+l$-te statt $2(k+l-1)$-te primitive Einheitswurzel: $\frac{2}{k+h^\vee-1} = \frac{2}{k+l}$ statt $\frac{1}{k+h^\vee}$. □

6.3 Berechnungen

Viele der affinen Ringe besitzen eine Graduierung. Es sei eine Graduierung gewählt, bei der der Teilring R_0 vom Grad 0 kleinstmögliche Dimension hat. Dann ist dieser Ring R_0 oft Charakterring einer endlichen Gruppe G. Wenn dies der Fall ist, beobachten wir häufig eine Ähnlichkeit des gesamten affinen Rings mit dem Darstellungsring des Quantendoppels der Gruppe G. In [6] ist eine Übersicht über solche Gemeinsamkeiten zwischen den modularen Daten von affinen Algebren und denjenigen von endlichen Gruppen zu finden. Nach einem direkten Zusammenhang wird jedoch noch gesucht.

In den folgenden Tabellen haben wir zu allen affinen Ringen mit $k \leq 10$ und höchstens 60 Basiselementen, bei denen die Weylgruppe höchstens 20000 Elemente hat, eine Graduierung mit den obigen Eigenschaften ausgerechnet und untersucht, ob R_0 ein Charakterring ist (dieser Eintrag ist nicht unbedingt eindeutig bestimmt). Falls R_0 ein Charakterring ist, befindet sich die Graduierung des Darstellungsrings des Quantendoppels in der letzten Spalte. In der Spalte „enthaltene Charakterringe“ stehen die Gruppen, deren Charakterring ein Teilring zur Teilmenge der Basis ist.

Zu den Graduierungen stehen die Anzahlen der Elemente der Mengen aus der Partition der Basis. Der Eintrag „4, 3, 3“ zum Beispiel bedeutet, daß der Ring über einem Teilring mit 4

Basiselementen C_3-graduiert ist. Die Ringe vom Typ G_2 und F_4 sind einfach (haben keine Teilringe zu Teilmengen der Basis) und haben somit auch keine interessante Graduierung. Bei den Typen E_6, E_7 und E_8 haben die Weylgruppen mehr als 20000 Elemente.

Typ $A^{(1)}$

l	k	Graduierung	enthaltene Charakterringe	R_0	Graduierung des Quantendoppels
1	1	1,1			
1	2	2,1	C_2	C_2	1,1,1,1
1	3	2,2	C_2		
1	4	3,2	C_2,S_3	S_3	6,2
1	5	3,3	C_2		
1	6	4,3	C_2		
1	7	4,4	C_2		
1	8	5,4	C_2		
1	9	5,5	C_2		
2	1	1,1,1			
2	2	2,2,2	C_3		
2	3	4,3,3	C_3,A_4	A_4	8,3,3
2	4	5,5,5	C_3		
2	5	7,7,7	C_3		
2	6	10,9,9	C_3		
2	7	12,12,12	C_3		
2	8	15,15,15	C_3		
2	9	19,18,18	C_3		
3	1	1,1,1,1			
3	2	3,3,2,2	C_2,C_4,S_3,$C_3 \rtimes C_4$	S_3	6,2
3	3	5,5,5,5	C_2,C_4		
3	4	10,8,9,8	C_2,C_4		
3	5	14,14,14,14	C_2,C_4		
4	1	1,1,1,1,1			
4	2	3,3,3,3,3	C_5		
4	3	7,7,7,7,7	C_5		
5	1	1,1,1,1,1,1			
5	2	4,4,3,4,3,3	C_2,C_3,C_6		
5	3	10,10,9,9,9,9	C_2,C_3,C_6		
6	1	1,1,1,1,1,1,1			
6	2	4,4,4,4,4,4,4	C_7		

Typ $B^{(1)}$

l	k	Graduierung	enthaltene Charakterringe	R_0	Graduierung des Quantendoppels
3	1	2,1	C_2	C_2	1,1,1,1
3	2	5,2	C_2,D_7	D_7	26,2
3	3	8,5	C_2		
3	4	14,8	C_2		
3	5	20,14	C_2		
3	6	30,20	C_2		
4	1	2,1	C_2	C_2	1,1,1,1
4	2	6,2	C_2,S_3,D_9	D_9	42,2
4	3	10,6	C_2		
4	4	20,10	C_2		
4	5	30,20	C_2		
5	1	2,1	C_2	C_2	1,1,1,1
5	2	7,2	C_2		
5	3	12,7	C_2		
5	4	27,12	C_2		

Typ $C^{(1)}$

l	k	Graduierung	enthaltene Charakterringe	R_0	Graduierung des Quantendoppels
2	1	2,1	C_2	C_2	1,1,1,1
2	2	4,2	C_2,D_5	D_5	14,2
2	3	6,4	C_2		
2	4	9,6	C_2		
2	5	12,9	C_2		
2	6	16,12	C_2		
2	7	20,16	C_2		
2	8	25,20	C_2		
2	9	30,25	C_2		
3	1	2,2	C_2		
3	2	6,4	C_2		
3	3	10,10	C_2		
3	4	19,16	C_2		
3	5	28,28	C_2		
4	1	3,2	C_2,S_3	S_3	6,2
4	2	9,6	C_2		
4	3	19,16	C_2		
5	1	3,3	C_2		
5	2	12,9	C_2		
5	3	28,28	C_2		

Typ $D^{(1)}$

l	k	Graduierung	enthaltene Charakterringe	R_0	Graduierung des Quantendoppels
4	1	1,1,1,1			
4	2	5,2,2,2	C_2,$C_2 \times C_2$,D_4,Q_8	D_4	8,2,2,2,2,2,2,2
4	3	6,6,6,6	C_2,$C_2 \times C_2$		
4	4	16,10,10,10	C_2,$C_2 \times C_2$		
5	1	1,1,1,1			
5	2	4,2,2,4	C_2,C_4,D_5	D_5	14,2
5	3	7,7,7,7	C_2,C_4		
5	4	18,12,12,16	C_2,C_4		

Typ $A_{2l}^{(2)}$

l	k	Graduierung	enthaltene Charakterringe	R_0	Graduierung des Quantendoppels
2	2	3			
2	3	2,1		C_2	1,1,1,1
2	4	6			
2	5	4,2	C_2, D_5	D_5	14,2
2	6	10			
2	7	6,4			
2	8	15			
2	9	9,6			
3	2	4			
3	3	2,2			
3	4	10			
3	5	6,4			
3	6	20			
3	7	10,10			
3	8	35			
3	9	19,16			
4	2	5			
4	3	3,2	C_2, S_3	S_3	6,2
4	4	15			
4	5	9,6			
4	6	35			
4	7	19,16			
5	2	6			
5	3	3,3			
5	4	21			
5	5	12,9			
5	6	56			
5	7	28,28			

Kapitel 7

Darstellungsring von $D(G)$

In unterschiedlichen Zusammenhängen ist der Darstellungsring des Quantendoppels einer endlichen Gruppe aufgetaucht. In der Physik finden wir ihn in der Quantenfeldtheorie. Dort wird er modulares Datum einer endlichen Gruppe genannt. In der Darstellungstheorie benutzte ihn Lusztig ([16],[17]), um die irreduziblen Charaktere von endlichen Gruppen vom Lie-Typ zu bestimmen. Die sogenannten unipotenten Charaktere führten zum Quantendoppel der Gruppen S_2^n, S_3, S_4 und S_5.

Die zu diesem Darstellungsring gehörige S-Matrix wird von Lusztig „nicht-abelsche Fouriermatrix“ genannt. Wir können diese explizit unter Benutzung der Charaktertafeln der Zentralisatoren der Elemente aus der Gruppe berechnen. Auch eine T-Matrix können wir explizit angeben. Diese Matrizen bilden ein Fusionsdatum (siehe Kapitel 2.3). Die Kategorie der Darstellungen des Quantendoppels ist sogar eine modulare Tensorkategorie (das werden wir gleich nochmals beweisen; es ist auch zum Beispiel in [2] zu finden). Eine interessante Frage, der wir hier aber nicht nachgehen, ist, zu welchen Fusionsdaten es modulare Tensorkategorien gibt, die diese definieren.

7.1 Quantendoppel einer endlichen Gruppe

Es seien G eine endliche Gruppe und N ein Normalteiler in G, so daß die Faktorgruppe G/N zyklisch der Ordnung n ist. Außerdem sei σ ein Urbild in G eines Erzeugers von G/N unter der kanonischen Projektion. Alle Sätze aus diesem Abschnitt (7.1) sind für den Fall $G = N$ zum Beispiel in [2] zu finden.

Es sei k ein Körper der Charakteristik 0. Die Gruppenalgebra $k[G]$ und die Algebra $F(N)$ der Funktionen von N nach k sind Hopf-Algebren. Wir schreiben δ_g für die Funktion $N \to k$, $h \mapsto \delta_{g,h}$.

In Analogie zum Quantendoppel versehen wir den Vektorraum $D_n = F(N) \otimes k[G]$ mit der Struktur einer Hopf-Algebra (das Quantendoppel ist der Spezialfall $N = G$):

Bemerkung 7.1.1. *Der Vektorraum $D_n = F(N) \otimes k[G]$ zusammen mit*

Multiplikation	$(\delta_g \otimes x)(\delta_h \otimes y) = \delta_{gx,xh}(\delta_g \otimes xy),$
Eins	$1 = \sum_{g\in N} \delta_g \otimes e,$
Comultiplikation	$\Delta(\delta_g \otimes x) = \sum_{g_1 g_2 = g}(\delta_{g_1} \otimes x) \otimes (\delta_{g_2} \otimes x),$
Co-Eins	$\varepsilon(\delta_g \otimes x) = \delta_{g,e},$
Antipode	$\gamma(\delta_g \otimes x) = \delta_{x^{-1}g^{-1}x} \otimes x^{-1},$

wobei $g, h, g_1, g_2 \in N$, $x, y \in G$, e neutrales Element von G sind, ist eine Hopf-Algebra. Außerdem ist

$$R = \sum_{g\in N}(\delta_g \otimes e) \otimes (\sum_{h\in N} \delta_h \otimes g)$$

eine R-Matrix, d.h. D_n ist fast cokommutativ und quasitriangulär.

Beweis. D_n ist eine Algebra:
Assoziativität der Multiplikation vererbt sich vom Quantendoppel $D(G)$ (siehe zum Beispiel [5], 4.2 D). Das Element $(\sum_{g\in N} \delta_g \otimes e)$ ist die Eins, da N ein Normalteiler ist:

$$(\delta_h \otimes x)(\sum_{g\in N} \delta_g \otimes e) = \sum_{g\in N} \delta_{hx,xg}\delta_h \otimes xe = \delta_h \otimes x,$$

$$(\sum_{g\in N} \delta_g \otimes e)(\delta_h \otimes x) = \sum_{g\in N} \delta_{ge,eh}\delta_h \otimes ex = \delta_h \otimes x.$$

D_n ist wie das Quantendoppel eine Co-Algebra.
Die Comultiplikation und die Co-Eins sind Algebrenhomomorphismen:

$$\begin{aligned}
&\Delta(\delta_g \otimes x)\Delta(\delta_h \otimes y)\\
&= (\sum_{g_1 g_2 = g} (\delta_{g_1} \otimes x) \otimes (\delta_{g_2} \otimes x))(\sum_{h_1 h_2 = h} (\delta_{h_1} \otimes y) \otimes (\delta_{h_2} \otimes y))\\
&= \sum_{g_1\in N} \sum_{h_1\in N} (\delta_{g_1 x, x h_1}\delta_{g_1} \otimes xy) \otimes (\delta_{g_1^{-1}gx, xh_1^{-1}h}\delta_{g_1^{-1}g} \otimes xy)\\
&= \sum_{g_1\in N} \sum_{h_1\in N} \delta_{x^{-1}g_1 x, h_1}\delta_{h(x^{-1}g_1^{-1}gx)^{-1}, h_1}(\delta_{g_1} \otimes xy) \otimes (\delta_{g_1^{-1}g} \otimes xy)\\
&= \sum_{g_1\in N} \delta_{x^{-1}g, hx^{-1}}(\delta_{g_1} \otimes xy) \otimes (\delta_{g_1^{-1}g} \otimes xy)\\
&= \Delta(\delta_{gx,xh}\delta_g \otimes xy),
\end{aligned}$$

$$\varepsilon(\delta_g \otimes x)\varepsilon(\delta_h \otimes y) = \delta_{g,e}\delta_{h,e} = \delta_{g,e}\delta_{gx,xh} = \varepsilon(\delta_{gx,xh}(\delta_g \otimes xy)).$$

Die Multiplikation μ und die Eins ι sind Co-Algebrenhomomorphismen:

$$\begin{aligned}
&(\mu\otimes\mu)(\Delta^{D_n\otimes D_n}((\delta_g\otimes x)\otimes(\delta_h\otimes y))\\
&=\sum_{g_1g_2=g}\sum_{h_1h_2=h}(\mu\otimes\mu)((\delta_{g_1}\otimes x)\otimes(\delta_{h_1}\otimes y)\otimes(\delta_{g_2}\otimes x)\otimes(\delta_{h_2}\otimes y)))\\
&=\sum_{g_1g_2=g}\sum_{h_1h_2=h}\delta_{g_1x,xh_1}(\delta_{g_1}\otimes xy)\otimes\delta_{g_2x,xh_2}(\delta_{g_2}\otimes xy)\\
&=\sum_{g_1g_2=g}(\delta_{g_1}\otimes xy)\otimes\delta_{g_2x,xx^{-1}g_1xh}(\delta_{g_2}\otimes xy)\\
&=\Delta(\delta_{gx,xh}(\delta_g\otimes xy))=\Delta(\mu((\delta_g\otimes x)\otimes(\delta_h\otimes y))),
\end{aligned}$$

$$\begin{aligned}
&\varepsilon^{D_n\otimes D_n}((\delta_g\otimes x)\otimes(\delta_h\otimes y))\\
&=\delta_{g,e}\delta_{h,e}=\delta_{gx,xh}\delta_{g,e}=\varepsilon(\mu((\delta_g\otimes x)\otimes(\delta_h\otimes y))),
\end{aligned}$$

$$\begin{aligned}
&(\iota\otimes\iota)(\Delta(1))=\sum_{g_1\in N}\sum_{g_2\in N}(\delta_{g_1}\otimes e)\otimes(\delta_{g_2}\otimes e)=\Delta(\iota(1)),\\
&\varepsilon(\iota(1))=\sum_{g\in N}\delta_{g,e}=1.
\end{aligned}$$

γ ist ein bijektiver k-Modul-Homomorphismus und erfüllt die Eigenschaften einer Antipode:

$$\begin{aligned}
&(\mu\circ(\gamma\otimes\mathrm{id})\circ\Delta)(\delta_g\otimes x)\\
&=\mu(\sum_{g_1g_2=g}(\delta_{x^{-1}g_1^{-1}x}\otimes x^{-1})\otimes(\delta_{g_2}\otimes x))\\
&=\sum_{g_1g_2=g}\delta_{g_1^{-1},g_2}(\delta_{x^{-1}g_1^{-1}x}\otimes e)\\
&=\delta_{g,e}\sum_{h\in N}\delta_h\otimes e=\iota(\delta_{g,e})=(\iota\circ\varepsilon)(\delta_g\otimes x).
\end{aligned}$$

Somit ist D_n eine Hopf-Algebra. Das Element R erfüllt die Bedingungen einer R-Matrix von D_n, da es die R-Matrix des Quantendoppels $D(N)$ ist: Die Gleichungen

$$\begin{aligned}
\Delta^{\mathrm{op}}(\delta_g\otimes x)\cdot R&=R\cdot\Delta(\delta_g\otimes x),\\
(\mathrm{id}\otimes\Delta)(R)&=R_{13}R_{12},\\
(\Delta\otimes\mathrm{id})(R)&=R_{13}R_{23}
\end{aligned}$$

gelten auch mit $x\in G$ (mit der Standard-Notation $R_{13}:=\sum_{g\in N}(\delta_g\otimes e)\otimes\mathbf{1}\otimes(\sum_{h\in N}\delta_h\otimes g)$ usw.). □

Da D_n eine quasitrianguläre Bialgebra ist, ist die Kategorie $\mathcal{R}ep_f(D_n)$ der endlichdimensionalen k-Darstellungen von D_n eine gezopfte Tensorkategorie (siehe [2], Beispiel 1.2.8), wobei die funktoriellen Isomorphismen $\sigma_{VW} : V \otimes W \to W \otimes V$ so definiert werden:

$$\sigma_{VW}(v \otimes w) := P(R \cdot (v \otimes w)),$$

$$P : V \otimes W \to W \otimes V, \quad v \otimes w \mapsto w \otimes v.$$

Satz 7.1.2. *Die Kategorie $\mathcal{R}ep_f(D_n)$ ist halbeinfach mit den unten definierten einfachen Objekten $V_{\bar{g},\pi}$, wobei $\bar{g}$ die Konjugationsklassen von G, die in N liegen, und π die irreduziblen Darstellungen des Zentralisators $C_G(g)$ von g durchlaufen.*

Beweis. Es sei V eine endlichdimensionale Darstellung von D_n. Wegen

$$(\delta_g \otimes e)(\delta_h \otimes e) = \delta_{g,h}(\delta_g \otimes e)$$

läßt sich $F(N)$ als Algebra in D_n einbetten, und ihre Elemente operieren als Projektoren, d.h. wir erhalten zunächst eine Zerlegung

$$(1) \quad V = \bigoplus_{g \in N} V_g, \quad V_g := (\delta_g \otimes e)V.$$

Wir schreiben $\mathbf{1} := \sum_{g \in N} \delta_g$ für die Eins in $F(N)$.
Es ist

$$(\mathbf{1} \otimes x)(\mathbf{1} \otimes y) = (\mathbf{1} \otimes xy),$$

also läßt sich auch $k[G]$ in D_n einbetten. Die Operation von $x \in k[G]$ auf einem $(\delta_g \otimes e)v \in V_g$ gibt

$$(\mathbf{1} \otimes x)(\delta_g \otimes e)v = (\delta_{xgx^{-1}} \otimes e)(\mathbf{1} \otimes x)v,$$

wir haben demnach

$$(\mathbf{1} \otimes x)V_g \subseteq V_{xgx^{-1}}.$$

Andererseits ist

$$(\delta_{xgx^{-1}} \otimes e)v = (\mathbf{1} \otimes x)(\delta_g \otimes e)(\mathbf{1} \otimes x^{-1})v,$$

also

$$(2) \quad (\mathbf{1} \otimes x)V_g = V_{xgx^{-1}}.$$

Die Gruppe G operiert auf N durch Konjugation. Dann bedeuten (1) und (2), daß V bezüglich dieser Operation ein G-äquivariantes k-Vektorbündel über N ist. Um die irreduziblen Komponenten von V zu bestimmen, müssen wir V also in irreduzible Vektorbündel zerlegen.
Über die obige Einbettung von $k[G]$ operiert auf jedem V_g der Zentralisator $C_G(g)$. Es sei R_g ein Vertretersystem für die Linksnebenklassen von $C_G(g)$ in G, d.h. G ist die disjunkte Vereinigung $G = \bigcup_{x \in R_g} xC_G(g)$.
Die Abbildung $R_g \to \bar{g}_G$, $x \mapsto g^{x^{-1}}$ ist eine Bijektion zwischen R_g und der Konjugationsklasse $\bar{g}_G$ von g in G. Wir können demnach V so zerlegen:

$$V = \bigoplus_{\bar{g}_G \subseteq N} \bigoplus_{h \in \bar{g}_G} V_h = \bigoplus_{\bar{g}_G \subseteq N} \bigoplus_{x \in R_g} (\mathbf{1} \otimes x)V_g.$$

Als $C_G(g)$-Modul zerlegen wir V_g in irreduzible Komponenten

$$V_g = \bigoplus_{\pi \in \mathrm{Irr}(C_G(g))} n_{g,\pi} \cdot \pi$$

($n_{g,\pi} \in \mathbb{N}_0$) und erhalten

$$V = \bigoplus_{\bar{g}_G \subseteq N} \bigoplus_{\pi \in \mathrm{Irr}(C_G(g))} n_{g,\pi} \bigoplus_{x \in R_g} (\mathbf{1} \otimes x)\pi.$$

Die Räume $V_{\bar{g},\pi} := \bigoplus_{x \in R_g} (\mathbf{1} \otimes x)\pi$ sind irreduzible G-äquivariante Vektorbündel über N, also irreduzible Darstellungen von D_n. □

Jeder halbeinfachen Bänder-Kategorie (siehe [2], Kapitel 2 für eine Definition) kann eine Matrix zugeordnet werden, die in [2] s-Matrix genannt wird. Das ist nicht die s-Matrix, wie wir sie in Kapitel 2 definiert haben. Um bei der Notation aus [2] zu bleiben, nennen wir diese dennoch s-Matrix. Wir schreiben, es ist die s-Matrix der Kategorie (im Gegensatz zur s-Matrix des Ringes).
Die Kategorie $\mathcal{R}ep_f(D_n)$ ist auch eine halbeinfache Bänder-Kategorie. Wenn ihre s-Matrix invertierbar ist, ist sie die S-Matrix des Grothendieck-Ringes der Kategorie. Die Kategorie ist dann eine modulare Tensorkategorie.

Satz 7.1.3. *Die Kategorie $\mathcal{R}ep_f(D_n)$ ist eine halbeinfache Bänder-Kategorie mit den einfachen Objekten $V_{\bar{g},\pi}$ aus Satz 7.1.2 und der s-Matrix*

$$s_{(\bar{g},\pi),(\bar{g}',\pi')} = \frac{1}{|C_G(g^{-1})||C_G(g')|} \sum_{\substack{h \in G \\ hg'h^{-1} \in C_G(g^{-1})}} \mathrm{tr}_{\pi^*}(hg'h^{-1}) \, \mathrm{tr}_{\pi'}(h^{-1}g^{-1}h).$$

Beweis. Wir wissen bereits, daß $\mathcal{R}ep_f(D_n)$ eine gezopfte Tensorkategorie ist. Es bleibt zu zeigen, daß jedes Objekt rechts- und linksduale Objekte hat, und daß die funktoriellen Isomorphismen $V \to V^{**}$ gewisse Bedingungen erfüllen (siehe [2], 2.2.2-2.2.4).
Zu $V_{\bar{g},\pi}$ ist das rechts- und linksduale Objekt $V^*_{\bar{g},\pi} = V_{\overline{g^{-1}},\pi^*}$. Es ist $V = V^{**}$, und die funktoriellen Isomorphismen $\delta_V : V \to V^{**}$ sind Identitätsabbildungen. Die geforderten Eigenschaften sind daher trivialerweise gegeben; $\mathcal{R}ep_f(D_n)$ ist eine Bänder-Kategorie.
Nach Satz 7.1.2 ist die Kategorie halbeinfach mit einer endlichen Anzahl von Isomorphieklassen von einfachen Objekten. Die Formel für die Matrix s überprüfen wir anhand der Definition (siehe [2], 3.1):

$$s = \frac{\tilde{s}}{D}, \quad D = \sqrt{p^+p^-}, \quad p^{\pm} = \sum_{(\bar{g},\pi)} \theta^{\pm 1}_{V_{\bar{g},\pi}} \dim(V_{\bar{g},\pi})^2,$$

$$\tilde{s}_{(\bar{g},\pi),(\overline{g'},\pi')} = \theta^{-1}_{V_{\bar{g},\pi}} \theta^{-1}_{V_{\bar{g}',\pi'}} \, \mathrm{tr}\, \theta_{V^*_{\bar{g},\pi} \otimes V_{\bar{g}',\pi'}},$$

wenn $\theta_V = \psi_V\delta_V$ die Twist-Isomorphismen sind und

$$\psi_V : V^{**} \to V, \quad v \mapsto (\mathrm{id}_V \otimes e_{V^*})(\mathrm{id}_V \otimes \sigma^{-1}_{V^*V^{**}})(i_V \otimes \mathrm{id}_{V^{**}})(v),$$

$$i_V : k \to V \otimes V^*, \quad 1 \mapsto \sum_j v_j \otimes v^j,$$

$$e_V : V^* \otimes V \to k, \quad v \otimes w \mapsto (v, w),$$

wobei $(v_j)_j$ Basis von V und $(v^j)_j$ Basis von V^*, $(\,,\,)$ das Skalarprodukt und σ_{VW} die obigen Isomorphismen sind.
Es ist

$$\sigma^{-1}_{VW} = (PR)^{-1} = (R_{21}P)^{-1} = PR^{-1}_{21} = P\sum_{g\in N}(\mathbf{1} \otimes g) \otimes (\delta_{g^{-1}} \otimes e),$$

mit

$$R_{21} := \sum_{g\in N}(\mathbf{1} \otimes g) \otimes (\delta_g \otimes e).$$

Das ergibt für θ_V auf $v \in V = V^{**}$:

$$\begin{aligned}
\theta_V(v) &= (\mathrm{id}_V \otimes e_{V^*})(\mathrm{id}_V \otimes \sigma^{-1}_{V^*V^{**}})(i_V \otimes \mathrm{id}_{V^{**}})(v)\\
&= (\mathrm{id}_V \otimes e_{V^*})(\mathrm{id}_V \otimes \sigma^{-1}_{V^*V^{**}})(\sum_i v_i \otimes v^i \otimes v)\\
&= (\mathrm{id}_V \otimes e_{V^*})(\sum_{g\in N}\sum_i v_i \otimes (\mathbf{1} \otimes g)v \otimes (\delta_{g^{-1}} \otimes e)v^i)\\
&= (\sum_{g\in N}\sum_i v_i \otimes ((\mathbf{1} \otimes g)v, (\delta_{g^{-1}} \otimes e)v^i)\\
&= (\sum_{g\in N}\sum_i v_i \cdot (\gamma^{-1}(\delta_{g^{-1}} \otimes e)(\mathbf{1} \otimes g)v^i, v)\\
&= \sum_{g\in N}(\delta_g \otimes g)\sum_i v_i \cdot (v^i, v) = \sum_{g\in N}(\delta_g \otimes g)v.
\end{aligned}$$

Auf einem $(\mathbf{1} \otimes x)v \in (\mathbf{1} \otimes x)V_{g,\pi}$ operiert $(\delta_f \otimes h) \in D_n$ folgendermaßen:

$$(*) \quad (\delta_f \otimes h)(\mathbf{1} \otimes x)(\delta_g \otimes e)v = \delta_{f,hxgx^{-1}h^{-1}}(\mathbf{1} \otimes hx)v.$$

Da g im Zentrum von $C_G(g)$ liegt, operiert es auf $V_{g,\pi}$ als Multiplikation mit $\mathrm{tr}_\pi(g)/\,\mathrm{tr}_\pi(e)$. Damit ist nach $(*)$:

$$\theta_{V_{\bar{g},\pi}}(\mathbf{1} \otimes x)v = \sum_{h\in N}\delta_{h,xgx^{-1}}(\mathbf{1} \otimes hx)v = (\mathbf{1} \otimes xg)v = \mathrm{tr}_\pi(g)/\,\mathrm{tr}_\pi(e)(\mathbf{1} \otimes x)v.$$

Es seien jetzt $v \in V_{g^{-1},\pi^*}$, $v' \in V_{g',\pi'}$, $x \in R_{g^{-1}}$, $x' \in R_{g'}$. Dann ist

$$\begin{aligned}
&\theta_{V^*_{\bar g,\pi}\otimes V_{\overline{g'},\pi'}}((\mathbf{1}\otimes x)v\otimes(\mathbf{1}\otimes x')v')\\
&= \Delta(\sum_{h\in N}(\delta_h\otimes h))((\mathbf{1}\otimes x)v\otimes(\mathbf{1}\otimes x')v')\\
&= (\sum_{h\in N}\sum_{g_1g_2=h}(\delta_{g_1}\otimes h)\otimes(\delta_{g_2}\otimes h))((\mathbf{1}\otimes x)v\otimes(\mathbf{1}\otimes x')v')\\
&= \sum_{h\in N}\sum_{g_1g_2=h}(\delta_{g_1,hxg^{-1}x^{-1}h^{-1}}(\delta_{g_1}\otimes hx)v)\otimes(\delta_{g_2,hx'g'x'^{-1}h^{-1}}(\delta_{g_2}\otimes hx')v')\\
&= \sum_{h\in N,\, xg^{-1}x^{-1}x'g'x'^{-1}=h}(\delta_{hxg^{-1}x^{-1}h^{-1}}\otimes hx)v\otimes(\delta_{hx'g'x'^{-1}h^{-1}}\otimes hx')v'\\
&= (\mathbf{1}\otimes fx)v\otimes(\mathbf{1}\otimes fx')v',
\end{aligned}$$

wobei $f := xg^{-1}x^{-1}x'g'x'^{-1}$. Nach $(*)$ ist

$$(\delta_h\otimes f)(\mathbf{1}\otimes x)v = \delta_{h,fxg^{-1}x^{-1}f^{-1}}(\mathbf{1}\otimes y)\pi^*(f')v$$

für $y \in R_{g^{-1}}$, $f' \in C_G(g^{-1})$ mit $fx = yf'$. Hierbei gilt $y = x$ genau dann, wenn $x^{-1}fx \in C_G(g^{-1})$. Analog hat man die Bedingung $x'^{-1}fx' \in C_G(g')$, die auch dazu äquivalent ist:

$$x^{-1}fxg^{-1} = g^{-1}x^{-1}fx \quad\Longleftrightarrow\quad x'^{-1}fx'g' = g'x'^{-1}fx'.$$

Jetzt können wir die Spur von $\theta_{V^*_{\bar g,\pi}\otimes V_{\overline{g'},\pi'}}$ berechnen:

$$\begin{aligned}
\operatorname{tr}\theta_{V^*_{\bar g,\pi}\otimes V_{\overline{g'},\pi'}} &= \sum_{\substack{x\in R_{g^{-1}}\\ x^{-1}fx\in C_G(g^{-1})}}\ \sum_{\substack{x'\in R_{g'}\\ x'^{-1}fx'\in C_G(g')}} \operatorname{tr}_{\pi^*}(x^{-1}fx)\operatorname{tr}_{\pi'}(x'^{-1}fx')\\
&= \sum_{\substack{x\in R_{g^{-1}},\, x'\in R_{g'}\\ x^{-1}x'g'x'^{-1}x\in C_G(g^{-1})}} \operatorname{tr}_{\pi^*}(g^{-1}x^{-1}x'g'x'^{-1}x)\operatorname{tr}_{\pi'}(x'^{-1}xg^{-1}x^{-1}x'g')\\
&= \frac{|G|}{|C_G(g^{-1})||C_G(g')|}\sum_{\substack{h\in G\\ hg'h^{-1}\in C_G(g^{-1})}} \operatorname{tr}_{\pi^*}(g^{-1}hg'h^{-1})\operatorname{tr}_{\pi'}(h^{-1}g^{-1}hg')\\
&= \theta_{V_{\bar g,\pi}}\theta_{V_{\overline{g'},\pi'}}\frac{|G|}{|C_G(g^{-1})||C_G(g')|}\sum_{\substack{h\in G\\ hg'h^{-1}\in C_G(g^{-1})}} \operatorname{tr}_{\pi^*}(hg'h^{-1})\operatorname{tr}_{\pi'}(h^{-1}g^{-1}h).
\end{aligned}$$

Es sind

$$\begin{aligned}
p^+ &= \sum_{(\bar g,\pi)} \theta_{V_{\bar g,\pi}} \dim(V_{\bar g,\pi})^2 = \sum_{(\bar g,\pi)} \frac{\mathrm{tr}_\pi(g)}{\mathrm{tr}_\pi(e)} (\sum_{x\in R_g} \dim(xV_{g,\pi}))^2 \\
&= \sum_{(\bar g,\pi)} \frac{\mathrm{tr}_\pi(g)}{\mathrm{tr}_\pi(e)} (|\bar g|\,\mathrm{tr}_\pi(e))^2 = \sum_{\bar g} |\bar g|^2 \sum_\pi \mathrm{tr}_\pi(g)\,\mathrm{tr}_\pi(e) \\
&= \sum_{\bar g} |\bar g|^2 |C_G(g)| \delta_{g,e} = |G|,
\end{aligned}$$

$$\begin{aligned}
p^- &= \sum_{(\bar g,\pi)} \theta^{-1}_{V_{\bar g,\pi}} \dim(V_{\bar g,\pi})^2 = \sum_{(\bar g,\pi)} \frac{\mathrm{tr}_\pi(e)}{\mathrm{tr}_\pi(g)} (|\bar g|\,\mathrm{tr}_\pi(e))^2 \\
&= \sum_{\bar g} |\bar g|^2 \sum_\pi \frac{\mathrm{tr}_\pi(g^{-1})}{\mathrm{tr}_\pi(e)} \mathrm{tr}_\pi(e)^2 = \sum_{\bar g} |\bar g|^2 |C_G(g)| \delta_{g^{-1},e} = |G|.
\end{aligned}$$

Insgesamt erhalten wir für s die obige Formel. □

Für den Fall $G = N$ ist $\mathcal{R}ep_f(D_n)$ sogar eine modulare Tensorkategorie, d.h. die Matrix s ist invertierbar.
Im allgemeinen ist s aber nicht invertierbar, wie zum Beispiel im Fall
$N = C_3$, $G = S_3$ mit

$$s = \begin{pmatrix}
\frac16 & \frac16 & \frac13 & \frac13 & \frac13 & \frac13 \\
\frac16 & \frac16 & \frac13 & \frac13 & \frac13 & \frac13 \\
\frac13 & \frac13 & \frac23 & -\frac13 & -\frac13 & -\frac13 \\
\frac13 & \frac13 & -\frac13 & \frac23 & -\frac13 & -\frac13 \\
\frac13 & \frac13 & -\frac13 & -\frac13 & \frac23 & -\frac13 \\
\frac13 & \frac13 & -\frac13 & -\frac13 & -\frac13 & \frac23
\end{pmatrix}.$$

7.2 $K(\mathcal{C})$ als Ring mit Basis

Wir betrachten jetzt die Kategorie $\mathcal{C}$ der Darstellungen des Quantendoppels $D(G) := F(G) \rtimes k[G]$. Der Körper k sei algebraisch abgeschlossen der Charakteristik 0. Nach 7.1.3 ist $\mathcal{C}$ eine halbeinfache Bänder-Kategorie mit den einfachen Objekten $V_0, \dots, V_m$. Dabei bezeichne $V_0 \cong k$ das Eins-Objekt. Da $D(G)$ eine Hopf-Algebra ist, existiert das Tensorprodukt $V_i \otimes V_j$ und seine Zerlegung

$$V_i \otimes V_j = \bigoplus_k N_{ij}^k \, V_k$$

definiert die Strukturkonstanten $N_{ij}^k \in \mathbb{N}$ des Grothendieck-Rings $K(\mathcal{C})$ von $\mathcal{C}$. Dieser ist als $\mathbb{Z}$-Modul isomorph zu $\mathbb{Z}^{m+1}$ mit den Erzeugern $b_0, \dots, b_m$, die sich in $K(\mathcal{C})$ folgendermaßen multiplizieren:

$$b_i \cdot b_j = \sum_k N_{ij}^k \, b_k.$$

Der Ring $K(\mathcal{C})$ ist ein Ring mit Basis mit der Involution $\widetilde{V}_{\bar{g},\pi} := V_{\overline{g^{-1}},\pi^*}$ (siehe zum Beispiel [16], 2.4).

Wir wollen im nächsten Kapitel Faktorringe von $K(\mathcal{C})$ berechnen. Dazu ist es sinnvoll zu untersuchen, wie $K(\mathcal{C})$ graduiert ist, weil wir daraus Informationen gewinnen, wie Ideale aussehen können.

7.2.1 Operation von $R(G)$ auf $K(\mathcal{C})$

Wir schreiben $R(A)$ für den Darstellungsring einer Hopf-Algebra A (d.h. für den Grothendieck-Ring der Kategorie $\mathcal{R}ep_f(A)$ der endlichdimensionalen Darstellungen von A). Für eine endliche Gruppe G schreiben wir $R(G)$ für den Ring $R(\mathbb{C}[G])$. Wir wählen für den Körper k ab jetzt die komplexen Zahlen.

Wie wir es im Beweis von Satz 7.1.2 gesehen haben, ist ein irreduzibler $D(G)$-Modul von der Form

$$\overline{W} := \bigoplus_{x \in R_g} (\mathbf{1} \otimes x) W = \operatorname{Ind}_{C_G(g)}^G W =: (g, \chi),$$

wobei W ein irreduzibler $k[C_G(g)]$-Modul mit Charakter χ ist. Multiplikation von links mit $(\mathbf{1} \otimes x)$ bildet W auf den irreduziblen $k[C_G(g^x)]$-Modul $(\mathbf{1} \otimes x)W$ ab. Multiplikation von links mit $(\delta_h \otimes e)$ für ein $h \in G$ ist eine Projektion, die W auf den Anteil W_h vom **Grad** h von W abbildet, d.h. $W = \bigoplus_{h \in G} W_h$ (hier ist nicht die Graduierung aus Abschnitt 3.2 gemeint!).

Wir schreiben ab jetzt oft nur x statt $(\mathbf{1} \otimes x)$, damit die Rechnungen übersichtlich bleiben. Die Teilring-Struktur von $K(\mathcal{C})$ wird durch folgende Bemerkung eingeschränkt (man beachte, daß dies stark von der Comultiplikation Δ in $D(G)$ abhängt):

Bemerkung 7.2.1. *Sind $\overline{W} := \bigoplus_{x \in R_g} xW$, $\overline{W}' := \bigoplus_{y \in R_{g'}} yW'$ zwei irreduzible Darstellungen von $D(G)$, so haben Elemente aus $\overline{W} \otimes \overline{W}'$ nur Anteile vom Grad $xgx^{-1}yg'y^{-1}$ mit $x \in R_g$, $y \in R_{g'}$, d.h. vom Grad h mit $h \in \bar{g}\bar{g}'$.*

Beweis. Es seien $xv \in \overline{W}$, $yw \in \overline{W}'$, d.h. $xv \otimes yw \in \overline{W} \otimes \overline{W}'$. Dann ist für ein $h \in G$

$$(\delta_h \otimes e) \cdot (xv \otimes yw) = \Delta(\delta_h \otimes e)(xv \otimes yw) = \sum_{\substack{h_1, h_2 \in G, \\ h_1 h_2 = h}} ((\delta_{h_1} \otimes e) \otimes (\delta_{h_2} \otimes e))(xv \otimes yw) =$$

$$= \sum_{\substack{h_1,h_2\in G,\\ h_1h_2=h}} (\delta_{h_1,xgx^{-1}}xv) \otimes (\delta_{h_2,yg'y^{-1}}yw) = \delta_{h,xgx^{-1}yg'y^{-1}}(xv \otimes yw),$$

d.h. $(xv \otimes yw) \in (\delta_{xgx^{-1}yg'y^{-1}} \otimes e)(\overline{W} \otimes \overline{W}')$. □

Das bedeutet, daß die Teilringe des Zentrums der Gruppenalgebra $k[G]$ die grobe Struktur der Teilringe von $K(\mathcal{C})$ liefern. Wenn $n := \dim(W)$ und $n' := \dim(W')$, so sind $\dim(\overline{W}) = |\bar{g}|n$ und $\dim(\overline{W}') = |\bar{g}'|n'$. Damit ist $\dim(\overline{W} \otimes \overline{W}') = |\bar{g}|n|\bar{g}'|n'$ und

$$\dim((\delta_h \otimes e)(\overline{W} \otimes \overline{W}')) = \sum_{\substack{h_1\in\bar{g},\, h_2\in\bar{g}'\\ h_1h_2=h}} nn'.$$

Wir schreiben jetzt wieder (g,χ) für einen irreduziblen $D(G)$-Modul $\bigoplus_{x\in R_g} xW$, wobei χ der Charakter von W ist. Es seien

$$B_g := \Big\{ \sum_{\chi\in\mathrm{Irr}(C_G(g))} n_\chi \cdot (g,\chi) \mid n_\chi \in \mathbb{Z} \Big\}$$

die von den Paaren (g,χ) mit $\chi \in \mathrm{Irr}(C_G(g))$ erzeugten $\mathbb{Z}$-Untermoduln von $K(\mathcal{C})$.

Bemerkung 7.2.2. *Der Modul B_e zum neutralen Element e ist ein Teilring zur Teilmenge $\{(e,\chi) \mid \chi \in \mathrm{Irr}(G)\}$ der Basis von $K(\mathcal{C})$, der zum Darstellungsring $R(G)$ isomorph ist.*

Beweis. Das können wir zum Beispiel mittels der Formel von Verlinde (siehe 2.4) nachprüfen: Zunächst ist nach Satz 7.1.3

$$s_{(g,\psi),(e,\chi)} = \frac{1}{|C_G(g^{-1})||G|} \sum_{h\in G} \overline{\psi(e)}\chi(h^{-1}gh) = \frac{\psi(e)\chi(g)}{|C_G(g)|}.$$

Damit ist

$$N^{(e,\chi_3)}_{(e,\chi_1),(e,\chi_2)} = \sum_{(\bar{g},\psi)\in\mathrm{Irr}(D(G))} \frac{|C_G(g)|^{-3}\psi(e)^3\chi_1(g)\chi_2(g)\overline{\chi_3(g)}}{|C_G(g)|^{-1}\psi(e)}$$

$$= \sum_{(\bar{g},\psi)} |C_G(g)|^{-2}\psi(e)^2\chi_1(g)\chi_2(g)\overline{\chi_3(g)} = \sum_{g\in G} |G|^{-1}\chi_1(g)\chi_2(g)\overline{\chi_3(g)} = (\chi_1\chi_2 \mid \chi_3)$$

weil $\sum_{\psi\in\mathrm{Irr}(C_G(g))} |C_G(g)|^{-1}\psi(e)^2 = 1$. Die Darstellungen (e,χ) verhalten sich demnach wie die Charaktere χ im Ring $R(G)$. □

Die Bemerkungen 7.2.1 und 7.2.2 besagen, daß die B_g, $g \in G$ sogar $R(G)$-Moduln sind (über die Identifizierung $B_e \cong R(G)$).

7.2.2 Abelsche Gruppen

Für den Fall, daß G abelsch ist, haben wir zwei einfache Beobachtungen:

Bemerkung 7.2.3. *Für eine endliche abelsche Gruppe G gilt $R(D(G)) \cong \mathbb{Z}[G \times G]$.*

Beweis. Die irreduziblen Darstellungen von G sind die Paare (g, χ) mit $g \in G$, $\chi \in \mathrm{Irr}(G)$. Für die S-Matrix gilt $S_{(g_1,\chi_1),(g_2,\chi_2)} = \frac{1}{|G|}\chi_1(g_2)\chi_2(g_1)$. Einsetzen in die Formel von Verlinde liefert die Behauptung. □

Bemerkung 7.2.4. *Es sei G eine endliche Gruppe. Ist $R(D(G))$ isomorph zu einem Gruppenring, so gilt*

$$R(D(G)) \cong \mathbb{Z}[G \times G].$$

Beweis. Wenn $R(D(G))$ ein Gruppenring ist, so ist auch der Charakterring von G als Teilring ein kommutativer Gruppenring. Somit muß aber G abelsch sein, und das bedeutet wiederum, daß $R(D(G)) \cong \mathbb{Z}[G \times G]$ der Gruppenring des direkten Produktes von G mit sich selbst ist. □

7.2.3 Ein Ideal in $R(D(G))$

Es sei jetzt G wieder beliebig (nicht unbedingt abelsch). Angenommen es gebe einen irreduziblen $D(G)$-Modul (e, χ) mit der Eigenschaft $(e, \chi) \cdot (e, \chi) = (e, 1)$, d.h. $\chi^2 = 1$ (wir schreiben „$\cdot$“ für das Tensorprodukt). Das könnte zum Beispiel für $G = S_n$ der Signum-Charakter sein. Das Ideal

$$I := \langle (e, 1) - (e, \chi) \rangle \trianglelefteq K(\mathcal{C})$$

wird in Kapitel 8 verwendet, um eine neue $\mathbb{Z}$-Algebra zu konstruieren, nämlich den Faktorring $K(\mathcal{C})/I$. Es sei $\pi : K(\mathcal{C}) \to K(\mathcal{C})/I$ die kanonische Projektion. Wir behaupten, daß $K(\mathcal{C})/I$ ein freier $\mathbb{Z}$-Modul ist:

Proposition 7.2.5. *Es sei (e, χ) ein irreduzibler $D(G)$-Modul mit $\chi^2 = 1$. Wenn (e, χ) via Multiplikation bijektiv auf der Basis von $K(\mathcal{C})$ operiert, so gibt es eine Teilmenge E der Basis von $K(\mathcal{C})$, so daß der Faktorring $K(\mathcal{C})/I$ eine freie $\mathbb{Z}$-Algebra mit Basis $\pi(E)$ und nicht-negativen Strukturkonstanten ist.*

Beweis. Da (e, χ) bijektiv operiert, und $\chi^2 = 1$ ist, teilt es die Basis von $K(\mathcal{C})$ in Äquivalenzklassen $\{(g, \psi), (e, \chi) \cdot (g, \psi)\}$, deren Bilder in $K(\mathcal{C})/I$ gleich sind. Es sei E ein Vertretersystem. Der $\mathbb{Z}$-Modul $R := K(\mathcal{C})/I$ ist frei, und die Menge $\pi(E)$ ist eine Basis: Angenommen, R hätte ein Torsionselement $\bar{w}$, $w \in K(\mathcal{C})$, also $n\bar{w} = 0$ für ein $n \in \mathbb{N}$.

Damit wäre $nw \in I$, d.h. von der Form $r(1-(e,\chi))$ für ein $r = \sum_i a_i b_i \in K(\mathcal{C})$, wenn b_i die Basis von $K(\mathcal{C})$ bilden. Es sei $\hat{i}$ der Index mit $b_{\hat{i}} = b_i \cdot (e,\chi)$. Dann ist

$$nw = r(1-(e,\chi)) = \sum_i a_i b_i (1-(e,\chi)) = \sum_i (a_i - a_{\hat{i}}) b_i,$$

deshalb ist $(a_i - a_{\hat{i}})$ durch n teilbar, d.h. $(a_i - a_{\hat{i}}) =: nc_i$ mit $c_i \in \mathbb{Z}$. Weiter gilt dann

$$\sum_i (a_i - a_{\hat{i}}) b_i = \sum_{b_i \in E} (a_i - a_{\hat{i}})(b_i - b_{\hat{i}}) = n \sum_{b_i \in E} c_i (b_i - b_{\hat{i}}) \in nI.$$

Ein $\mathbb{Z}$-Ring mit Basis ist aber ein freier $\mathbb{Z}$-Modul. Aus $nr_1 = nr_2$ folgt somit $r_1 = r_2$ für alle $r_1, r_2 \in K(\mathcal{C})$. Wegen $nw \in nI$ gilt also $w \in I$, d.h. $\bar{w} = 0$.
Die Strukturkonstanten $\tilde{N}^*_{*,*}$ von $K(\mathcal{C})/I$ für $b_i, b_j, b_k \in E$ sind

$$\tilde{N}^{\overline{b_k}}_{\overline{b_i},\overline{b_j}} = N^{b_k}_{b_i,b_j} + N^{(e,\chi)\cdot b_k}_{b_i,b_j}$$

und daher nicht negativ. □

7.3 Gruppen und Fusionsdaten

Zu einer modularen Tensorkategorie gehört neben der s-Matrix auch eine T-Matrix. Zusammen ergeben diese ein Fusionsdatum (Definition in 2.3) und somit eine Darstellung der Gruppe $\mathrm{PSL}_2(\mathbb{Z})$. Die S-Matrix des modularen Datums aus der Physik, das einer endlichen Gruppe zugeordnet wird (siehe [6]), ist nicht die Matrix aus Satz 7.1.3, sondern eine leichte Variante davon (sie definiert zusammen mit einer T-Matrix eine Darstellung der Gruppe $\mathrm{SL}_2(\mathbb{Z})$). Dies sind die Matrizen S, T, wie sie in [6] definiert werden:

$$S_{(a,\chi),(b,\chi')} := \frac{1}{|C_G(a)||C_G(b)|} \sum_{\substack{g\in G\\ agbg^{-1}=gbg^{-1}a}} \overline{\chi(gbg^{-1})\chi'(g^{-1}ag)},$$

$$T_{(a,\chi),(a',\chi')} := \delta_{a,a'}\delta_{\chi,\chi'}\frac{\chi(a)}{\chi(e)}.$$

Die Diedergruppe D_4 und die Quaternionengruppe Q_8 sind nicht isomorph und haben dennoch die gleiche Charaktertafel und somit isomorphe Charakterringe. Die Charaktertafel enthält deshalb nicht genug Information, um die Gruppe zu rekonstruieren. In [6] wird die Frage gestellt, ob es Quantendoppel zu verschiedenen Gruppen gibt, die gleiche S- und T-Matrizen haben. Es wird vorgeschlagen, bei Gruppen der Ordnung 16 zu suchen. Dort gibt es aber kein solches Beispiel, bei dem die Gruppen auch noch isomorphe Charakterringe haben.

Anmerkung 7.3.1. Sind zwei $\mathbb{Z}$-Ringe mit Basis nicht isomorph, so sind die zugehörigen S-Matrizen ungleich (bis auf unabhängige Permutation der Zeilen und der Spalten).

Satz 7.3.2. *Es seien $G_1 \not\cong G_2$ Gruppen der Ordnung höchstens* 50. *Dann sind entweder die Charakterringe als Ringe mit Basis nicht isomorph, oder die T-Matrizen der Quantendoppel sind nicht gleich (bis auf Permutation).*

Beweis. Ohne Einschränkung seien G_1 und G_2 nicht abelsch (nach den Bemerkungen 7.2.3 und 7.2.4). Wir berechnen mit dem Computer (Magma) zu den restlichen Gruppen der Ordnung höchstens 50 die T-Matrizen. Es gibt zwei Paare von Gruppen der Ordnung 16, die gleiches T haben. Für diese sind die Charakterringe als Ring mit Basis nicht isomorph. Bei den Gruppen der Ordnung 32 gibt es 5 solche Paare, ein 3-Tupel und zwei 4-Tupel. Bei den Gruppen der Ordnung 48 gibt es 3 Paare und ein 3-Tupel. Alle haben nicht isomorphe Charakterringe. □

Anmerkung 7.3.3. Das einzige Paar G_1, G_2 (unter den Gruppen der Ordnung höchstens 50) mit gleichem T und unterschiedlich vielen Konjugationsklassen sind die 27. und die 49. Gruppe der Ordnung 32.

Anmerkung 7.3.4. Die 13. und die 14. Gruppe der Ordnung 64 haben isomorphe Charakterringe, gleiche T-Matrizen und jeder Zentralisator der ersten Gruppe, der nicht die ganze Gruppe ist, ist isomorph zu einem Zentralisator der anderen Gruppe. Die Matrizen haben 316 Zeilen und Spalten. Es ist deshalb nicht einfach festzustellen, ob es eine monomiale Matrix M mit Einträgen in $\{1, -1\}$ gibt, so daß die S-Matrizen über M zueinander konjugiert sind. Genauso schwer ist es, einen Isomorphismus von $\mathbb{Z}$-Ringen mit Basis zwischen den Darstellungsringen der Quantendoppel zu finden. Dennoch kann nachgeprüft werden, daß es keine unabhängige Permutationen der Zeilen und Spalten gibt, die die S- und T-Matrizen der beiden Gruppen ineinander überführen.

Die Frage aus [6], ob die Matrizen S und T eine eindeutige Gruppe G festlegen, so daß sie die Matrizen zu $D(G)$ sind, können wir beantworten:

Satz 7.3.5. *Es gibt nicht-isomorphe Gruppen mit „gleichen“ S- und T-Matrizen.*

Beweis. Es seien G_1 und G_2 die 3. bzw. 13. Gruppe der Ordnung 16 in der Numerierung der „small groups“-Datenbank. Dann gibt es eine Permutation, die die S- und T-Matrizen durch simultane Zeilen- und Spaltenpermutation ineinander überführt. □

Allerdings haben diese Gruppen nicht isomorphe Charakterringe (es sind sogar die Einträge in den Charaktertafeln unterschiedlich). Das beantwortet eine andere Frage aus [6]: Die Charaktertafel kann aus den Matrizen S und T nicht rekonstruiert werden.

Offen bleibt die Frage, ob eine Gruppe schon durch die Vorgabe von S, T und ihrer Charaktertafel eindeutig bestimmt ist.

7.4 Getwistete Quantendoppel

In [9] wird erstmals beschrieben, wie das Quantendoppel einer endlichen Gruppe kohomologisch getwistet werden kann. In [6] wird sogar eine explizite Formel für die zum Darstellungsring gehörige getwistete S-Matrix gegeben, woraus wir wiederum die Strukturkonstanten gewinnen können. Wenn wir zu einer endlichen Gruppe einen expliziten 3-Kozykel haben, dann können wir diese Matrix konkret berechnen.

7.4.1 Die Quasi-Hopf Algebra $D^\omega(G)$

Es bezeichne $U(1)$ die Gruppe der komplexen Zahlen vom Betrag 1 und es sei G eine endliche Gruppe. Wir fassen $U(1)$ als $\mathbb{Z}[G]$-Modul auf, indem wir G trivial operieren lassen. Dann ist $M(G) := H^2(G, U(1))$ der Schur-Multiplikator von G. Ist $\bar{\omega}$ ein Element von $H^3(G, U(1))$, d.h. die Klasse des 3-Kozykels ω, so ist für alle $a \in G$

$$\beta_a(h, g) := \omega(a, h, g)\omega(h, h^{-1}ah, g)^{-1}\omega(h, g, (hg)^{-1}ahg)$$

eine Abbildung von $G \times G$ nach $U(1)$, die eingeschränkt auf den Zentralisator $C_G(a)$ ein 2-Kozykel aus $Z^2(C_G(a), U(1))$ ist (setzen wir die definierende Gleichung in die 2-Kozykel-Bedingung ein, so folgt dies nach viermaliger Anwendung der 3-Kozykel-Eigenschaft).

Wir definieren eine Quasi-Hopf Algebra $D^\omega(G)$. Als Vektorraum ist diese isomorph zum Quantendoppel $D(G)$. Die Multiplikation wird jedoch anders definiert (siehe zum Beispiel [8]):

$$(\delta_g \otimes x)(\delta_h \otimes y) := \delta_{gx,xh}\beta_g(x, y)(\delta_g \otimes xy).$$

In [8] werden auch die Comultiplikation, die Co-Eins und die Antipode definiert. Die Comultiplikation ist quasi-coassoziativ und sie ist ein Algebrenhomomorphismus. Die Kategorie der endlich dimensionalen Darstellungen von $D^\omega(G)$ ist halbeinfach (siehe z.B. [5], 16.1B oder [8]). In [8] wird auch erklärt, warum die Kategorie der Darstellungen von $D^\omega(G)$ nur von der Kohomologieklasse von ω abhängt.

7.4.2 $\mathrm{Irr}(D^\omega(G))$ und S-Matrix

Es sei ω ein normalisierter 3-Kozykel, d.h.

$$\omega(e, g, h) = \omega(g, e, h) = \omega(g, h, e) = 1 \quad \text{für alle} \quad g, h \in G,$$

(e neutrales Element von G). Die irreduziblen Darstellungen von $D^\omega(G)$ werden durch Paare $(\bar{a}, \chi)$ parametrisiert, wobei a wie bei $D(G)$ die Konjugationsklassen von G durchläuft und χ ein irreduzibler projektiver β_a-Charakter von $C_G(a)$ ist (siehe [8]).

Die Anzahl $r(C_G(a), \beta_a)$ der linear nicht äquivalenten irreduziblen β_a-Charaktere von $C_G(a)$ ist gleich der Anzahl der β_a-regulären Konjugationsklassen von $C_G(a)$. Ist ein $g \in C_G(a)$ β_a-regulär, so sind alle Konjugierten von g β_a-regulär, d.h. $r(C_G(a), \beta_a)$ ist kleiner oder gleich der Anzahl der Konjugationsklassen von $C_G(a)$. Es folgt:

$$|\operatorname{Irr}(D^\omega(G))| \leq |\operatorname{Irr}(D(G))|.$$

Die zu $D^\omega(G)$ gehörige S-Matrix wird in [6] explizit berechnet („ $^-$ “ ist die komplexe Konjugation):

$$\overline{S^\omega_{(\bar{a},\chi),(\bar{b},\chi')}} = \frac{1}{|G|} \sum_{g\in\bar{a},\ g'\in\bar{b}\cap C_G(g)} \frac{\beta_a(x,g')\beta_a(xg',x^{-1})\beta_b(y,g)\beta_b(yg,y^{-1})}{\beta_a(x,x^{-1})\beta_b(y,y^{-1})} \chi(h)\chi'(h'),$$

wobei $x, y \in G$, $h \in C_G(a)$, $h' \in C_G(b)$ zu g, g' so gewählt sind, daß

$$g = x^{-1}ax = y^{-1}h'y, \quad g' = y^{-1}by = x^{-1}hx.$$

Da ω normalisiert ist, folgt für die 2-Kozykel

$$\beta_e(g,h) = \beta_g(e,h) = \beta_g(h,e) = 1$$

für alle $g, h \in G$. Das bedeutet aber, daß in den Paaren $(\bar{e}, \chi)$ der Charakter χ projektiv zum trivialen 2-Kozykel ist, d.h. er ist ein gewöhnlicher Charakter von G. Für die zugehörigen Einträge in der S-Matrix vereinfacht sich die obige Formel zu

$$S^\omega_{(\bar{e},\chi),(\bar{b},\chi')} = \frac{1}{|G|} \sum_{g\in\bar{a},\ g'\in\bar{b}\cap C_G(g)} \overline{\chi(h)\chi'(h')}.$$

In der Formel von Verlinde verschwindet auch der Bruch mit den 2-Kozykeln. Es ist

$$N^{(\bar{a},\eta)}_{(\bar{e},\chi_1)(\bar{e},\chi_2)} = 0, \quad N^{(\bar{e},\chi_3)}_{(\bar{e},\chi_1)(\bar{e},\chi_2)} = (\chi_1\chi_2 \mid \chi_3)$$

für $\chi_1, \chi_2, \chi_3 \in \operatorname{Irr}(G)$, $e \neq a \in G$, $\eta \in \operatorname{Irr}(C_G(a))$. Somit ist auch in $R(D^\omega(G))$ der Charakterring von G ein Teilring zur Teilmenge der Basis.

7.5 Explizite Berechnungen

7.5.1 Berechnung von $H^3(G, U(1))$

Wir beschreiben nun ein Verfahren, um die Gruppe H^3 explizit auszurechnen. Es sei G eine endliche Gruppe. Ein Kozykel aus $Z^3(G, U(1))$ (G operiert trivial auf $U(1)$) ist eine Abbildung

$$\alpha : G \times G \times G \to U(1)$$

mit der Eigenschaft

$$\alpha(g,h,k)\alpha(h,k,l)\alpha(g,hk,l) = \alpha(gh,k,l)\alpha(g,h,kl).$$

Wir können fordern, daß es ein $n \in \mathbb{N}$ gibt, so daß alle Werte von α Potenzen von ζ sind, wobei ζ eine primitive n-te Einheitswurzel in $U(1)$ ist. Denn falls dies nicht der Fall ist, ist α kohomolog zu einem Kozykel, der diese Eigenschaft hat (siehe [6]).

Somit ist $\alpha(g,h,k) = \zeta^{\gamma(g,h,k)}$ für eine passende Abbildung $\gamma : G \times G \times G \to \mathbb{Z}/n\mathbb{Z}$ mit der Eigenschaft

$$\gamma(g,h,k) + \gamma(h,k,l) + \gamma(g,hk,l) - \gamma(gh,k,l) - \gamma(g,h,kl) = 0. \tag{7.1}$$

Umgekehrt liefert jedes solche γ natürlich einen 3-Kozykel. Die Abbildung γ ist aber Lösung des linearen Gleichungssystems, das $\gamma(g,h,k)$ als Variablen und zu jedem Tupel $(g,h,k,l) \in G \times G \times G \times G$ eine Gleichung der Form 7.1 hat. Den Lösungsraum bezeichnen wir mit Z. Er ist isomorph zu $Z^3(G,U(1))$ als abelsche Gruppe.

Die Gruppe $Z^3(G,U(1))$ ist sehr groß (hat viele Erzeuger), $H^3(G,U(1))$ ist dagegen sehr klein, weil es fast genauso viele Koränder wie Kozykel gibt. Da die Twists, die von einem 3-Kozykel herkommen, für kohomologe 3-Kozykel gleich sind, sind wir an einem Vertretersystem der Gruppe $H^3(G,U(1))$ interessiert. Wir berechnen den Teilmodul $B^3(G,U(1))$ von $Z^3(G,U(1))$, indem wir die Bilder

$$\gamma(g,h,k) := \beta(h,k) - \beta(g,h) + \beta(g,hk) - \beta(gh,k)$$

von $\beta : G \times G \to \mathbb{Z}/m\mathbb{Z}$ als Erzeuger nehmen. Hier müssen wir vorsichtig sein: Wir dürfen bei den 2-Koketten β nicht Abbildungen nach $\mathbb{Z}/n\mathbb{Z}$ wählen, da es 3-Kozykel mit Werten in $\mathbb{Z}/n\mathbb{Z}$ gibt, die über Koränder mit Werten in $\mathbb{Z}/m\mathbb{Z}$ mit $m > n$ nullkohomolog sind. Wir wählen ein $a \in \mathbb{N}$ und erweitern alle 3-Kozykel γ (Lösungen des obigen Gleichungssystems) zu

$$\gamma' : G \times G \times G \to \mathbb{Z}/an\mathbb{Z}, \quad (g,h,k) \mapsto a \cdot \gamma(g,h,k).$$

Dabei wird aus Z die Teilmenge Z' des Lösungsraums zu $a \cdot n$ statt n (in Z' sind nicht alle 3-Kozykel mit Werten in $\mathbb{Z}/an\mathbb{Z}$). Dann erzeugen wir den Modul B durch die Bilder aller 2-Koketten

$$\beta_{(g,h)} : G \times G \to \mathbb{Z}/an\mathbb{Z}, \quad (k,l) \mapsto \delta_{(k,l),(g,h)},$$

für alle $(g,h) \in G \times G$. Dieser ist kein Teilmodul von Z, enthält aber alle nötigen Koränder: Wenn wir a groß genug gewählt haben (im schlechtesten Fall a=n), liegen in B alle nullkohomologen 3-Kozykel mit Werten in $a \cdot \mathbb{Z}/an\mathbb{Z}$, d.h. alle Elemente aus Z', die nullkohomolog sind.

Für genügend großes a ist $Z/(B \cap Z)$ als abelsche Gruppe also isomorph zu $H^3(G,U(1))$ und wir haben explizite 3-Kozykel (Repräsentanten der Klassen), die wir zur Berechnung der projektiven Darstellungen der Zentralisatoren verwenden können.

Beispiel 10. Es sei $G = D_4$ die Diedergruppe mit 8 Elementen. Dann haben wir ein Gleichungssystem mit $8^4 = 4096$ Gleichungen und $8^3 = 512$ Variablen. Der Computer liefert innerhalb einer Sekunde (mit dem System Magma), daß der Lösungsraum für $n = 4$ Rang 61 über $\mathbb{Z}/4\mathbb{Z}$ hat. Der Teilraum der Koränder hat Rang 57 und der Faktormodul ist isomorph zu $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$.

Wenn man nur an bestimmten Kozykeln interessiert ist, kann man die Berechnung deutlich beschleunigen, indem man noch Zusatzbedingungen an den Kozykel stellt (z.B. $\alpha(1, g, h) = \alpha(g, 1, h) = \alpha(g, h, 1) = 1$ für alle $g, h \in G$).

7.5.2 Berechnung von projektiven Darstellungen

Es sei G eine endliche Gruppe mit neutralem Element e und $C_n := \mathbb{Z}/n\mathbb{Z}$. Es sei

$$\beta : G \times G \to C_n$$

ein normalisierter 2-Kozykel, $\beta \in Z^2(G, C_n)$. Normalisiert bedeutet $\beta(e, g) = \beta(g, e) = 0$ für alle $g \in G$. Damit definiert β eine zentrale Erweiterung Γ von G durch C_n:

$$\Gamma := G \times C_n, \quad (g, \eta) \cdot (h, \tau) := (gh, \eta + \tau + \beta(g, h))$$

für $g, h \in G$, $\eta, \tau \in C_n$. Da β normalisiert ist, ist $(e, \eta) \cdot (g, \tau) = (g, \eta + \tau)$, womit

$$1 \longrightarrow C_n \longrightarrow \Gamma \longrightarrow G \longrightarrow 1$$

eine zentrale Erweiterung ist. Für eine Darstellung ρ von Γ mit $\rho((e, 1)) = \zeta I$ (ζ n-te primitive Einheitswurzel) gilt:

$$\rho((g, 0) \cdot (h, 0)) = \rho((gh, \beta(g, h)) = \rho((gh, 0) \cdot (e, \beta(g, h))) = \zeta^{\beta(g,h)} \rho((gh, 0)),$$

$\rho' : G \to \mathbb{C}$, $\rho'(g) := \rho((g, 0))$, ist also eine projektive Darstellung zum 2-Kozykel $\beta' \in Z^2(G, U(1))$ von G mit $\beta'(g, h) = \zeta^{\beta(g,h)}$. Andererseits ist jede projektive β'-Darstellung von G von dieser Form (siehe zum Beispiel [13], Theorem 11.28). Wir wissen sogar, daß ρ genau dann irreduzibel ist, wenn ρ' irreduzibel ist.

Konkret bedeutet dies, daß wir die irreduziblen projektiven Charaktere von G zu β' erhalten, indem wir die irreduziblen Charaktere von Γ berechnen, die auf $(e, 1)$ den Wert ζ haben.

7.5.3 Beispiele für getwistete Quantendoppel

Die letzten beiden Abschnitte ermöglichen es uns, für kleine Gruppen G alle getwisteten S-Matrizen zu $D^\omega(G)$ zu bestimmen. Wir können auch untersuchen, ob die zugehörigen Ringe eventuell zu anderen bekannten Ringen isomorph sind.

Wir wollen alle solche Ringe bestimmen, die höchstens 20 Basiselemente haben. Die Gruppen, aus denen solche entstehen können, wurden in [6], Theorem 4 ohne Beweis angegeben:

Satz 7.5.1 (Coste, Gannon, Ruelle). *Die einzigen Gruppen, für die $D^\omega(G)$ höchstens* 20 *irreduzible Darstellungen haben kann, sind C_1, C_2, C_3, S_3, A_4, C_4, $C_2 \times C_2$, D_5, S_4, D_4 und eine Frobenius-Gruppe der Ordnung* 48. *Diese haben mindestens* 1, 4, 9, 8, 14, 16, 16, 16, 18, 19, 19 *irreduzible Darstellungen.*

Diese Frobenius-Gruppe der Ordnung 48 liegt außerhalb der Reichweite der Methode aus den letzten Abschnitten. Vermutlich haben die getwisteten Quantendoppel dieser Gruppe aber wesentlich mehr als 19 irreduzible Darstellungen, weil die ungetwistete Algebra schon mehr als 50 hat.

Beispiel 11. Es sei $G = C_2 \times C_2$. Es gibt (bis auf Kohomologie) 8 normalisierte 3-Kozykel in $Z^3(G, U(1))$. Diese liefern zwei Isomorphieklassen von $\mathbb{Z}$-Ringen mit Basis der Form $R(D^\omega(G))$. Die eine hat Elemente isomorph zu $R(D(G))$, die andere zu $R(D(C_4))$.
Zu $G = C_4$ gibt es unter den getwisteten Ringen (bis auf Isomorphie) auch nur zwei Ringe. Derjenige, der nicht zu $R(D(G))$ isomorph ist, ist isomorph zum Gruppenring von $C_2 \times C_8$. Dieser kann aber nicht von der Form $R(D(H))$ für eine Gruppe H sein, denn $C_2 \times C_8$ ist nicht von der Form $H \times H$ (nach Bemerkung 7.2.4).

7.5.4 Daten

In den nachfolgenden Tabellen stehen alle Ringe, die zu getwisteten Quantendoppeln von Gruppen der Ordnung bis einschließlich 50 gehören, bei denen das ungetwistete $D(G)$ höchstens 30 irreduzible Darstellungen hat. (Das Quantendoppel der obigen Frobenius-Gruppe hat 94 irreduzible Darstellungen.)

Oft sind die Daten aus den Tabellen für verschiedene 3-Kozykel gleich. Deshalb sind die zugehörigen Zeilen dann in eine einzige Zeile zusammengefaßt. Die Anzahl dieser Zeilen steht in der ersten Spalte („Anzahl“). (In einer Tabelle ist demnach die Summe der Einträge der ersten Spalte gleich der Ordnung von $H^3(G, \mathbb{C}^\times)$.)
In der zweiten Spalte steht die Anzahl der Basiselemente des Ringes. Ein Eintrag n^k in der Spalte „Teilringe“ bedeutet, daß es k Teilringe zu Teilmengen mit n Elementen der Basis gibt.
Zur Graduierung stehen hier aus Platzgründen nur die Vielfachheiten der Anzahlen der Basiselemente, die zu einem Grad gehören. Ein Eintrag „$4^3, 10$“ etwa bedeutet, daß sich die Basis durch die Graduierung in $4+4+4+10$ Elemente partitioniert. Oder „1^{16}“ zum Beispiel bedeutet, daß der Ring ein Gruppenring ist.
Steht in der letzten Spalte d, so liegen die Einträge der S-Matrix in $\mathbb{Q}(\zeta_d)$, wobei ζ_d eine primitive d-te Einheitswurzel ist (dieses d ist minimal).
Zum Beispiel haben wir bei der zyklischen Gruppe mit drei Elementen immer die Gradu-

ierung 1^9. Wenn dann $d = 3$ ist, muß der Ring isomorph zu $\mathbb{Z}[C_3 \times C_3]$ sein. Ist $d = 9$, so ist er isomorph zu $\mathbb{Z}[C_9] = Z_9$.

Es fällt bei den Tabellen sofort auf, daß hier die getwisteten Quantendoppel für alle Kozykel gleich viele irreduzible Darstellungen haben. Das liegt aber nur daran, daß die Beispiele noch zu klein sind. Ein Beispiel, daß das nicht immer so ist, ist $G = C_2^3$. Das Quantendoppel $D(G)$ hat 64 irreduzible Darstellungen und kommt deshalb nicht in den Tabellen vor. Man kann aber mit der obigen Methode ausrechnen, daß es Kozykel ω gibt, für die $D^\omega(G)$ nur 22 irreduzible Darstellungen hat. In [7] wird gezeigt, daß verschiedene Kozykel Darstellungsringe ergeben, die zu $D(D_4)$ oder $D(Q_8)$ isomorph sind.

Gruppe: $G := C_2$, $H^3(G, \mathbb{C}^\times)$: C_2,

Anzahl	$\|B\|$	Teilringe	Graduierung	$\mathbb{Q}(\zeta)$
2	4	$1, 2^3$	1^4	1

Gruppe: $G := C_3$, $H^3(G, \mathbb{C}^\times)$: C_3,

Anzahl	$\|B\|$	Teilringe	Graduierung	$\mathbb{Q}(\zeta)$
1	9	$1, 3^4$	1^9	3
2	9	$1, 3$	1^9	9

Gruppe: $G := C_4$, $H^3(G, \mathbb{C}^\times)$: C_4,

Anzahl	$\|B\|$	Teilringe	Graduierung	$\mathbb{Q}(\zeta)$
2	16	$1, 2^3, 4^7, 8^3$	1^{16}	4
2	16	$1, 2^3, 4^3, 8^3$	1^{16}	8

Gruppe: $G := C_2 \times C_2$, $H^3(G, \mathbb{C}^\times)$: $C_2 \times C_2 \times C_2$,

Anzahl	$\|B\|$	Teilringe	Graduierung	$\mathbb{Q}(\zeta)$
4	16	$1, 2^3, 4^7, 8^3$	1^{16}	4
4	16	$1, 2^{15}, 4^{35}, 8^{15}$	1^{16}	1

Gruppe: $G := C_5$, $H^3(G, \mathbb{C}^\times)$: C_5,

Anzahl	$\|B\|$	Teilringe	Graduierung	$\mathbb{Q}(\zeta)$
4	25	$1, 5$	1^{25}	25
1	25	$1, 5^6$	1^{25}	5

Gruppe: $G := S_3$, $H^3(G, \mathbb{C}^\times)$: C_6,

Anzahl	$\|B\|$	Teilringe	Graduierung	$\mathbb{Q}(\zeta)$
4	8	$1, 2, 3, 6$	$2, 6$	9
2	8	$1, 2, 3^4, 6$	$2, 6$	1

Gruppe: $G := D_4$, $H^3(G, \mathbb{C}^\times)$: $C_2 \times C_2 \times C_4$,

Anzahl	$\|B\|$	Teilringe	Graduierung	$\mathbb{Q}(\zeta)$
8	22	$1, 2^7, 4^7, 5^{14}, 8, 10^7, 14^7$	$2^7, 8$	1
8	22	$1, 2^3, 4^3, 5^2, 7^2, 8, 10, 14^3$	$2^6, 5^2$	8

Gruppe: $G := Q_8$, $H^3(G, \mathbb{C}^\times)$: C_8,

Anzahl	$\|B\|$	Teilringe	Graduierung	$\mathbb{Q}(\zeta)$
4	22	$1, 2^7, 4^7, 5^{14}, 8, 10^7, 14^7$	$2^7, 8$	1
4	22	$1, 2^7, 4^7, 5^2, 7^6, 8, 10, 11^4, 14^3$	$2^6, 5^2$	8

Gruppe: $G := D_5$, $H^3(G, \mathbb{C}^\times)$: C_{10},

Anzahl	$\|B\|$	Teilringe	Graduierung	$\mathbb{Q}(\zeta)$
2	16	$1, 2, 4^6, 14$	$2, 14$	5
8	16	$1, 2, 4, 14$	$2, 14$	25

Gruppe: $G := A_4$, $H^3(G, \mathbb{C}^\times)$: C_6,

Anzahl	$\|B\|$	Teilringe	Graduierung	$\mathbb{Q}(\zeta)$
1	14	$1, 3, 4^5, 8$	$3^2, 8$	3
1	14	$1, 3, 4, 8$	$3^2, 8$	12
2	14	$1, 3, 4, 8$	$3^2, 8$	36
2	14	$1, 3, 4^5, 8$	$3^2, 8$	9

Gruppe: $G := D_7$, $H^3(G, \mathbb{C}^\times)$: C_{14},

Anzahl	$\|B\|$	Teilringe	Graduierung	$\mathbb{Q}(\zeta)$
2	28	$1, 2, 5^8, 26$	$2, 26$	7
12	28	$1, 2, 5, 26$	$2, 26$	49

Gruppe: $G := (20, 3) \cong C_5 \rtimes C_4$, $H^3(G, \mathbb{C}^\times)$: C_4,

Anzahl	$\|B\|$	Teilringe	Graduierung	$\mathbb{Q}(\zeta)$
2	22	$1, 2, 4, 5^2, 10, 14$	$4^3, 10$	40
2	22	$1, 2, 4, 5^2, 10, 14$	$4^3, 10$	20

Gruppe: $G := (21, 1) \cong C_7 \rtimes C_3$, $H^3(G, \mathbb{C}^\times)$: C_3,

Anzahl	$\|B\|$	Teilringe	Graduierung	$\mathbb{Q}(\zeta)$
2	25	$1, 3, 5^2, 19$	$3^2, 19$	63
1	25	$1, 3, 5^2, 19$	$3^2, 19$	21

Gruppe: $G := S_4$, $H^3(G, \mathbb{C}^\times)$: $C_2 \times C_{12}$,

Anzahl	$\|B\|$	Teilringe	Graduierung	$\mathbb{Q}(\zeta)$
4	21	$1, 2, 3, 5^3, 10, 13$	$8, 13$	1
8	21	$1, 2, 3, 5^3, 10, 13$	$8, 13$	9
8	21	$1, 2, 3, 5, 10, 13$	$8, 13$	72
4	21	$1, 2, 3, 5, 10, 13$	$8, 13$	8

Kapitel 8

Anwendungen

In [12] werden anhand der Eigenschaften, die Fourier-Transformationen und Frobenius-Eigenwerte erfüllen müssen, für endliche Coxeter-Gruppen Fusionsdaten definiert. Die zugehörigen Ringe können wir zum Teil mit den Methoden aus den vorherigen Kapiteln zerlegen und damit sozusagen verstehen. „Verstehen“ bedeutet, daß sie aus verschiedenen Konstruktionen entstehen, die wir in den nächsten Abschnitten beschreiben werden.

Wir konzentrieren uns dann auf die Fourier-Matrizen der spetsiellen exzeptionellen irreduziblen komplexen Spiegelungsgruppen (insgesamt 274 Matrizen). Wir schreiben G_n-m für den Ring, der zur Fourier-Matrix der m-ten Familie der exzeptionellen Spiegelungsgruppe G_n gehört.

8.1 Komplexe Spiegelungsgruppen

Wir benötigen für die folgenden Abschnitte ein paar Begriffe (vergleiche [22]).

Es sei V ein endlich dimensionaler $\mathbb{C}$-Vektorraum. Ein Element $g \in \mathrm{GL}(V)$ heißt **komplexe Spiegelung**, falls $\mathrm{codim}(\ker(g-1)) = 1$ gilt, d.h. wenn g eine Hyperebene punktweise fixiert. Eine endliche Untergruppe $W \leq \mathrm{GL}(V)$, die von komplexen Spiegelungen erzeugt wird, heißt **komplexe Spiegelungsgruppe**.

Es seien $e, n \in \mathbb{Z}$, $n \geq 1$, $e \geq 2$ und $\zeta \in \mathbb{C}$ eine primitive e-te Einheitswurzel. Weiterhin seien s_0 die Diagonalmatrix mit $(\zeta, 1, \ldots, 1)$ auf der Diagonalen und s_i, $1 \leq i \leq n-1$ die zu den Transpositionen $(i, i+1)$ gehörigen $n \times n$ Permutationsmatrizen. Dann ist

$$G(e, 1, n) := \langle s_0, s_1, \ldots, s_{n-1} \rangle \leq \mathrm{GL}_n(\mathbb{C})$$

eine irreduzible n-dimensionale komplexe Spiegelungsgruppe. Die Abbildung

$$\gamma : G(e, 1, n) \to \mathbb{C}^\times, \qquad \gamma(s_0) := \zeta, \quad \gamma(s_i) := 1 \quad (1 \leq i \leq n-1),$$

definiert einen linearen Charakter von $G(e, 1, n)$. Für ein $p|e$, $(e, p, n) \neq (2, 2, 2)$ und $n > 1$ für $p > 1$ ist die Gruppe $G(e, p, n) := \ker(\gamma^{e/p})$ auch eine irreduzible komplexe Spiegelungsgruppe.

Jede irreduzible komplexe Spiegelungsgruppe ist nach der Klassifizierung von Shephard und Todd [26] entweder eine symmetrische Gruppe S_n, eine Gruppe der Form $G(e, p, n)$ oder eine von 34 exzeptionellen Gruppen, die wir mit $G_4, \ldots, G_{37}$ bezeichnen.

In [23], 8A werden anhand von sechs äquivalenten charaktertheoretischen Bedingungen an eine endliche irreduzible komplexe Spiegelungsgruppe die sogenannten **spetsiellen Spiegelungsgruppen** definiert. Dort wird auch gezeigt, daß das folgende Gruppen sind:

$$S_n, \quad G(e, 1, n), \quad G(e, e, n), \quad G_i \text{ mit } i \in \{4, 6, 8, 14, 23, \ldots, 30, 32, \ldots, 37\}.$$

Die unipotenten Charaktergrade und die Scheingrade (fake degrees) dieser Gruppen bilden Vektoren v bzw. w aus $\mathbb{C}[X]^m$ für ein geeignetes m (siehe [20]). Wenn diese Grade als Vektoren über $\mathbb{C}$ aufgefasst werden, kann man eine gewisse Übergangsmatrix zwischen v und w festlegen, die Fourier-Transformation (oder Fouriermatrix) genannt wird.

Eine solche $m \times m$ Fouriermatrix zerfällt in Blöcke. Diese Blöcke definieren eine Partition von $\{1, \ldots, m\} = F_1 \cup \ldots \cup F_r$ für ein geeignetes $r \in \mathbb{N}$. Wir bezeichnen mit $\mathcal{F}_i$ die Liste der unipotenten Charaktergrade v_j, $j \in F_i$ und mit $\mathfrak{F}$ die Menge der $\mathcal{F}_i$, $1 \leq i \leq r$.

Für eine Familie $\mathcal{F} \in \mathfrak{F}$ definieren wir

$$\begin{aligned} a(\mathcal{F}) &:= \max\{i \in \mathbb{Z} \mid X^i | g \text{ für alle } g \in \mathcal{F}\}, \\ A(\mathcal{F}) &:= \max\{\deg g \mid g \in \mathcal{F}\}. \end{aligned}$$

Durch die Zahlen $a(\mathcal{F})$, $A(\mathcal{F})$ und $|\mathcal{F}|$ ist die Familie $\mathcal{F}$ eindeutig bestimmt.

8.2 Fouriermatrizen und Konstruktionen

Bis auf drei Fälle können wir für alle Fouriermatrizen, die zu Familien der Spetses gehören, einfache Konstruktionsvorschriften angeben, um die entsprechenden Ringe zu erhalten.

Diese sind zusammengesetzt aus

(i) Charakterringen von endlichen Gruppen ($R(G)$),

(ii) Darstellungsringen von Quantendoppeln endlicher Gruppen ($R(D(G))$),

(iii) Affinen Ringen.

Die Operationen, die wir dabei verwenden, sind:

(a) Tensorprodukte und äußere Produkte,

(b) Übergang zu Faktorringen,

(c) Übergang zu Teilringen zu Teilmengen der Basen,

(d) Basiswechsel.

Die meisten unserer Ringe sind einfach vom Typ (i), (ii) und (iii) ohne irgendeine Operation darauf anzuwenden.

Wir bezeichnen mit $X_{l,k}^{(r)}$ den affinen Ring vom Typ $X_l^{(r)}$ und Level k.

8.2.1 Involution $\sim$ und negative Strukturkonstanten

Betrachten wir den Ring $Z_n := \mathbb{Z}[\mathbb{Z}/n\mathbb{Z}]$ mit der Basis $\{b_0, \ldots, b_{n-1}\}$ (so daß $b_i b_j = b_{(i+j \mod n)}$). Dies ist ein Ring mit Basis mit der Involution $\tilde{b}_i = b_{(-i \mod n)}$. Insbesondere ist $\sim$ für $n > 2$ nicht die identische Abbildung. Eine häufige Situation ist folgende: Es sei R ein $\mathbb{Z}$-Ring mit Basis B, der C_2-graduiert ist, d.h. die Basis teilt sich in zwei Mengen: die Elemente $B_0 := \{b_1, \ldots, b_p\}$ vom Grad 0 und die Elemente $B_1 := \{c_1, \ldots, c_q\}$ vom Grad 1:

$$B = \{\underbrace{b_1, \ldots, b_p}_{0}, \underbrace{c_1, \ldots, c_q}_{1}\}.$$

Das Produkt zweier Elemente vom Grad 1 ist eine Kombination der Elemente aus B_0. Der von B_0 erzeugte $\mathbb{Z}$-Modul ist ein Teilring zur Teilmenge B_0. Das bedeutet allerdings nicht, daß es einen Ring $\tilde{R}$ gibt mit $R = \tilde{R} \otimes Z_2$. Zum Beispiel ist der Wess-Zumino-Witten-Verlinde-Ring (siehe 2.3.2) C_2-graduiert über dem Teilring, der von $\{b_1, b_3, b_5, \ldots\}$ erzeugt wird, aber nicht gleich dem Tensorprodukt dieses Teilrings mit Z_2.

Wir können die Basis von R verdoppeln und damit erreichen, daß der neue Ring R' (mit der Multiplikation, die wir gleich noch definieren) C_4-graduiert ist: Die neue Basis ist

$$B' := \{\underbrace{b_1, \ldots, b_p}_{0}, \underbrace{c_1, \ldots, c_q}_{1}, \underbrace{b'_1, \ldots, b'_p}_{2}, \underbrace{c'_1, \ldots, c'_q}_{3}\}.$$

In R gilt $c_i c_j = \sum_{k=1}^{p} N_{c_i c_j}^{b_k} b_k$. In R' ist dann $c_i c_j = \sum_{k=1}^{p} N_{c_i c_j}^{b_k} b'_k$ eine Kombination von Elementen vom Grad 2. Diese Graduierung erhält man auch anders: R' ist isomorph zu einem Teilring von $R \otimes Z_4$.

Dieser Vorgang ist interessant, weil wir dadurch die Involution $\sim$ verändern können. War $\sim$ auf R noch trivial, so ist es auf R' nicht mehr die Identität, weil R' C_4-graduiert ist: $\tilde{c}_i = c'_i$.

In vielen Fällen gibt es in R ein Element b_i (vom Grad 0) mit $b_i^2 = 1$ und derart, daß Multiplikation mit b_i die Basiselemente von R permutiert. Wir definieren ein Ideal in R':

$$I := \langle a + b'_i \cdot a \mid a \in B' \rangle,$$

wobei b'_i das zu b_i entsprechende Element vom Grad 2 ist. Wenn der Faktorring R'/I ein $\mathbb{Z}$-Ring mit Basis ist, dann ist die zugehörige Involution $\sim$ meistens nicht trivial.

Wählen wir für b_i die Eins von R, so ändert sich $\sim$ nicht. Der Faktorring hat dann als s-Matrix die s-Matrix von R, bei der wir jede Spalte, die zu einem Element vom Grad 1 gehört, mit $\sqrt{-1}$ multiplizieren. Wir können den Vorgang im Fall $b_i = 1$ also auch als einen Basiswechsel in $R \otimes_{\mathbb{Z}} \mathbb{Z}[\sqrt{-1}]$ ansehen, bei dem ein $b \in B$ vom Grad 1 auf $\sqrt{-1} \cdot b$ abgebildet wird. Der neue Ring hat ganze Strukturkonstanten, welche demnach eine $\mathbb{Z}$-Algebra definieren, nämlich genau den obigen Faktorring. Er ist aber nicht isomorph zu R als $\mathbb{Z}$-Ring mit Basis.

Wenn wir Ideale definieren, die von Elementen der Form $b_1 \pm b_2$ mit $b_1, b_2 \in B$ erzeugt werden, hat die Wahl der Basis im Faktorring keinen Einfluß darauf, in welcher Isomorphieklasse von $\mathbb{Z}$-Ringen mit Basis der Faktorring liegt: Da der Faktorring ein freier $\mathbb{Z}$-Modul sein soll, dürfen wir nicht b_1 und b_2 in die Basis aufnehmen. Ob wir $b_1, -b_1, b_2$ oder $-b_2$ wählen, ändert den Ring um einen Isomorphismus von $\mathbb{Z}$-Ringen mit Basis.

Faktorringe eines Ringes mit Basis sind im allgemeinen keine $\mathbb{Z}$-Ringe mit Basis, weil es nicht immer eine passende Involution gibt. Schon wenn wir $R = Z_2$ wählen, erhalten wir mit der obigen Konstruktion den Ring $\mathbb{Z}[\sqrt{-1}]$, welcher kein $\mathbb{Z}$-Ring mit Basis ist. Diesen bekommen wir auch als Faktorring von Z_4 mit Basis $\{b_0, \ldots, b_3\}$ nach dem Ideal $\langle b_0 + b_2, b_1 + b_3 \rangle$. Wir werden übrigens später ein Beispiel dafür sehen, daß im Faktorring $\tau(ab)$ für $a \in B$ für mehrere $b \in B$ ungleich Null ist. Auch wenn wir bei der Involution Vorzeichen zulassen, sind Faktorringe im Allgemeinen keine $\mathbb{Z}$-Ringe mit Basis.

Beispiel 12. Es sei R der WZWV-Ring zu $p = 6$ mit 5 Basiselementen. Dieser ist C_2-graduiert und das 5-te Basiselement b_5 (Numerierung wie in 2.3.2) operiert auf der Basis durch Multiplikation wie eine Transposition. Der Faktorring (siehe oben) ist isomorph zum Ring G_4-4.

Statt einen Teilring R' von $R \otimes Z_4$ können wir auch einen Teilring von $R \otimes Z_{4n}$ wählen, so daß wir eine C_{4n}-Graduierung erhalten:

$$\underbrace{B_0 \cup B_1}_{0,1} \cup \underbrace{B_0' \cup B_1'}_{2,3} \cup \underbrace{B_0'' \cup B_1''}_{4,5} \cup \cdots \cup \underbrace{B_0'^{\cdots\prime} \cup B_1'^{\cdots\prime}}_{4n-2,4n-1}.$$

Auch hier können wir unter Umständen ein Element vom Grad $2n$ nutzen, um ein Ideal zu definieren, das wiederum einen interessanten Faktorring liefert.

Wir bezeichnen mit $R_{t(n,b)}$ den Faktorring von R' modulo dem Ideal $I = \langle 1 + b'^{\cdots\prime} \rangle$, wobei b ein Element vom Grad 0 und $b'^{\cdots\prime} \in B_0'^{\cdots\prime}$ (n Striche „$'$") das zu b gehörige Element im Grad $2n$ ist.

Beispiel 13. Es sei (R, B) der WZWV-Ring zu $p = 4$ mit 3 Basiselementen. Mit $n = 2$ und dem Ideal $\langle a + a \cdot b_3''' \mid a \in B' \rangle$ ergibt die Konstruktion einen Ring, der isomorph zum äußeren Quadrat eines zyklischen Ringes ist (5.1.4 mit $e = 4$ und $n = 2$). Dieser Ring ist außerdem ein Beispiel dafür, daß es $\mathbb{Z}$-Ringe mit Basis gibt, die nicht isomorph zu einem Ring mit Basis sind, weil kein Vorzeichenwechsel der Basiselemente einen Ring liefert, der nur positive Strukturkonstanten hat.

Beispiel 14. Es sei (R, B) der WZWV-Ring zu $p = 12$ mit 11 Basiselementen. Die obige Konstruktion mit $n = 2$ und dem letzten Basiselement liefert den Ring G_6-2.

Beispiel 15. Es sei (R, B) der affine Ring vom Typ $B_3^{(1)}$ und Level 2. Die obige Konstruktion mit $n = 1$ und dem letzten Basiselement liefert den Ring G_{24}-2 (R ist nicht immer ein WZWV-Ring.)

Wir können aber auch das Ideal etwas anders definieren. Anstatt a mit $-ab_i'$ zu identifizieren, ist es manchmal auch sinnvoll $I := \langle a - ab_i' \mid a \in B' \rangle$ zu betrachten. Dabei entstehen übrigens keine negativen Strukturkonstanten, siehe zum Vergleich Proposition 7.2.5. Diese Variante hat also nur den Effekt, daß die Involution $\sim$ verändert wird.

8.2.2 Basiswechsel

Es sei R ein $\mathbb{Z}$-Ring mit Basis. Wir können an der s-Matrix von R ablesen, ob R Charakterring einer endlichen Gruppe sein kann. Die s-Matrix ist dann nämlich die (transponierte) Charaktertafel. Es muss also eine Zeile geben, die nur ganze Einträge ungleich Null hat. Die Summe der Quadrate der Einträge in einer solchen Zeile ist die Ordnung der potentiellen Gruppe. In manchen Fällen ist diese Gruppe dadurch eindeutig festgelegt, weil wir wissen, daß sie genauso viele Konjugationsklassen haben muß, wie die s-Matrix Spalten hat.

Finden wir einen Teilring R' zu einer Teilmenge der Basis, der kein Charakterring sein kann, so ist nach Korollar 3.1.7 jeder Teilring R'', der R' enthält, d.h. $R' \subseteq R''$, auch kein Charakterring.

Einige Ringe entstehen aus einem Ring $R(D(G))$, zum Beispiel indem wir zu einem Faktorring übergehen, bei dem allerdings der Charakterring von G erhalten bleibt. Wenn wir wissen wollen, ob ein gegebener Ring in dieser Weise entsteht, so suchen wir deshalb unter den Teilringen nach Charakterringen.

Beispiel 16. Der Ring R zur Matrix G_{32}-12 hat 40 Basiselemente. Er ist C_6-graduiert über einem Teilring R' mit 10 Basiselementen. Die Basis zerlegt sich so in $10+6+6+6+6+6$ Elemente. An der s-Matrix von R' sehen wir, daß R' der Charakterring der 6. Gruppe der Ordnung 150 ist. Der Ring $Q := R(D(150,6))$ hat eine C_6-Graduierung der Form $110, 6, 6, 6, 6, 6$. Es gibt ein Ideal I in Q, so daß Q/I dem Ring R sehr ähnlich ist, nämlich (bei geeigneter Numerierung der Basis von Q)

$$I := \langle b_{28+i} - b_{78+i} \mid 1 \leq i \leq 25 \rangle.$$

Dieses Ideal wird in 8.2.3 genauer erklärt. Es muß noch ein Basiswechsel M auf R vorgenommen werden, bevor wir den gesuchten Ring erhalten:

$$M := \begin{pmatrix} \boxed{E_{10}} & & & & & \\ & \boxed{A} & & & 0 & \\ & & \boxed{A} & & & \\ & & & \boxed{A} & & \\ & 0 & & & \boxed{A} & \\ & & & & & \boxed{A} \end{pmatrix}, \quad A := \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix},$$

wobei E_{10} die 10×10 Einheitsmatrix ist.

Eine solche Konstruktion mit Basiswechsel ist natürlich nur dann sinnvoll, wenn die Basiswechselmatrix eine einfache Form hat. Ansonsten können wir nicht begründen, daß die Ringe eine ähnliche Struktur besitzen (die s-Matrix selbst ist auch ein Basiswechsel).

Einen Basiswechsel können wir durch zwei Methoden erraten. Eine Möglichkeit ist, die s-Matrizen s_1, s_2 der beiden Ringe zu berechnen. Dann ist (falls wir die Spalten und Zeilen richtig sortieren) $s_1^{-1}s_2$ ein „schöner“ Basiswechsel. Bei dem vorherigen Beispiel ist das aber nicht möglich, weil Q/I zu groß ist, um die s-Matrix zu berechnen.

Die zweite Möglichkeit ergibt sich aus folgendem Lemma:

Lemma 8.2.1. *Es seien $(R, \{b_1, \ldots, b_n\})$ ein $\mathbb{Z}$-Ring mit Basis mit den Strukturkonstanten $B_{i,j}^k$ und E eine freie endlich erzeugte $\mathbb{Z}$-Algebra mit Basis $\{a_1, \ldots, a_n\}$, $a_1 = 1$ und den Strukturkonstanten $A_{i,j}^k$. Ist $M^T = M = (m_{i,j}) \in \mathbb{C}^n$ ein Basiswechsel von R nach E, d.h. ist*

$$a_i = \sum_{j=1}^{n} m_{ji} b_j, \quad m_{ij} = m_{ji},$$

so gelten

$$A_i = MD_iM^{-1}, \quad (A_{i\bar{j}}^1)_{i,j} = M^2,$$

wobei $A_i := (A_{ij}^k)_{j,k}$, $B_i := (B_{ij}^k)_{j,k}$, $D_i := \sum_j B_j m_{ji}$ *und* $\sim$ *in kanonischer Weise auf* E *definiert wird.*

Beweis. Wir haben $a_i a_k = \sum_j A_{ik}^j a_j$. Setzen wir $a_i = \sum_{j=1}^n m_{ji} b_j$ in diese Formel ein, so erhalten wir

$$(*) \qquad \sum_\nu A_{ik}^\nu m_{j\nu} = \sum_\mu \sum_\nu m_{\mu i} m_{\nu k} B_{\mu,\nu}^j,$$

woraus die linke Gleichung folgt. Die rechte Gleichung ergibt sich aus dem Fall $j = 1$:
Es ist $B_{ij}^1 = \delta_{i,\tilde{j}}$. Außerdem ist

$$\sum_j m_{j\tilde{i}} b_j = a_{\tilde{i}} = \tilde{a}_i = \sum_j m_{ji} \tilde{b}_j = \sum_j m_{\tilde{j}i} b_j,$$

d.h. $m_{j\tilde{i}} = m_{\tilde{j}i}$. Die Gleichung $(*)$ mit $j = 1$ und $\tilde{k}$ statt k lautet $A_{i\tilde{k}}^1 = \sum_\mu m_{\mu i} m_{\tilde{\mu}\tilde{k}} = \sum_\mu m_{\mu i} m_{\mu k}$. □

Wenn wir raten, wie $\sim$ sich auf Q/I verhält (das ist zum Teil durch Q gegeben), und nur Matrizen M mit $M = M^T$ suchen, so kennen wir demnach zumindest M^2.

8.2.3 G_{25}-7, G_8-5 und G_{32}-12

Für die Ringe G_8-5 und G_{32}-12 gibt es eine gemeinsame Konstruktion (vergleiche Beispiel 16 in 8.2.2). Höchstwahrscheinlich kann man diese noch verallgemeinern, weil der Ring G_{26}-7 eine sehr ähnliche Struktur aufweist und dennoch nicht so wie im folgenden beschrieben werden kann.

Es sei G eine endliche Gruppe und $N \trianglelefteq G$ ein Normalteiler. In $R(D(G))$ betrachten wir folgendes Ideal:

$$I := \langle (\bar{g}, \chi) - (\bar{g}, \chi') \mid g \in G,\ \chi, \chi' \in \mathrm{Irr}(G_G(g)),\ \ \chi_{|_{N \cap C_G(g)}} \neq 1,\ \ \chi'_{|_{N \cap C_G(g)}} \neq 1 \rangle.$$

Es sei B die Teilmenge des Faktorrings $R(D(G))/I$

$$B := \{\overline{(\bar{g}, \chi)} \in R(D(G))/I \mid (\bar{g}, \chi) \in \mathrm{Irr}(D(G)),\ \ \chi_{|_{N \cap C_G(g)}} = 1\}.$$

Weiterhin sei für $g \in G$, $\chi \in \mathrm{Irr}(C_G(g))$:

$$d(\bar{g}, \chi) := \left(\sum_{\chi \neq \chi' \in \mathrm{Irr}(C_G(g))} n_{\bar{g}}^{-1} (\bar{g}, \chi') \right) - \frac{n_{\bar{g}} - 1}{n_{\bar{g}}} (\bar{g}, \chi),$$

wobei $n_{\bar{g}} := |\operatorname{Irr}(C_G(g))| - 1$. Bei passenden G und N ist $(R(D(G))/I, B')$ mit

$$B' := \{\overline{(\bar{g}, \chi)} \in B \mid \bar{g} \cap N \neq \emptyset\} \cup \{\overline{d(\bar{g}, \chi)} \in B \mid \bar{g} \cap N = \emptyset\}$$

ein $\mathbb{Z}$-Ring mit Basis B' (B' ist eine Basis, weil die lineare Fortsetzung von d auf $R(D(G))$ invertierbar ist: Sie beschreibt den Basiswechsel aus Beispiel 16).

Mit $G = (C_3 \times C_3) \rtimes C_4$ (genauer: die 9. Gruppe der Ordnung 36 in der Numerierung von „small groups“) und dem Normalteiler N, der 9 Elemente hat, gilt $R' \cong G_8$-5.
Mit $G = (C_5 \times C_5) \rtimes C_6$ (genauer: die 6. Gruppe der Ordnung 150 in der Numerierung von „small groups“) und dem Normalteiler N, der 25 Elemente hat, gilt $R' \cong G_{32}$-12.

Das Ideal

$$I' := \langle (\bar{g}, \chi) - \sum_{\chi' \in \mathrm{Irr}(C_G(g)),\ \chi'_{|N \cap C_G(g)} = 1} (\bar{g}, \chi') \mid (\bar{g}, \chi) \in \mathrm{Irr}(D(G)),\ \ \chi_{|N \cap C_G(g)} \neq 1 \rangle$$

ist in den beiden Beispielen gleich I, hat aber den Vorteil, daß es auch noch in einem weiteren Fall einen unserer Ringe liefert: $G = A_4$, $N = C_2 \times C_2 \trianglelefteq G$ liefern mit I' (und der Basis B') den Ring G_{25}-7. Dieser hat übrigens eine große Ähnlichkeit mit dem Ring $A^{(1)}_{2,3}$.

Wir schreiben $Q(G)$ für die Konstruktion mit dem Ideal I'. Diese Bezeichnung legt den Ring nicht eindeutig fest. Sie besagt nur, daß der Ring auf diese Weise erhalten werden kann.

8.2.4 G_{27}-2

Es sei $R' := C^{(1)}_{2,2}$. Dieser hat als Teilring den Charakterring von D_5, über dem er C_2-graduiert ist. Eine Basis teilt sich demnach auf:

$$B' := \{\underbrace{b_0, \ldots, b_3}_{0}, \underbrace{b_4, b_5}_{1}\}.$$

In $R'' := R' \otimes Z_6$ mit einer passenden Basis $B'' = \{b_{i,j} \mid 0 \leq i, j < 6\}$ liegt folgende $(C_2 \times C_6)$-Graduierung vor:

$$B'' = \bigcup_{i=0}^{5} \{\underbrace{b_{i,0}, \ldots, b_{i,3}}_{2i}, \underbrace{b_{i,4}, b_{i,5}}_{2i+1}\}.$$

Der Teilring R von R'' zur Teilmenge

$$B := \{b_{2i,k}, b_{2i+1,l} \mid 0 \leq i < 6,\ 0 \leq k < 4,\ 4 \leq l < 6\}$$

ist zum Ring G_{27}-2 als $\mathbb{Z}$-Ring mit Basis isomorph. Es sei noch angemerkt, wie die Teilringe von R aussehen. Sie könnten Auskunft darüber geben, wie R mit einer der anderen Konstruktionen erreicht werden könnte. Die (nicht-trivialen) Teilringe sind:

$$Z_2, Z_3, Z_6, R(D_5), C^{(1)}_{2,2} \text{ und } R(30, 2),$$

wobei $R(30,2)$ der Charakterring eines semidirekten Produktes der Form $C_3 \rtimes D_5$ ist. Der Ring R ist C_2-graduiert über dem Teilring $R(30,2)$. Wir bezeichnen den Ring R in den nächsten Abschnitten mit T_{27-2}.

8.3 T-Matrizen

Die Abschnitte aus diesem Kapitel ergeben Konstruktionen für Ringe, die zu Fourier-Matrizen gehören. Es stellt sich hierbei die Frage, ob die T-Matrizen (bei den komplexen Spiegelungsgruppen enthalten diese die Frobenius-Eigenwerte) nebenher mitkonstruiert werden.

Die Überlegungen dieser Arbeit konzentrieren sich alle auf die Struktur der Fusionsalgebren bis auf Isomorphie von $\mathbb{Z}$-Ringen mit Basis. Hier muss noch einmal betont werden, daß die Isomorphieklasse des Ringes alleine nicht genug Informationen liefert, um eine eindeutige S-Matrix und schon gar nicht eine T-Matrix zu bestimmen. Eine gründliche Untersuchung der T-Matrizen (etwa ihr Verhalten beim Übergang zu Faktorringen) würde deshalb den Rahmen dieser Arbeit sprengen. Einige Aspekte sollten wir dennoch anmerken.

Die S-Matrix aus Kapitel 2 ist durch die Bedingung, daß die Einträge in der ersten Spalte positiv reell sind, bis auf Permutation der Zeilen eindeutig bestimmt. Die Reihenfolge der Spalten ist durch die Reihenfolge der Basiselemente gegeben.

Ist durch die Definition der S-Matrix aus irgendeinem Grund schon eine natürliche Bijektion zwischen den Zeilen und Spalten gegeben (etwa wie bei den irreduziblen Darstellungen des Darstellungsrings des Quantendoppels), so ist zumindest für die S-Matrix eine kanonische Wahl gegeben. Ein Problem ist, daß diese Matrix mit positiven reellen Einträgen in der ersten Spalte in vielen Beispielen nicht für ein Fusionsdatum oder modulares Datum in Frage kommt, weil sie nicht immer symmetrisch ist.

Je nachdem, ob wir eine Matrix T suchen, so daß S, T ein modulares Datum oder ein Fusionsdatum bilden, ergeben sich verschiedene Gleichungssysteme, die mögliche T-Matrizen als Lösungen besitzen. Wir konzentrieren uns auf die modularen Daten, weil die Fusionsdaten aus anderen Gründen für unsere Beispiele weniger geeignet sind (siehe 2.3). Beim modularen Datum müssen gelten:

$$T \text{ ist diagonal}, \quad S\bar{S}^T = T\bar{T}^T = I, \quad (ST)^3 = S^2,$$

wobei S^2 im Allgemeinen nicht die Einheitsmatrix sondern eine Permutationsmatrix der Ordnung 2 ist.

Beispiel 17. Es sei S die Matrix zum äußeren Quadrat des Gruppenrings der zyklischen Gruppe C_4 (siehe Beispiel 8 in 5.1.2). Die Matrix S ist symmetrisch. Das Quadrat S^2 ist aber keine Permutationsmatrix, sondern eine monomiale Matrix mit Einträgen ± 1. Das

liegt daran, daß wir die Substitution aus Satz 5.1.5 nicht durchführen, weil die Matrix sonst nicht mehr symmetrisch ist. Außerdem sind die Einträge $\{S_{i,1} \mid 1 \leq i \leq 6\}$ nicht positive reelle Zahlen, anders als es vom Fusionsdatum verlangt wird.
Das Gleichungssystem $(ST)^3 = I$, $T_{1,1} = 1$ hat zwei Diagonalmatrizen T, T' als Lösungen (es läßt sich leicht mit dem Computer lösen). Die Matrizen S und T oder T' bilden dann weder ein Fusionsdatum noch ein modulares Datum.
Bei den komplexen Spiegelungsgruppen taucht diese Matrix S sehr oft auf, allerdings manchmal mit T und manchmal mit T' als T-Matrix.
Man beachte wieder, daß S nicht die S-Matrix des zugehörigen Ringes ist (diese entsteht aus S, indem die Einträge in der ersten Spalte durch Normierung der Zeilen positiv reell gemacht werden). Die S-Matrix des zugehörigen $\mathbb{Z}$-Ringes mit Basis ist nicht symmetrisch und ist damit kein besserer Kandidat für ein Datum, das dem Ring zugeordnet werden könnte.

Nach Beispiel 17 kann folgendes passieren: Zu zwei Paaren (S,T), (S',T') sind die $\mathbb{Z}$-Ringe mit Basis zu S und S' isomorph, aber der Isomorphismus bildet T nicht auf T' ab.
Einen Fall können wir leicht erkennen und kennzeichnen: Wenn R der Ring zu (S,T) ist, so schreiben wir $\overline{R}$ für den Ring der komplex konjugierten Matrizen $(\bar{S},\bar{T})$. (Die Ringe R und $\overline{R}$ sind gleich, aber durch die unterschiedliche Notation ist noch die Information über T enthalten.)

Die Matrizen der ungetwisteten komplexen Spiegelungsgruppen haben dieselben Eigenschaften wie Beispiel 17. Sie haben in der ersten Spalte nur Einträge ungleich Null, sind symmetrisch und definieren zusammen mit ihrer T-Matrix eine Darstellung von $\mathrm{SL}_2(\mathbb{Z})$. Außerdem sind die Quadrate S^2 im Allgemeinen keine Permutationsmatrizen.

8.4 Beschreibungen

8.4.1 Zusammenfassung

In der folgenden Tabelle wollen wir die „schwierigen“ Ringe zusammenfassen. Das sind diejenigen, die wir durch Anwendung irgendwelcher Operationen erhalten. Die zweite Spalte besagt, ob es negative Strukturkonstanten gibt („$-$“), oder ob es einen Isomorphismus gibt, so daß alle Strukturkonstanten nicht negativ sind („$+$“). In der vierten Spalte steht ein zum Teilring vom Grad 0 isomorpher Ring. Man beachte, daß z.B. bei der Graduierung von G_{27}-6 die Zahlen $4,4,4,4$ stehen, und daß der Ring $C_2 \times C_2$- und nicht C_4-graduiert ist. Die letzte Spalte beschreibt den Ring in der hier eingeführten Notation.

Ring	$\pm$	Graduierung	Grad 0	isomorph zu
G_4-4	$-$	3,2	$R(S_3)$	$(A^{(1)}_{1,4})_{t(b_5,1)}$
G_6-2	$-$	6,5,6,5	$\leq A^{(1)}_{1,10}$	$(A^{(1)}_{1,10})_{t(b_{11},2)}$
G_8-5	$+$	6,4,4,4	$R((C_3 \times C_3) \rtimes C_4)$	$Q((C_3 \times C_3) \rtimes C_4)$
G_8-2, ...	$-$	4,2	$R(C_4)$	$\Lambda(4,2)$
G_{14}-2	?	10,8,10,8,10,8	?	?
G_{14}-5	$-$	5,4	$R(D_4)$	$(A^{(1)}_{1,2} \otimes A^{(1)}_{1,2})_{t(-b_3 \otimes b_3,1)}$
G_{23}-2, G_{23}-6, ...	$+$	4	-	Dih(5)
G_{24}-2, G_{24}-6	$-$	5,2	$R(D_7)$	$(B^{(1)}_{3,2})_{t(b_7,1)}$
G_{25}-7	$+$	4,3,3	$R(A_4)$	$Q(A_4)$
G_{26}-7	?	13,6,9,6,9,6	$R((C_3 \times C_9) \rtimes C_6)$	?
G_{27}-2, G_{27}-10	$+$	4,2,4,2,4,2	$R(D_5)$	T_{27-2}
G_{27}-6	$+$	4,4,4,4	Dih(5)	Dih(5) $\otimes Z_2 \otimes Z_2$
G_{32}-12	$+$	10,6,6,6,6,6	$R((C_5 \times C_5) \rtimes C_6)$	$Q((C_5 \times C_5) \rtimes C_6))$

8.4.2 Tabellen

Hier ist eine Übersicht über die Ringe der Fourier-Matrizen der Familien der spetsiellen exzeptionellen Spiegelungsgruppen (bis auf die Weylgruppen $G_{28} = F_4$, $G_{35} = E_6$, $G_{36} = E_7$, $G_{37} = E_8$, welche in [15] von Lusztig beschrieben wurden).

Die Familien zu G_{30} sind in CHEVIE anders sortiert. Welche Familie jeweils gemeint ist, kann man an den ersten drei Spalten ablesen.

Familien für G_4.

$a(\mathcal{F})$	$A(\mathcal{F})$	$\|\mathcal{F}\|$	R
0	0	1	1
1	5	3	Z_3
2	6	1	1
4	8	5	$(A^{(1)}_{1,4})_{t(b_5,1)}$

Familien für G_6.

$a(\mathcal{F})$	$A(\mathcal{F})$	$\lvert\mathcal{F}\rvert$	R
0	0	1	1
1	11	22	$(A^{(1)}_{1,10})_{t(b_{11},2)}$
4	12	1	1
5	13	4	Z_4
10	14	3	Z_3

Familien für G_8.

$a(\mathcal{F})$	$A(\mathcal{F})$	$\lvert\mathcal{F}\rvert$	R
0	0	1	1
1	11	6	$\Lambda(4,2)$
2	14	6	$\Lambda(4,2)$
3	15	4	Z_4
6	18	18	$Q((C_3 \times C_3) \rtimes C_4)$

Familien für G_{14}.

$a(\mathcal{F})$	$A(\mathcal{F})$	$\lvert\mathcal{F}\rvert$	R
0	0	1	1
1	23	54	?
5	25	3	Z_3
6	26	9	Z_9
9	27	9	$(A^{(1)}_{1,2} \otimes A^{(1)}_{1,2})_{t(-b_3 \otimes b_3,1)}$
20	28	3	Z_3

Familien für G_{23}.

$a(\mathcal{F})$	$A(\mathcal{F})$	$\lvert\mathcal{F}\rvert$	R
0	0	1	1
1	9	4	Dih(5)
2	10	1	1
3	12	4	$Z_2 \otimes Z_2$
5	13	1	1
6	14	4	Dih(5)
15	15	1	1

Familien für G_{24}.

$a(\mathcal{F})$	$A(\mathcal{F})$	$\|\mathcal{F}\|$	R
0	0	1	1
1	13	7	$(B^{(1)}_{3,2})_{t(b_7,1)}$
3	15	1	1
4	17	4	$Z_2 \otimes Z_2$
6	18	1	1
8	20	7	$\overline{(B^{(1)}_{3,2})_{t(b_7,1)}}$
21	21	1	1

Familien für G_{25}.

$a(\mathcal{F})$	$A(\mathcal{F})$	$\|\mathcal{F}\|$	R
0	0	1	1
1	11	3	Z_3
2	16	9	$Z_3 \otimes Z_3$
4	20	15	$\bar{Z}_3 \otimes (A^{(1)}_{1,4})_{t(b_5,1)}$
6	21	3	Z_3
8	22	3	Z_3
12	24	10	$Q(A_4)$

Familien für G_{26}.

$a(\mathcal{F})$	$A(\mathcal{F})$	$\|\mathcal{F}\|$	R
0	0	1	1
1	17	9	$Z_3 \otimes Z_3$
2	22	9	$Z_3 \otimes Z_3$
3	24	4	$Z_2 \otimes Z_2$
4	26	12	$Z_3 \otimes Z_2 \otimes Z_2$
5	25	3	Z_3
6	30	49	?
11	31	9	$Z_3 \otimes Z_3$
16	32	3	Z_3
21	33	5	$(A^{(1)}_{1,4})_{t(b_5,1)}$

Familien für G_{27}.

$a(\mathcal{F})$	$A(\mathcal{F})$	$\lvert\mathcal{F}\rvert$	R
0	0	1	1
1	29	18	T_{27-2}
3	33	4	$Z_2 \otimes Z_2$
4	36	9	$\bar{Z}_9$
5	37	3	$\bar{Z}_3$
6	39	16	$\mathrm{Dih}(5) \otimes Z_2 \otimes Z_2$
8	40	3	Z_3
9	41	9	Z_9
12	42	4	$Z_2 \otimes Z_2$
16	44	18	$\overline{T_{27-2}}$
45	45	1	1

Familien für G_{29}.

$a(\mathcal{F})$	$A(\mathcal{F})$	$\lvert\mathcal{F}\rvert$	R
0	0	1	1
1	19	6	$\Lambda(4,2)$
2	22	1	1
3	27	4	$\bar{Z}_4$
4	28	4	$Z_2 \otimes Z_2$
4	28	1	1
5	31	6	$\overline{\Lambda(4,2)}$
6	34	22	$R(D(20,3))$[1]
9	35	6	$\Lambda(4,2)$
12	36	1	1
12	36	4	$Z_2 \otimes Z_2$
13	37	4	Z_4
18	38	1	1
21	39	6	$\overline{\Lambda(4,2)}$
40	40	1	1

[1] $R(D(C_5 \rtimes C_4))$

Familien für G_{30}.

$a(\mathcal{F})$	$A(\mathcal{F})$	$\lvert\mathcal{F}\rvert$	R
0	0	1	1
1	29	4	Dih(5)
2	38	4	Dih(5)
3	42	4	$Z_2 \otimes Z_2$
4	44	1	1
5	45	1	1
6	54	74	?
15	55	1	1
16	56	1	1
18	57	4	$Z_2 \otimes Z_2$
22	58	4	Dih(5)
31	59	4	Dih(5)
60	60	1	1

Familien für G_{32}.

$a(\mathcal{F})$	$A(\mathcal{F})$	$\lvert\mathcal{F}\rvert$	R
0	0	1	1
1	29	3	Z_3
2	46	9	$Z_3 \otimes Z_3$
3	51	3	Z_3
4	56	15	$\bar{Z}_3 \otimes (A^{(1)}_{1,4})_{t(b_5,1)}$
5	61	15	$Z_3 \otimes (A^{(1)}_{1,4})_{t(b_5,1)}$
6	66	42	$R(D(\mathrm{SL}_2(\mathbb{F}_3)))$
8	67	12	$Z_3 \otimes Z_2 \otimes Z_2$
9	69	9	$Z_3 \otimes Z_3$
10	70	9	Z_9
12	72	45	$(A^{(1)}_{1,4})_{t(b_5,1)} \otimes Z_3 \otimes Z_3$
15	75	40	$Q((C_5 \times C_5) \rtimes C_6))$
20	76	15	$\bar{Z}_3 \otimes (A^{(1)}_{1,4})_{t(b_5,1)}$
25	77	9	$Z_3 \otimes Z_3$
30	78	5	$(A^{(1)}_{1,4})_{t(b_5,1)}$
40	80	15	$Z_3 \otimes \overline{(A^{(1)}_{1,4})_{t(b_5,1)}}$

Familien für G_{33}.

$a(\mathcal{F})$	$A(\mathcal{F})$	$\lvert\mathcal{F}\rvert$	R
0	0	1	1
1	17	3	$\bar{Z}_3$
2	22	1	1
3	27	4	$Z_2 \otimes Z_2$
4	32	15	$Z_3 \otimes \overline{(A_{1,4}^{(1)})_{t(b_5,1)}}$
6	34	1	1
7	35	1	1
7	35	3	$\bar{Z}_3$
8	37	4	$Z_2 \otimes Z_2$
9	33	1	1
10	38	3	Z_3
11	39	1	1
10	38	1	1
12	36	1	1
13	41	15	$\bar{Z}_3 \otimes (A_{1,4}^{(1)})_{t(b_5,1)}$
18	42	4	$Z_2 \otimes Z_2$
23	43	1	1
28	44	3	Z_3
45	45	1	1

Familien für G_{34}.

$a(\mathcal{F})$	$A(\mathcal{F})$	$\lvert\mathcal{F}\rvert$	R
0	0	1	1
1	41	3	$\bar{Z}_3$
2	58	3	$\bar{Z}_3$
3	69	4	$Z_2 \otimes Z_2$
4	80	15	$Z_3 \otimes \overline{(A_{1,4}^{(1)})_{t(b_5,1)}}$
5	85	9	$Z_3 \otimes Z_3$
6	90	9	$Z_3 \otimes Z_3$
7	95	15	$Z_3 \otimes \overline{(A_{1,4}^{(1)})_{t(b_5,1)}}$
8	97	12	$\bar{Z}_3 \otimes Z_2 \otimes Z_2$
9	81	1	1
9	99	4	$Z_2 \otimes Z_2$
10	98	9	$Z_3 \otimes Z_3$
10	102	9	$\bar{Z}_9$
11	103	3	$\bar{Z}_3$
11	103	9	$Z_3 \otimes Z_3$
12	96	1	1
12	105	4	$Z_2 \otimes Z_2$
13	107	36	$Z_6 \otimes Z_6$
14	106	3	Z_3
15	111	44	$R(D(42,1))$[2]
18	108	4	$Z_2 \otimes Z_2$
20	112	3	$\bar{Z}_3$
19	113	36	$Z_6 \otimes Z_6$
21	114	4	$Z_2 \otimes Z_2$
30	114	1	1
23	115	9	$Z_3 \otimes Z_3$
23	115	3	Z_3
24	116	9	Z_9
28	116	9	$Z_3 \otimes Z_3$
27	117	4	$Z_2 \otimes Z_2$
45	117	1	1
29	118	12	$Z_3 \otimes Z_2 \otimes Z_2$
31	119	15	$\bar{Z}_3 \otimes (A_{1,4}^{(1)})_{t(b_5,1)}$
36	120	9	$Z_3 \otimes Z_3$
41	121	9	$Z_3 \otimes Z_3$
46	122	15	$\bar{Z}_3 \otimes (A_{1,4}^{(1)})_{t(b_5,1)}$
57	123	4	$Z_2 \otimes Z_2$
68	124	3	Z_3
85	125	3	Z_3
126	126	1	1

[2] $R(D(C_7 \rtimes C_6)) = R(D(C_7 \times_f C_6))$

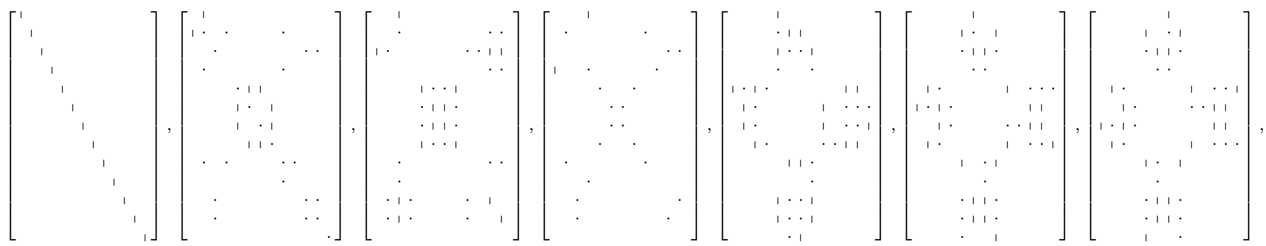
8.5 Die Fouriermatrix zu ${}^2F_4$

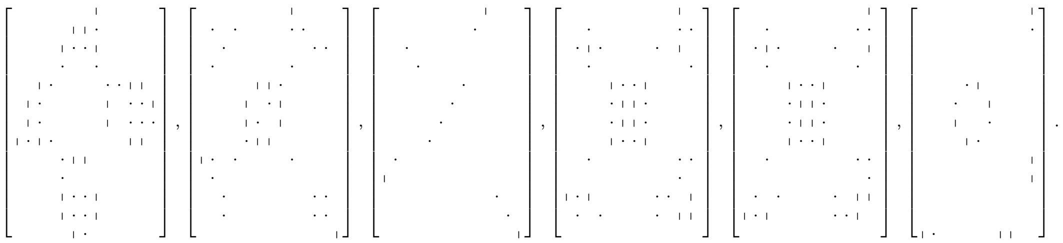
8.5.1 Untersuchung des zugehörigen Ringes

In [12] wird für die Ree Gruppe ${}^2F_4(q^2)$ eine bis auf Multiplikation der Zeilen mit Einheitswurzeln eindeutig bestimmte Fourier-Matrix (die transponierte S-Matrix) berechnet:

$$S^T = \frac{1}{12}\begin{pmatrix}
3 & 3 & 6 & 1 & 1 & 2 & 3 & 3 & 3 & 3 & 4 & 4 & 4\\
3 & 3 & 6 & -3 & -3 & -6 & -3 & -3 & -3 & -3 & 0 & 0 & 0\\
0 & 0 & 0 & 4 & 4 & -4 & 0 & 0 & 0 & 0 & 4 & 4 & -8\\
-6 & -6 & 0 & -2 & -2 & -4 & 0 & 0 & 0 & 0 & 4 & 4 & 4\\
3\sqrt{2} & -3\sqrt{2} & 0 & -3\sqrt{2} & 3\sqrt{2} & 0 & 3\sqrt{2} & 3\sqrt{2} & -3\sqrt{2} & -3\sqrt{2} & 0 & 0 & 0\\
3\sqrt{2} & -3\sqrt{2} & 0 & 3\sqrt{2} & -3\sqrt{2} & 0 & -3\sqrt{2} & 3\sqrt{2} & 3\sqrt{2} & -3\sqrt{2} & 0 & 0 & 0\\
3\sqrt{2} & -3\sqrt{2} & 0 & 3\sqrt{2} & -3\sqrt{2} & 0 & 3\sqrt{2} & -3\sqrt{2} & -3\sqrt{2} & 3\sqrt{2} & 0 & 0 & 0\\
3\sqrt{2} & -3\sqrt{2} & 0 & -3\sqrt{2} & 3\sqrt{2} & 0 & -3\sqrt{2} & -3\sqrt{2} & 3\sqrt{2} & 3\sqrt{2} & 0 & 0 & 0\\
3 & 3 & -6 & -3 & -3 & -6 & 3 & 3 & 3 & 3 & 0 & 0 & 0\\
-3 & -3 & 6 & -1 & -1 & -2 & 3 & 3 & 3 & 3 & -4 & -4 & -4\\
0 & 0 & 0 & 4 & 4 & -4 & 0 & 0 & 0 & 0 & 4 & -8 & 4\\
0 & 0 & 0 & 4 & 4 & -4 & 0 & 0 & 0 & 0 & -8 & 4 & 4\\
0 & 0 & 0 & 0 & 0 & 0 & 6 & -6 & 6 & -6 & 0 & 0 & 0
\end{pmatrix}.$$

Diese definiert den $\mathbb{Z}$-Ring mit Basis R, der die folgende Multiplikationstafel hat. Man beachte, daß es negative Strukturkonstanten gibt („·“ steht für -1, „ı“ für 1).





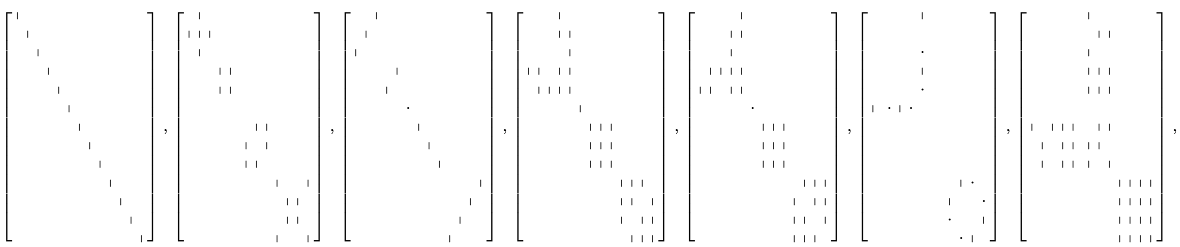
Es gibt für diesen Ring nach wie vor keine Interpretation als Grothendieck-Ring einer Tensorkategorie. Von einer modularen Tensorkategorie kann er nicht herkommen, da er negative Strukturkonstanten hat. Es ist aber denkbar, daß R ein Faktorring eines solchen Grothendieck-Rings ist. Mit den Techniken aus den letzten Kapiteln können wir eine Ähnlichkeit zum Darstellungsring des Quantendoppels der symmetrischen Gruppe S_4 nachweisen, was auch erwartet wird, da dies der Ring ist, den Lusztig zu der Fourier-Matrix im Typ F_4 erhalten hat.

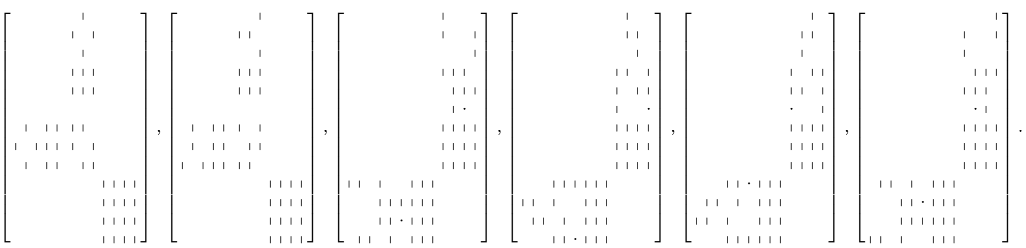
Wir erkennen sofort, daß R eine C_2-Graduierung besitzt. Die Teilringe zu Teilmengen der

Basis sind:

$$\begin{aligned}
&\{1\},\\
&\{1,10\},\\
&\{1,4,10\},\\
&\{1,2,4,9,10\},\\
&\{1,2,4,9,10,13\},\\
&\{1,2,3,4,9,10,11,12\},\\
&\{1,2,3,4,9,10,11,12,13\},\\
&\{1,2,3,4,5,6,7,8,9,10,11,12,13\}.
\end{aligned}$$

Der ganze Ring ist über dem vorletzten C_2-graduiert. Der vorletzte ist über den vorherigen C_2-graduiert. Der Teilring $\{1,2,4,9,10\}$ ist isomorph zum Charakterring der Gruppe S_4. Es ist zunächst sinnvoll, die Basiselemente anders zu sortieren, um die Graduierungen hervorzuheben. Außerdem können wir durch Vorzeichenwechsel erreichen (Multiplikationen mit Einheitswurzeln sind erlaubt), daß der Teilring zu $\{1,2,3,4,9,10,11,12\}$ positive Strukturkonstanten hat. Danach sieht die Multiplikationstafel folgendermaßen aus:





Es bezeichne jetzt (R,B) diesen veränderten Ring. Untersuchen wir nun den Darstellungsring $Q := R(D(S_4))$ des Quantendoppels der symmetrischen Gruppe S_4. Die Konjugationsklassen von S_4 werden wie in [4] mit $1, g_2', g_2, g_3, g_4$ bezeichnet. Die Zentralisatoren sind dann $S_4, D_4, C_2\times C_2, C_3, C_4$. Es seien $b_1,\dots,b_{21}$ die Paare (g,χ), wobei $b_1,\dots,b_5$ die zu $(1,*)$ gehörigen Basiselemente, $b_6,\dots,b_{10}$ die zu $(g_2',*)$ gehörigen Basiselemente usw. sind.

Dann ergeben sich bezüglich dieser Numerierung (bis auf die Reihenfolge der Charaktere) folgende Teilringe zu Teilmengen der Basis:

$$\begin{array}{l}\{1\},\\ \{1,2\},\\ \{1,2,3\},\\ \{1,2,3,4,5\},\\ \{1,2,3,7,9\},\\ \{1,2,3,6,8\},\\ \{1,2,3,4,5,6,7,8,9,10\},\\ \{1,2,3,4,5,6,7,8,9,10,15,16,17\},\\ \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21\}.\end{array}$$

Dieser Ring ist über dem Teilring mit 13 Elementen C_2-graduiert. Der Ring zu $\{1,2,3,4,5\}$ ist der Charakterring der S_4. Der Teilring mit 13 Basiselementen hat in der Tat eine große Ähnlichkeit zu R. Wir sehen aber schon alleine an der Graduierung oder an der Teilringstruktur, daß er nicht zu R isomorph ist.

Die s-Matrix von Q hat übrigens nur ganze Einträge, was bei der s-Matrix von R nicht der Fall ist (dort finden wir mehrmals $\sqrt{2}$). Damit können wir auch ausschließen, daß R ein Faktorring von Q ist, bei dem wir Basiselemente identifizieren und als Basis ein Vertretersystem aus Basiselementen von Q wählen:
In der s-Matrix sind die Zeilen die eindimensionalen Darstellungen des Ringes. Die Einträge sind demnach Lösungen eines quadratischen Gleichungssystems. Die Gleichungen der s-Matrix des Faktorrings sind dieselben mit zusätzlichen Gleichungen. Deswegen verlassen die Lösungen beim Übergang zum Faktorring die Körpererweiterung nicht.

Die Basiselemente von Q parametrisieren die Charaktere der größten Familie unipotenter Charaktere von F_4. In Charakteristik 2 hat F_4 einen Automorphismus, der die unipotenten Charaktere, die den Basiselementen $\{b_1, b_3, b_2, b_7, b_9, b_{10}, b_{15}, b_{16}, b_{17}, b_{11}, b_{19}, b_{21}, b_{14}\}$ von Q entsprechen, invariant läßt. (Diese Teilmenge der Basis liefert nicht einen Teilring von Q!) Es sei τ das 13-Tupel

$$\tau := (1,3,2,7,9,10,15,16,17,11,19,21,14).$$

Dann stellen wir fest:

Bemerkung 8.5.1. *Es bezeichnen N_{**}^{*}, $\tilde{N}_{**}^{*}$ die Strukturkonstanten von R bzw. Q. Dann gilt*

$$N_{i,j}^{k} \equiv \tilde{N}_{\tau(i),\tau(j)}^{\tau(k)} \pmod{2}.$$

Eine andere Konstruktion liefert einen Ring, der nach einem einfachen Basiswechsel gleich R ist:
Es sei I das Hauptideal, das von $1-b_2$ erzeugt wird. Die Numerierung sei hier so gewählt, daß b_2 die irreduzible Darstellung $(1,\sigma)$ ist, wobei σ der Signumcharakter von S_4 ist. Das

Element b_2 hat Quadrat 1 und operiert durch Multiplikation auf den restlichen Basiselementen bijektiv. Der Faktorring $E := Q/I$ ist torsionsfrei (siehe Proposition 7.2.5) vom Rang 13. In E wählen wir die Basis

$$B' := \{b_1, b_3, b_4, b_6, b_7, b_{10}, b_{15}, b_{16}, b_{17}, b_{11}, b_{12}, b_{18}, b_{19}\}.$$

Es sei

$$A := \begin{pmatrix}
1 & \frac{1}{2} & -\frac{1}{2} & & & & & & & & & & \\
0 & -\frac{1}{2} & \frac{1}{2} & & & & & & & & & & \\
0 & \frac{1}{2} & \frac{1}{2} & & & & & & & & & & \\
 & & & \frac{1}{2} & \frac{1}{2} & & & & & 0 & & & \\
 & & & \frac{1}{2} & -\frac{1}{2} & & & & & & & & \\
 & & & & & \frac{1}{2} & & & & & & & \\
 & & & & & & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & & & & \\
 & & & & & & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & & & & \\
 & & & & & & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & & & & \\
 & & 0 & & & & & & & \frac{1}{\sqrt{2}} & & & \\
 & & & & & & & & & & \frac{1}{\sqrt{2}} & & \\
 & & & & & & & & & & & \frac{1}{\sqrt{2}} & \\
 & & & & & & & & & & & & \frac{1}{\sqrt{2}}
\end{pmatrix}.$$

Dann ist $A : R' \otimes_{\mathbb{Z}} \mathbb{C} \to E \otimes_{\mathbb{Z}} \mathbb{C}$ ein Ringisomorphismus, und R' ist als $\mathbb{Z}$-Ring mit Basis isomorph zu R (Permutation der Basiselemente). Oder anders formuliert: E ist mit der Basis $1, \frac{1}{2}(b_1 - b_3 + b_4), \frac{1}{2}(-b_1 + b_3 + b_4), \frac{1}{2}(b_6 + b_7), \ldots$ isomorph zu R. Da aber die Einträge von A und A^{-1} nicht ganzzahlig sind, sind diese Ringe auch nicht als $\mathbb{Z}$-Algebren isomorph.

8.5.2 $^2G_2$ und Verallgemeinerung

Den Ring der Fourier-Matrix zu $^2G_2$ erhalten wir aus einer Konstruktion, die in [12] beschrieben wird. Es ist naheliegend, etwas ähnliches für die Matrix zu $^2F_4$ zu versuchen. Hier ist eine verallgemeinerte Form dieser Konstruktion und eine Erklärung, warum diese im Fall $^2F_4$ wahrscheinlich nicht verwendet werden kann.

Es seien R_1 und R_2 $\mathbb{Z}$-Ringe mit Basen B_1 bzw. B_2, die beide eine C_2-Graduierung besitzen. Es gibt also Basiselemente vom Grad 0 und vom Grad 1; wir bezeichnen den Grad von b mit $\deg(b)$.

Weiter sei R der Teilring von $R_1 \otimes R_2$, der von der Basis

$$B := \{b_1 \otimes b_2 \mid \deg(b_1) = \deg(b_2)\}$$

erzeugt wird. Wir setzen voraus, daß es Elemente $a_1 \in B_1$, $a_2 \in B_2$ mit $a_1^2 = 1$, $a_2^2 = 1$ gibt, so daß $\deg(a_i) = 0$ und a_i durch Multiplikation bijektiv auf der Basis B_i operiert $(i = 1, 2)$.

Für $i = 1, 2$ und $j = 0, 1$ seien

$$\begin{array}{rcl} F_i &:=& \{b \in B_i \mid a_i b = b\}, \\ F_i^j &:=& \{b \in F_i \mid \deg(b) = j\}, \\ B_i^j &:=& \{b \in B_i \mid \deg(b) = j\}. \end{array}$$

Wir betrachten das Ideal von R

$$I := \langle (b_1 \otimes b_2) + (a_1 \otimes a_2)(b_1 \otimes b_2),\ \ (c_1 \otimes c_2) \mid b_1 \otimes b_2 \in B,\ \ c_i \in F_i \rangle \trianglelefteq R.$$

Es ist klar, daß wir eine Basis B' für $R' := R/I$ wählen können, die aus Elementen, die Vertreter in B haben, besteht:

$$B' := \{\overline{a \otimes b} = a \otimes b + I \mid a \otimes b \in B\}.$$

Für geeignete R_1, R_2 usw. ist (R', B') ein $\mathbb{Z}$-Ring mit Basis.

Beispiel 18. Ist $R_1 = R_2 = A_{1,6}^{(1)}$ und $a_1 = a_2 = b_5$, so ist (R', B') isomorph zum Ring der Matrix zu ${}^2G_2$.

Wir wollen zählen, wieviele Elemente in B' von $\overline{a_1 \otimes 1} = -\overline{1 \otimes a_2}$ fixiert werden: Es sei $\overline{a \otimes b} \in B'$. Dann ist

$$(\overline{a \otimes b})(\overline{a_1 \otimes 1}) = \overline{a_1 a \otimes b} = \begin{cases} \overline{a \otimes b} & \text{falls } a \in F_1 \\ -\overline{a \otimes b} & \text{falls } b \in F_2 \\ \neq \pm\overline{a \otimes b} & \text{sonst,} \end{cases}$$

($\overline{a \otimes b} = 0$, falls $a \in F_1$ und $b \in F_2$). Daraus folgen sofort die Gleichungen

$$|\{\overline{a \otimes b} \in B' \mid (\overline{a \otimes b})(\overline{a_1 \otimes 1}) = \overline{a \otimes b}\}| = \frac{1}{2}|F_1^0|(|B_2^0| - |F_2^0|) + \frac{1}{2}|F_1^1|(|B_2^1| - |F_2^1|),$$

$$|\{\overline{a \otimes b} \in B' \mid (\overline{a \otimes b})(\overline{a_1 \otimes 1}) = -\overline{a \otimes b}\}| = \frac{1}{2}|F_2^0|(|B_1^0| - |F_1^0|) + \frac{1}{2}|F_2^1|(|B_1^1| - |F_1^1|).$$

Außerdem haben wir noch

$$|B_1^0||B_2^0| - |F_1^0||F_2^0| + |B_1^1||B_2^1| - |F_1^1||F_2^1| = 2|B'|,$$

wir wissen sogar mehr: Mit $B'^j := \{b \in B' \mid \deg(b) = j\}$ gelten

$$|B_1^0||B_2^0| - |F_1^0||F_2^0| = 2|B'^0|, \quad |B_1^1||B_2^1| - |F_1^1||F_2^1| = 2|B'^1|.$$

Wir wollen jetzt nachprüfen, ob der Ring zu ${}^2F_4$ von dieser Form sein kann. Angenommen er wäre isomorph zu (R', B'). Dann wäre R' C_2-graduiert über einen Teilring mit 9 Elementen. Es gibt nur ein Basiselement im Ring zu ${}^2F_4$, das die Eigenschaften von $\overline{a_1 \otimes 1}$ hat. An der Multiplikationstafel können wir ablesen, daß 4 Elemente von $\overline{a_1 \otimes 1}$ fixiert werden und

1 Element auf sein Negatives abgebildet wird. Alle diese Elemente haben Grad 0. Daraus folgt:

$$|F_1^0|(|B_2^0| - |F_2^0|) = 8, \quad |F_2^0|(|B_1^0| - |F_1^0|) = 2,$$
$$|B_1^0||B_2^0| - |F_1^0||F_2^0| = 18, \quad |B_1^1||B_2^1| = 8,$$

weil $|F_1^1||F_2^1| = 0$. Für die Variablen ergeben sich aus den Gleichungen Schranken: $0 < |F_1^0| \leq 8$, $0 < |F_2^0| \leq 2$, d.h. $|B_1^0|, |B_2^0| \geq 2$. Außerdem ist $|B_1^0||B_2^0| = |F_1^0||F_2^0| + 18 \leq 16 + 18 = 34$ und somit $|B_1^0|, |B_2^0| \leq 17$.

Nach all diesen Einschränkungen bleiben nur zwei Lösungen für $(|B_1^0|, |B_2^0|, |F_1^0|, |F_2^0|)$ übrig: $(4, 5, 2, 1)$ und $(2, 10, 1, 2)$. Diese Lösungen schränken die Suche sehr stark ein. Es ist aber dennoch nicht klar, ob wir diese Konstruktion ausschließen können.

Anhang

Alternative Beweise der Lemmata 5.1.2 und 5.1.3

Wir verwenden die Notation aus 5.1.

Für den Beweis von Satz 5.1.4 benötigen wir eine passende Darstellung des Quotienten $D_{\bar{\imath},\bar{\jmath}} := \frac{(\bigwedge^n S)_{\bar{\imath},\bar{\jmath}}}{(\bigwedge^n S)_{\bar{\imath},\bar{\imath}_0}}$. Alternativ zu den Lemmata 5.1.2 und 5.1.3 erreichen wir dieses Ziel auch unter Verwendung verschiedener Sätze aus der Kombinatorik.

Aus dem Satz über Jacobi-Trudi-Determinanten (siehe z.B. [24], Theorem 4.5.1) folgt ([24], Lemma 4.6.1 und Korollar 4.6.2), daß $D_{\bar{\imath},\bar{\jmath}}$ die Schur-Funktion $s_{\bar{\jmath}'}(\bar{x})$ ausgewertet bei $x_1 = \zeta^{i_1}, \ldots, x_n = \zeta^{i_n}, x_{n+1} = 0, \ldots$ ist, wobei $\bar{\jmath}'$ die Partition

$$\bar{\jmath}' := (j_n - (n-1), \ldots, j_2 - 1, j_1)$$

ist. Lemma 5.1.3 ist sozusagen ein Ersatz für diese Tatsache.

Die Definition der Schur-Funktion $s_{\bar{\jmath}'}$ (siehe z.B. [24], 4.4.1) ist

$$s_{\bar{\jmath}'} = \sum_{T \in \mathcal{T}_{\bar{\jmath}'}} \bar{x}^T,$$

wobei $\mathcal{T}_{\bar{\jmath}'}$ die Menge der semistandard $\bar{\jmath}'$-Tableaux ist, d.h. Tableaux der Gestalt (Ferrers-Diagramm) $\bar{\jmath}'$ mit monoton wachsenden Zeilen, streng monoton wachsenden Spalten und Einträgen aus $\mathbb{N}$. Sind T_{h_1,h_2} die Einträge von einem $T \in \mathcal{T}_{\bar{\jmath}'}$, so ist

$$\bar{x}^T := \prod_{h_1,h_2} x_{T_{h_1,h_2}}.$$

Mit passenden $u_\nu(T) \in \mathbb{N}$ können wir das letzte Produkt auch als

$$\bar{x}^T = \prod_{\nu \in \mathbb{N}} x_\nu^{u_\nu(T)}$$

schreiben. Da wir eigentlich für $x_{n+1}, x_{n+2}, \ldots$ die Zahl 0 einsetzen wollen, betrachten wir ab jetzt

$$s_{\bar{j}'} = \sum_{T \in \mathcal{T}_{\bar{j}'}} \prod_{\nu=1}^{n} x_\nu^{u_\nu(T)}$$

(mit derselben Bezeichnung). Das Analogon zu Lemma 5.1.2 ist nun folgende Aussage:

Bemerkung 8.5.2. *Es seien $a \in \mathbb{N}$ und*

$$z_\nu(a) := \{T \in \mathcal{T}_{\bar{j}'} \mid u_\nu(T) = a\}$$

für $1 \leq \nu \leq n$. Dann gilt für alle $1 \leq \nu' \leq n$

$$|z_\nu(a)| = |z_{\nu'}(a)|.$$

Beweis. Nach [24], Proposition 4.4.2 ist $s_{\bar{j}'}(\bar{x})$ eine symmetrische Funktion (dieses wird unter Verwendung der Kostka-Zahlen, oder mit einer zum Beweis von Lemma 5.1.2 ähnlichen Methode bewiesen). Das bedeutet, daß für alle Permutationen $\pi \in S_n$

$$s_{\bar{j}'} = s_{\bar{j}'}(x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)})$$

und somit

$$\sum_{T \in \mathcal{T}_{\bar{j}'}} \prod_{\nu=1}^{n} x_\nu^{u_{\pi(\nu)}(T)} = \sum_{T \in \mathcal{T}_{\bar{j}'}} \prod_{\nu=1}^{n} x_\nu^{u_\nu(T)}$$

gilt. Damit gibt es für alle $1 \leq \nu \leq n$, $a \in \mathbb{N}$ und $T \in \mathcal{T}_{\bar{j}'}$ mit $u_\nu(T) = a$ ein $T' \in \mathcal{T}_{\bar{j}'}$ mit $u_{\pi(\nu)}(T') = u_\nu(T)$. Daraus folgt aber $|z_\nu(a)| = |z_{\nu'}(a)|$ für alle $1 \leq \nu' \leq n$. □

Der Beweis von Satz 5.1.4 funktioniert jetzt auch, wenn wir alle „$w_{\nu+1}(m)$“ und „$m \in M_{\bar{m}}$“ durch „$u_\nu(T)$“ und „$T \in \mathcal{T}_{\bar{m}'}$“ ersetzen.

Literaturverzeichnis

[1] Arad, Zvi, David Chillag und Marcel Herzog: *Powers of characters of finite groups.* J. Algebra, 103(1):241–255, 1986.

[2] Bakalov, Bojko und Alexander Kirillov, Jr.: *Lectures on tensor categories and modular functors*, Band 21 der Reihe *University Lecture Series.* American Mathematical Society, Providence, RI, 2001.

[3] Blau, Harvey I. und Paul-Hermann Zieschang: *Sylow theory for table algebras, fusion rule algebras, and hypergroups.* J. Algebra, 273(2):551–570, 2004.

[4] Carter, Roger W.: *Finite groups of Lie type.* Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, 1985. Conjugacy classes and complex characters, A Wiley-Interscience Publication.

[5] Chari, Vyjayanthi und Andrew Pressley: *A guide to quantum groups.* Cambridge University Press, Cambridge, 1995.

[6] Coste, Antoine, Terry Gannon und Philippe Ruelle: *Finite group modular data.* Nuclear Phys. B, 581(3):679–717, 2000.

[7] De Wild Propitius, M.: *Spontaneously broken Abelian Chern-Simons.* Nuclear Phys. B, 489:297–359, 1997.

[8] Dijkgraaf, R., V. Pasquier und P. Roche: *Quasi Hopf algebras, group cohomology and orbifold models.* Nuclear Phys. B Proc. Suppl., 18B:60–72 (1991), 1990. Recent advances in field theory (Annecy-le-Vieux, 1990).

[9] Dijkgraaf, Robbert, Cumrun Vafa, Erik Verlinde und Herman Verlinde: *The operator algebra of orbifold models.* Comm. Math. Phys., 123(3):485–526, 1989.

[10] Drozd, Yurij A. und Vladimir V. Kirichenko: *Finite-dimensional algebras.* Springer-Verlag, Berlin, 1994.

[11] Gannon, Terry: *The automorphisms of affine fusion rings.* Adv. Math., 165(2):165–193, 2002.

[12] Geck, Meinolf und Gunter Malle: *Fourier transforms and Frobenius eigenvalues for finite Coxeter groups*. J. Algebra, 260(1):162–193, 2003.

[13] Isaacs, I. Martin: *Character theory of finite groups*. Dover Publications Inc., New York, 1994. Corrected reprint of the 1976 original.

[14] Kac, Victor G.: *Infinite-dimensional Lie algebras*. Cambridge University Press, Cambridge, dritte Auflage, 1990.

[15] Lusztig, George: *Characters of reductive groups over a finite field*, Band 107 der Reihe *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1984.

[16] Lusztig, George: *Leading coefficients of character values of Hecke algebras*. In: *The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986)*, Band 47 der Reihe *Proc. Sympos. Pure Math.*, Seiten 235–262. Amer. Math. Soc., Providence, RI, 1987.

[17] Lusztig, George: *Exotic Fourier transform*. Duke Math. J., 73(1):227–241, 243–248, 1994. Mit einem Anhang von Gunter Malle.

[18] Macdonald, I. G.: *Symmetric functions and Hall polynomials*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, Second Auflage, 1995.

[19] MacLane, Saunders: *Categories for the working mathematician*. Springer-Verlag, New York, 1971. Graduate Texts in Mathematics, Vol. 5.

[20] Malle, Gunter: *Unipotente Grade imprimitiver komplexer Spiegelungsgruppen*. J. Algebra, 177(3):768–826, 1995.

[21] Malle, Gunter: *Spetses*. In: *Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998), Extra Vol. II*, Seiten 87–96 (elektronisch), 1998.

[22] Malle, Gunter: *Complex reflection groups and related objects*. Mathematische Schriften Kassel, Preprint-Reihe, No. 22/00, 2000.

[23] Malle, Gunter: *On the generic degrees of cyclotomic algebras*. Represent. Theory, 4:342–369 (electronic), 2000.

[24] Sagan, Bruce E.: *The symmetric group*, Band 203 der Reihe *Graduate Texts in Mathematics*. Springer-Verlag, New York, Zweite Auflage, 2001. Representations, combinatorial algorithms, and symmetric functions.

[25] Serre, Jean-Pierre: *Linear representations of finite groups*. Springer-Verlag, New York, 1977.

[26] Shephard, G. C. und J. A. Todd: *Finite unitary reflection groups.* Canadian J. Math., 6:274–304, 1954.

[27] Tambara, Daisuke und Shigeru Yamagami: *Tensor categories with fusion rules of self-duality for finite abelian groups.* J. Algebra, 209(2):692–707, 1998.

[28] Verlinde, Erik: *Fusion rules and modular transformations in 2D conformal field theory.* Nuclear Phys. B, 300(3):360–376, 1988.

Index

Hiermit versichere ich, dass ich die vorliegende Dissertation selbständig und ohne unerlaubte Hilfe angefertigt und andere als die in der Dissertation angegebene Hilfsmittel nicht benutzt habe. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder unveröffentlichten Schriften entnommen sind, habe ich als solche kenntlich gemacht. Kein Teil dieser Arbeit ist in einem anderen Promotions- oder Habilitationsverfahren verwendet worden.