Basen von Moduln mit Anwendung auf Kreiseinheiten und Stickelbergerelemente

Dissertation
zur Erlangung des Grades
des Doktors der Naturwissenschaften
der Mathematisch-Naturwissenschaftlichen Fakultät
der Universität des Saarlandes

von
Marc Conrad
Saarbrücken
1997

Tag des Kolloquiums:	13. Februar 1998
Dekan:	Prof. Dr. Th. Wichert
Berichterstatter:	Prof. Dr. H. G. Zimmer Prof. Dr. E.-U. Gekeler

Inhaltsverzeichnis

Einleitung

Ausgangspunkt dieser Arbeit sind die Relationen innerhalb der Gruppe der Kreiseinheiten $C^{(n)}$. Die Gruppe der Kreiseinheiten $C^{(n)}$ ist zu $n \in \mathbf{N}$ und zu einer primitiven n-ten Einheitswurzel ϵ_n definiert als die Einheiten in der Maximalordnung des n-ten Kreisteilungskörpers $\mathbf{Q}(\epsilon_n)$, die im multiplikativen Erzeugnis der Zahlen $1-\epsilon_n^a$ liegen, wobei a die ganzen Zahlen inkongruent 0 modulo n durchläuft, modulo Torsion.

Konkret ist $C^{(n)}$ eine multiplikative Gruppe algebraischer Zahlen, die untereinander gewissen Relationen genügen. In $C^{(n)}$ gibt es zwei offensichtliche Typen von Relationen. Zum einen solche, die durch Bildung von Relativnormen entstehen, wie beispielsweise

$$N_{\mathbf{Q}(\epsilon_{18})\to\mathbf{Q}(\epsilon_6)}(1-\epsilon_{18}) = (1-\epsilon_{18})(1-\epsilon_{18}^7)(1-\epsilon_{18}^{13}) = 1-\epsilon_6, \tag{1}$$

und allgemein von der Form $N_{\mathbf{Q}(\epsilon_d)\to\mathbf{Q}(\epsilon_t)}(1-\epsilon_d^a) \in C^{(t)}$ sind, wobei t ein Teiler von d ist. Zum anderen entstehen Relationen durch komplexe Konjugation gemäß

$$1-\epsilon_n = -\epsilon_n\overline{(1-\epsilon_n)} = -\epsilon_n(1-\epsilon_n^{-1}). \tag{2}$$

Wir nennen im folgenden diese beiden Arten von Relationen (Normbildung und komplexe Konjugation) die offensichtlichen Relationen.

Milnor vermutete noch, daß die offensichtlichen Relationen alle Relationen erzeugen (vergleiche [1]). Ennola zeigt in [4] überraschend eine Relation in $C^{(105)}$ die nicht von offensichtlichen Relationen erzeugt werden kann. Ennola beweist dort, daß aber zumindest das Quadrat jeder Relation von offensichtlichen Relationen gebildet wird. C. G. Schmidt untersucht in [12] den Unterschied zwischen allen Relationen und den offensichtlichen Relationen genauer und stellt einen Zusammenhang her zwischen diesem Unterschied und der σ-Kohomologie eines explizit angegebenen Moduls, wobei σ eine Involution auf diesem Modul bezeichnet, das heißt, einen Homomorphismus mit $\sigma^2 = \mathrm{id}$. Die entsprechenden Kohomologiegruppen werden mit Hilfe eines Ergebnisses von Sinnot in [15] explizit berechnet. Im Rahmen dieser Arbeit werden Schmidts Ergebnisse angewendet, um die Kreiseinheiten $C^{(n)}$ umfangreich zu untersuchen.

Das Hauptziel dieser Arbeit ist die Konstruktion von Basen von $C^{(n)}$. Der gewählte Ansatz dazu unterscheidet sich völlig von entsprechenden Konstruktionen von Gold/Kim in [5] oder Kučera in [8]. In [5] wird in der Notation von Kuberts universellen Distributionen (die beispielsweise in [16], Kapitel 12.3 beschrieben sind) gearbeitet. An entscheidender Stelle, nämlich genau dort, wo der Unterschied zwischen den offensichtlichen und allen Relationen zum Tragen kommt, wird (indirekt über [16] und dann [13]) ein Ergebnis aus [18] benutzt, dessen Beweis in [18] lückenhaft ist. Die Konstruktion einer Basis der Kreiseinheiten in [8] hingegen ist sehr technisch, und es ist nicht nachvollziehbar, welchen allgemeinen Prinzipien diese Konstruktion folgt.

Im Gegensatz dazu ist die Basiskonstruktion in dieser Arbeit nicht nur allgemeiner, da die wesentlichen Konstruktionsprinzipien über $\mathbf{Z}[\sigma]$-Moduln formuliert und bewiesen werden, sondern auch methodisch anders. Die Kreiseinheiten werden in dieser Arbeit als ein System einzelner "Schichten" betrachtet, die den Teilern von n entsprechen. Dies geschieht im wesentlichen dadurch, daß von dem genauen Wert der Relativnorm, also der rechten Seite in (1) abstrahiert wird. Innerhalb dieser Schichten ist eine Basiskonstruktion mit einfachen Methoden möglich.

Ein anderer Aspekt des Unterschieds zwischen der Basiskonstruktion in dieser Arbeit und der bei [5] und [8] ist dadurch gegeben, daß die Basis hier, im Gegensatz zu [5] und [8], streng hierarchisch aufgebaut ist. Das heißt konkret, daß beispielsweise die Basis von $C^{(18)}$ die Basis von $C^{(6)}$ als Teilmenge enthält und zu einer Basis von $C^{(90)}$ erweiterbar ist. In Kapitel 2.4 wird dieser Aspekt ausführlich diskutiert.

Im folgenden umreißen wir zunächst den Aufbau dieser Arbeit und gehen anschließend detailliert auf die einzelnen Kapitel ein. Im ersten Kapitel betrachten wir freie Moduln über $\mathbf{Z}$ der Form $N = M/R$, wobei der Relationsmodul R bei der Übertragung auf Kreiseinheiten gerade den Normrelationen wie in (1) entspricht. Lassen wir die Involution σ auf N operieren, so erhalten wir einen $\mathbf{Z}[\sigma]$-Modul. Die Operation von σ entspricht bei den Kreiseinheiten der komplexen Konjugation, die Relationen wie in (2) liefert.

Der Ansatz, die Kreiseinheiten als Faktormodul eines $\mathbf{Z}[\sigma]$-Moduls zu betrachten, erlaubt es, im ersten Kapitel eine schlüssige Basiskonstruktion für $\mathbf{Z}[\sigma]$-Moduln durchzuführen, die von wesentlich größerer Allgemeinheit ist, als das für Kreiseinheiten notwendig ist. Erst im zweiten Kapitel werden dann die für die Anwendung auf Kreiseinheiten interessanten Moduln, die Kreismoduln und der sogenannte kombinierte Kreismodul, als spezielle Anwendung der im ersten Kapitel behandelten allgemeinen Moduln eingeführt.

Die im zweiten Kapitel entwickelten Zusammenhänge zwischen den Kreismoduln und der Gruppe der Kreiszahlen, einer Gruppe, die die Kreiseinheiten als Untergruppe enthält, werden im dritten Kapitel auf Kreiseinheiten angewendet. Dort findet sich unter anderem auch eine detaillierte Beschreibung, wie man schrittweise eine Basis der Kreiseinheiten aus den Konstruktionen der vorangegangenen Kapitel erhält.

In direktem Zusammenhang mit den Relationen innerhalb der Kreiseinheiten stehen die Relationen, die zwischen den sogenannten Stickelbergerelementen bestehen. Dies ist Gegenstand des vierten Kapitels, das wesentlich auf die bereits im Zusammenhang mit den Kreiseinheiten geleistete Arbeit zurückgreift.

Im folgenden geben wir einen detaillierten Überblick über die einzelnen Kapitel.

1. Kapitel

Im ersten Kapitel "Grundlagen" wird ausführlich die Frage behandelt, wie sich geeignete Basen, sogenannte *Normalbasen*, auf $\mathbf{Z}[\sigma]$-Moduln konstruieren

lassen. Eine Normalbasis ist definiert als eine Basis, die sich als disjunkte Vereinigung $E^0 \cup \sigma E^0 \cup E^+ \cup E^-$ schreiben läßt, wobei σ auf E^+ trivial operiert und $\sigma e = -e$ für $e \in E^-$ gilt. Ist N ein $\mathbf{Z}[\sigma]$-Modul, so liefern Normalbasen Basen von $N_+ := N/\ker_N(1+\sigma)$ und $N_- := N/\ker_N(1-\sigma)$: Es ist $E^0 \cup E^+$ eine Basis von N_+ und $E^0 \cup E^-$ eine Basis von N_- (Lemma 1.2.10). Es sei angemerkt, daß in dieser Arbeit noch allgemeinere Basen als Normalbasen betrachtet werden, die als *Quasinormalbasen* bezeichnet werden und ähnliche Eigenschaften wie Normalbasen haben. Im Rahmen dieser Einleitung beschränken wir uns auf Normalbasen.

Innerhalb der vorliegenden Arbeit werden Normalbasen auf die folgenden Arten konstruiert.

I) Gegeben seien zwei Moduln M und N mit Normalbasen. Man konstruiere eine Normalbasis von $M \otimes N$. Dies wird in Satz 1.3.4 gezeigt.

II) Gegeben sei eine endliche Menge A, auf der σ operiert. Man konstruiere eine Normalbasis der durch A definierten $\mathbf{Z}[\sigma]$-Moduln $\langle A \rangle$ und $\langle A \rangle / \langle \sum_{a \in A} a \rangle$. Dies ist Gegenstand von Lemma 1.4.6.

III) Gegeben sei eine kurze exakte Sequenz $0 \to M \to L \to K \to 0$ von Moduln. Man konstruiere aus Normalbasen von M und K eine Normalbasis von L. In Algorithmus 1.6.6 geben wir diese Konstruktion explizit an.

IV) Gegeben sei ein partiell geordnetes System von Moduln, die untereinander durch Abbildungen verbunden sind (wir geben weiter unten eine exakte Definition an). Solche Systeme werden in dieser Arbeit als *M&n-Systeme* bezeichnet und definieren einen weiteren Modul, der *Kombinat* des M&n-Systems genannt wird. Man konstruiere eine Normalbasis dieses Kombinates. Algorithmus 1.6.15 löst dieses Problem.

Diese vier Konstruktionsprinzipien werden in voller Ausführlichkeit behandelt. Beispielsweise wird Prinzip I verallgemeinert auf Tensorprodukte von mehr als zwei Moduln und immer in Zusammenhang mit dem wichtigen Begriff der Normal*zerlegung* gebracht. Die Normalzerlegung liefert eine Aussage über die Struktur eines $\mathbf{Z}[\sigma]$-Moduls, die unabhängig von konkret gewählten Basen ist.

Das Konstruktionsprinzip II ist technisch unproblematisch, aber dennoch wesentlich, da mit diesem die Verbindung von endlichen Mengen, auf denen σ operiert, zu durch diese Mengen definierten Moduln geschaffen wird. Die beiden durch A definierten Moduln, nämlich das freie $\mathbf{Z}$-Erzeugnis $\langle A \rangle$ der Menge A und der freie Modul $\langle A \rangle / \langle \sum_{a \in A} a \rangle$ werden als *elementare Zeilenfaktormoduln* bezeichnet.

Die Konstruktion nach Prinzip III ist dann sehr einfach, wenn die Sequenz eine Eigenschaft hat, die in dieser Arbeit "Gutartigkeit" genannt wird. Gutartigkeit läßt sich mit verschiedenen Kriterien nachweisen, beispielsweise als Exaktheit einer Sequenz von Kohomologiegruppen, oder aber als Additivität von Invarianten der Moduln N, L und K (Satz 1.6.8). Ist eine Sequenz als gutartig

erkannt, so erhält man eine Basis beispielsweise von L_+ ohne Umweg über Normalbasen direkt aus Basen von N_+ und K_+.

Das Prinzip der Gutartigkeit findet auch im Zusammenhang mit den $M\mathfrak{En}$-Systemen in Prinzip IV Anwendung. Konkret ist ein $M\mathfrak{En}$-System ein System von Tripeln $(M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d\in\Delta}$. Dabei ist Δ partiell geordnet, die M_d sind freie $\mathbf{Z}$-Moduln, und die $\mathfrak{n}_d$ sind Abbildungen $\mathfrak{n}_d : \mathcal{E}_d \to \bigoplus_{t<d} M_t$, wobei $\mathcal{E}_d \subseteq M_d$ eine Teilmenge von M_d ist. Ist das System *kombinierbar* (eine leicht zu verifizierende Eigenschaft der $\mathfrak{n}_d$), so erlaubt es Prinzip IV, aus Normalbasen der Moduln $M_d/\langle\mathcal{E}_d\rangle$ eine Normalbasis des Moduls $L := N/Q$ mit $N := \bigoplus_{d\in\Delta} M_d$ und $Q := \sum_{d\in\Delta}\langle r + \mathfrak{n}_d(r);\ r \in \mathcal{E}_d\rangle$ zu konstruieren. Dieser Modul L wird als *Kombinat* des $M\mathfrak{En}$-Systems bezeichnet. Ist das System gutartig, so läßt sich auch hier wie in Prinzip III die Konstruktion abkürzen, so daß man eine Basis von beispielsweise L_+ durch Vereinigung von in L definierten Basen der $(M_d/\langle\mathcal{E}_d\rangle)_+$ erhält.

Konkret handelt es sich bei der Anwendung auf Kreiseinheiten bei den Moduln $M_d/\langle\mathcal{E}_d\rangle$ um sogenannte *Zeilenfaktormoduln*, die in Abschnitt 1.4 des ersten Kapitels eingeführt und untersucht werden. Wir identifizieren die Zeilenfaktormoduln dabei zunächst als das Tensorprodukt elementarer Zeilenfaktormoduln (Korollar 1.4.4 zu Satz 1.4.3), für die wir nach Konstruktionsprinzip II Normalbasen konstruieren können. Mit Prinzip I erhalten wir dann eine Normalbasis eines beliebigen Zeilenfaktormoduls.

2. Kapitel

Im zweiten Kapitel werden aus der allgemeinen Situation des ersten Kapitels heraus die für die Anwendungen auf Kreiseinheiten notwendigen Objekte eingeführt und untersucht.

Zunächst führen wir *Kreismoduln* ein (Definition 2.1.1). Die Kreismoduln sind definiert als Tensorprodukte geeigneter elementarer Zeilenfaktormoduln. Dadurch ist es möglich, mit Hilfe der im ersten Kapitel entwickelten Konstruktionsprinzipien explizit Normalbasen von Kreismoduln zu berechnen. Kreismoduln lassen sich auch interpretieren als freies $\mathbf{Z}$-Erzeugnis der Menge $G_n := \{1 \le a < n;\ \gcd(a,n) = 1\}$ modulo gewisser explizit definierter Relationen. Dies wird in Satz 2.1.3 ausführlich diskutiert. Grob gesagt ist mit dieser Interpretation der Zusammenhang zwischen Kreismoduln und Kreiseinheiten gegeben durch die Zuordnung $a \mapsto 1 - \epsilon_n^a$ für $a \in G_n$.

Im Abschnitt 2.2 werden dann die Kreismoduln zu einem größerem Modul, dem *kombinierten Kreismodul* $\mathcal{L}(n)$ zusammengesetzt. Dies geschieht durch die Festlegung eines geeigneten $M\mathfrak{En}$-Systems, dem *Kreissystem*, welches den Modul $\mathcal{L}(n)$ als sein Kombinat definiert. Die Relationen innerhalb von $\mathcal{L}(n)$ entsprechen dabei den Normrelationen in der Gruppe der Kreiseinheiten.

Dieser Modul $\mathcal{L}(n)$ wird identifiziert als ein in [12] behandelter Modul, dessen σ-Kohomologie bekannt ist. Die Kenntnis der σ-Kohomologie wird ausgenutzt, um in Abschnitt 2.2.3 die Gutartigkeit bei der Anwendung von Prinzip IV nachzuweisen. Mit diesem Nachweis erhalten wir leicht eine Basis von $\mathcal{L}(n)_+$

und $\mathcal{L}(n)_-$, nämlich im wesentlichen durch Vereinigung von entsprechenden Basen der Kreismoduln.

In Abschnitt 2.3 stellen wir den Zusammenhang zwischen Kreismoduln und Kreiszahlen explizit her. Die Gruppe der Kreiszahlen ist definiert als das multiplikative Erzeugnis der Elemente $1 - \epsilon_n^a$ für $a = 1, \ldots, n-1$ modulo Torsion, und sie enthält die Gruppe der Kreiseinheiten als Untergruppe.

Im letzten Abschnitt des zweiten Kapitels wird dargestellt, wie die Konstruktion, die mit dem Kreissystem durchgeführt wurde, mit einem anderen $M\mathcal{E}$n-System, dem *P-Kreissystem*, durchzuführen wäre. Dieser alternative Ansatz zur Konstruktion einer Basis der Kreiseinheiten ist deswegen interessant, weil die Vorgehensweise beim P-Kreissystem derjenigen bisheriger Abhandlungen über Basen von Kreiseinheiten, wie beispielsweise in [8], [5] oder [2], entspricht. In Abschnitt 2.4.3 gehen wir ausführlich auf die Unterschiede zwischen Kreissystem und P-Kreissystem ein, stellen die Vorteile des Kreissystems heraus und zeigen auf, wo die Grenzen des P-Kreissystems zu ziehen sind.

3. Kapitel

Im dritten Kapitel wird endlich die Gruppe der Kreiseinheiten $C^{(n)}$ selbst behandelt. Der Unterschied zwischen der Gruppe der Kreiseinheiten und der Gruppe der Kreiszahlen besteht darin, daß in den Fällen, in denen n die Potenz einer Primzahl ist, statt $1 - \epsilon_n^a$ die Zahlen der Form $(1 - \epsilon_n^a)/(1 - \epsilon_n)$ betrachtet werden müssen, denn es ist $1 - \epsilon_n^a$ nicht immer eine Einheit in $\mathbf{Z}[\epsilon_n]$. Diesem Unterschied wird durch das Konzept des *Differenzenmoduls* Rechnung getragen, das in Kapitel 1.5 eingeführt wird und hier seine Anwendung findet.

In den Abschnitten 3.1 und 3.2 untersuchen wir den Zusammenhang zwischen Kreiszahlen und Kreiseinheiten und gehen insbesondere darauf ein, wie man aus Basen der Gruppe der Kreiszahlen eine Basis der Gruppe der Kreiseinheiten erhält und umgekehrt. Als Ergebnis erhalten wir, daß wir eine Basis der Gruppe der Kreiseinheiten $C^{(n)}$ durch Vereinigung von (in $C^{(n)}$ definierten) Basen der *relativen Kreiseinheiten* $\widehat{C^{(n)}}$ konstruieren können (Satz 3.2.3). Die relativen Kreiseinheiten sind definiert durch $\widehat{C^{(n)}} := C^{(n)} / \prod_d C^{(d)}$, wobei d alle echten Teiler von n durchläuft. Durch den konsequent hierarchischen Aufbau erhalten wir auch direkt eine Basis von $C^{(\infty)} := \bigcup_{d \in \mathbf{N}} C^{(d)}$ durch die Vereinigung über $d \in \mathbf{N}$ von in $C^{(d)}$ definierten Basen der $\widehat{C^{(d)}}$ (Korollar 3.2.5).

Im anschließenden Abschnitt 3.3 wird dann zusammenfassend der Weg von einfachen Mengen, auf denen σ operiert, bis hin zu einer Basis der Gruppe der Kreiseinheiten explizit beschrieben und an einem Beispiel für $n = 45$ erläutert.

Neben der Konstruktion von Basen sind auch die Relationen zwischen den Kreiseinheiten von Interesse. Dies ist Gegenstand von Abschnitt 3.4, wo vor allem die *Ennolarelationen* untersucht werden, die die Lücke zwischen den offensichtlichen Relationen und allen Relationen füllen. Darüber hinaus wird geklärt, warum es durch das Zusammenspiel von Norm- und Konjugationsrelationen wie (1) und (2) zwangsläufig zu diesen Ennolarelationen kommen muß.

4. Kapitel
Das vierte Kapitel behandelt die Relationen des *allgemeinen Stickelbergerideals*, das als **Z**-Erzeugnis der gemäß [15] definierten Stickelbergerelemente entsteht. Der Unterschied zu und der Zusammenhang mit den Kreiseinheiten liegt darin, daß das allgemeine Stickelbergerideal im wesentlichen isomorph zu $\mathcal{L}(n)_-$ ist, wohingegen die Gruppe der Kreiseinheiten, wie schon erwähnt, $\mathcal{L}(n)_+$ entspricht, wobei $\mathcal{L}(n)$ der im zweiten Kapitel definierte und untersuchte kombinierte Kreismodul ist. Daher ist die Hauptarbeit, nämlich die Untersuchung von $\mathcal{L}(n)$, schon getan.

Ähnlich wie bei den Kreiseinheiten geben wir ausführlich und explizit an, wie man eine Basis des allgemeinen Stickelbergerideals erhält. Das Kapitel endet mit einer Diskussion der auch in diesem Fall analog zu den Kreiseinheiten vorkommenden Ennolarelationen. Beispiele zur Berechnung einer solchen Ennolarelation für $n = 15$ und $n = 5005$ runden diese Betrachtung ab.

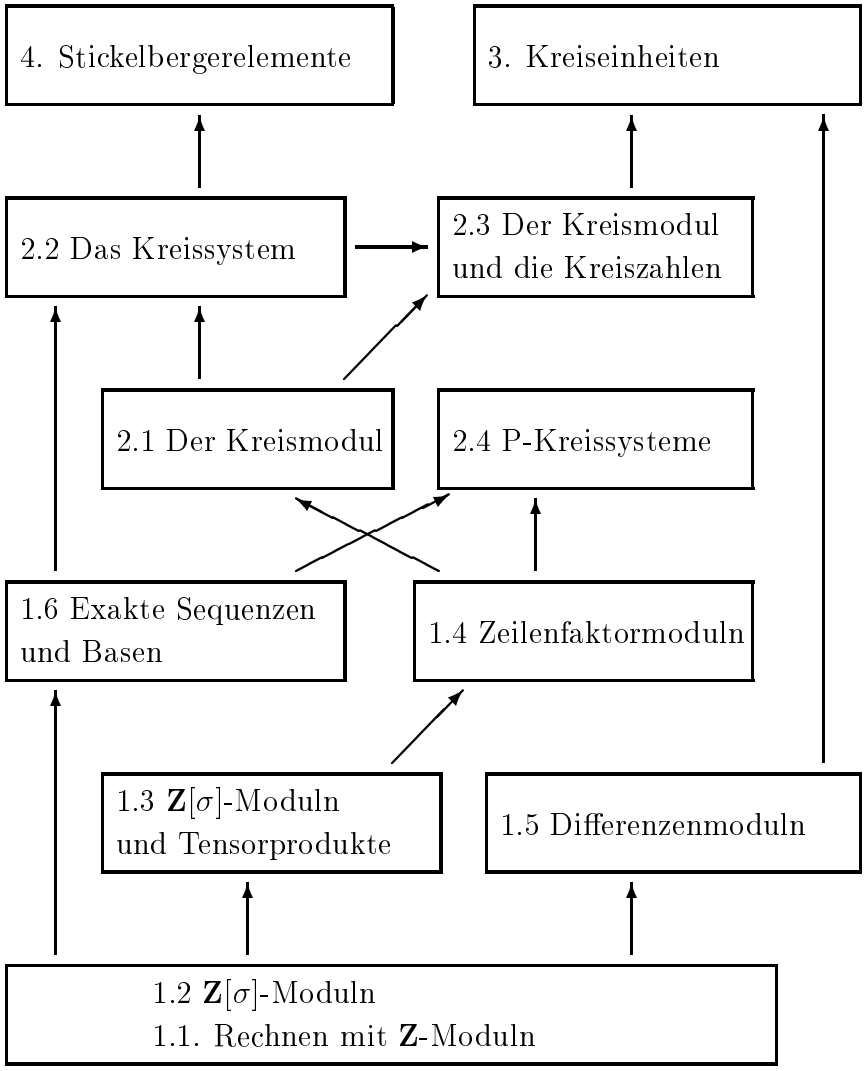
Schließlich sei noch auf den Anhang hingewiesen, in dem explizit ein Algorithmus vorgestellt wird, der nicht nur eine Basis der Kreiseinheiten ausgibt, sondern auch zu einem gegebenem $u \in C^{(n)}$ dessen Basisdarstellung berechnet. Dieser Algorithmus wurde in der hier angegebenen Form als Aufsatz zum SIMATH-System in der Sprache C++ implementiert. Damit ausgerechnete Beispiele illustrieren die Wirkungsweise des Algorithmus. Abschließend werden noch einige programmiertechnisch interessante Aspekte wie Laufzeit, Optimierungs- und Verifikationsmöglichkeiten diskutiert.

An dieser Stelle möchte ich mich bei Herrn Prof. Dr. H. G. Zimmer für die Anregung zu dieser Arbeit, seine großzügige Unterstützung und hilfreichen Anmerkungen bedanken. Ganz besonders gedankt sei auch Herrn Prof. Dr. Klaus Hoechsmann, der von Beginn an als geduldiger Zuhörer und kompetenter Ratgeber die Arbeit begleitete. Insbesondere die Vorgehensweise, sich nicht damit zufriedenzugeben, auf direktem Weg irgendeine Basis der Kreiseinheiten konstruieren zu können, sondern danach zu streben, jeden Einzelschritt auf diesem Weg zu hinterfragen und zu verstehen, um Resultate in größtmöglicher Allgemeinheit zu erhalten, ist wesentlich durch die zahlreichen Diskussionen mit ihm geprägt worden.

Ebenfalls bedanken möchte ich mich bei meiner Frau Vesna für ihre Unterstützung im allgemeinen und für ihre Hinweise und Bemerkungen zur Arbeit selbst. Weiterhin geht mein Dank an Dr. Stefan Kühnlein für seine nützlichen Kommentare zur fast fertigen Arbeit.

Schließlich seien auch alle diejenigen Mitglieder des Fachbereichs 9 Mathematik der Universität des Saarlandes in meinen Dank eingeschlossen, die für die angenehme Athmosphäre dort verantwortlich sind, in der ein produktives und fruchtbares Arbeiten überhaupt erst möglich wird.

Wegweiser


4. Stickelbergerelemente
3. Kreiseinheiten
2.2 Das Kreissystem
2.3 Der Kreismodul und die Kreiszahlen
2.1 Der Kreismodul
2.4 P-Kreissysteme
1.6 Exakte Sequenzen und Basen
1.4 Zeilenfaktormoduln
1.3 $\mathbf{Z}[\sigma]$-Moduln und Tensorprodukte
1.5 Differenzenmoduln
1.2 $\mathbf{Z}[\sigma]$-Moduln
1.1. Rechnen mit $\mathbf{Z}$-Moduln

1 Grundlagen

1.1 Rechnen mit Z-Moduln

1.1.1 Basen und direkte Summen

Das Hauptanliegen dieser Arbeit ist die Konstruktion von Basen. Dabei kommt es häufig vor, daß die Basis eines Moduls nicht als Teilmenge dieses Moduls definiert ist, sondern als Teilmenge eines anderen Moduls. Wir führen dazu den folgenden Sprachgebrauch ein.

Definition 1.1.1 *Es sei E eine Menge, N ein freier Modul, und es sei eine Abbildung $\xi : E \to N$ gegeben. Ist $B \subseteq E$ so definiert, daß ξ auf B injektiv ist und $\{\xi(b);\ b \in B\}$ eine Basis von N ist, so sagen wir, daß $B \subseteq E$ eine Basis in N induziert oder auch, daß die Basis B von N in E lebt.*

Bemerkung 1.1.2 *Von besonderer Bedeutung ist der folgende Fall: Es sei M ein freier Modul, $R \leq M$ ein Teilmodul von M und M/R ebenfalls frei. M und M/R seien durch den kanonischen Homomorphismus $M \to M/R$ miteinander verbunden. Dann gilt:*

- *Jede Teilmenge $B \subseteq M$, die eine Basis von M/R induziert, impliziert eine Zerlegung von M gemäß*

$$M \cong \langle B \rangle \oplus R. \tag{3}$$

- *Ist umgekehrt eine Zerlegung*

$$M \cong C \oplus R \tag{4}$$

  gegeben, und B eine Basis von C, so induziert B eine Basis von M/R.

Mit Bemerkung 1.1.2 erhalten wir den Isomorphismus des folgenden Lemmas.

Lemma 1.1.3 *Es sei M ein freier **Z**-Modul und $R \leq M$ ein Teilmodul, derart daß M/R ebenfalls frei ist. Dann gilt*

$$M \cong (M/R) \oplus R. \tag{5}$$

Beweis
Man fixiere eine Basis B' von M/R und lifte diese zu einer Menge $B \subseteq M$. Mit Bemerkung 1.1.2 gilt $M \cong \langle B \rangle \oplus R$.
Gleichzeitig ist $\langle B \rangle \cong M/R$, da Basiselemente auf Basiselemente abgebildet werden.

QED.

1.1.2 Tensorprodukte

Das Tensorprodukt $M \otimes N$ zweier **Z**-Moduln M und N ist definiert als das Erzeugnis von $M \times N$ modulo dem freien **Z**-Erzeugnis der Elemente der Form

- $(m + m', n) - (m, n) - (m', n)$,
- $(m, n + n') - (m, n) - (m, n')$,
- $(\alpha m, n) - (m, \alpha n)$,

jeweils mit $m, m' \in M$, $n, n' \in N$ und $\alpha \in \mathbf{Z}$.
Die erzeugenden Elemente von $M \otimes N$ bezeichnen wir mit $m \otimes n$ mit $m \in M$ und $n \in N$.
Ist im folgenden die Rede davon, daß Teilmengen von $M \times N$ Basen von $M \otimes N$ induzieren, so geschieht dies über die Abbildung $M \times N \to M \otimes N$, die (m, n) nach $m \otimes n$ abbildet.
Wir stellen zunächst einige Eigenschaften des Tensorproduktes fest.

Lemma 1.1.4 *Das Tensorprodukt ist assoziativ, kommutativ und bezüglich $\oplus$ distributiv. Das heißt, sind L, M und N drei* **Z***-Moduln, so gilt*

a) $(L \otimes M) \otimes N \cong L \otimes (M \otimes N)$,

b) $M \otimes N \cong N \otimes M$,

c) $L \otimes (M \oplus N) \cong (L \otimes M) \oplus (L \otimes N)$.

Beweis
Einen Beweis dazu findet man beispielsweise in [6], Seite 212ff.

QED.

Durch die Assoziativität aus Lemma 1.1.4 ist auch das Tensorprodukt $M_1 \otimes \cdots \otimes M_k$ endlich vieler Moduln $M_1, \ldots, M_k$ (bis auf Isomorphie) eindeutig definiert.
Eine Basis des Tensorproduktes $M \otimes N$ erhält man aus den Basen von M und N wie folgt.

Lemma 1.1.5 *Für zwei freie* **Z***-Moduln M und N gilt: Ist B eine Basis von M und C eine Basis von N dann ist $M \otimes N$ frei, und es induziert $B \times C$ eine Basis von $M \otimes N$.*

Beweis
$B \times C$ induziert die Menge $\{b \otimes c;\ b \in B, c \in C\}$. Diese ist nach [6], Corollary 5.12, eine Basis von $M \otimes N$.

QED.

Um Klammern zu sparen vereinbaren wir im folgenden, daß / stärker bindet als $\otimes$ und $\oplus$.

Lemma 1.1.6 *Zu zwei freien* $\mathbf{Z}$*-Moduln* M *und* N *seien Teilmoduln* $R \leq M$ *und* $Q \leq N$ *gegeben, derart daß* M/R *und* N/Q *frei sind. Dann ist*

$$M/R \otimes N/Q \cong {(M \otimes N)}\Big/{((M \otimes Q) + (R \otimes N))} \ . \tag{6}$$

Beweis
Mit Hilfe der Zerlegungen $M \cong M/R \oplus R$ und $N \cong N/Q \oplus Q$ und der Distributivität von $\otimes$ bezüglich $\oplus$ erhalten wir mittels Lemma 1.1.3

$$\begin{aligned} M \otimes N &\cong (M/R \oplus R) \otimes (N/Q \oplus Q) \\ &\cong (M/R \otimes N/Q) \oplus (M/R \otimes Q) \oplus (R \otimes N/Q) \oplus (R \otimes Q) \\ &\cong (M/R \otimes N/Q) \oplus ((M \otimes Q) + (R \otimes N)). \end{aligned} \tag{7}$$

Faktorisieren wir (7) modulo $(M \otimes Q) + (R \otimes N)$, so folgt die Behauptung.

QED.

In Lemma 1.1.6 kommt die nicht direkte Summe $(M \otimes Q) + (R \otimes N)$ vor, die wir im folgenden genauer untersuchen werden.

Lemma 1.1.7 *Zu zwei freien* $\mathbf{Z}$*-Moduln* M *und* N *seien Teilmoduln* $R \leq M$ *und* $Q \leq N$ *gegeben, derart daß* M/R *und* N/Q *frei sind. Dann gilt*

a) $(R \otimes N) \cap (M \otimes Q) = R \otimes Q$,

b) $(M \otimes Q) + (R \otimes N) \cong (M/R \otimes Q) \oplus (R \otimes N)$.

Beweis
Wie schon in (7) benutzt, ist

$$(R \otimes N) + (M \otimes Q) \cong (M/R \otimes Q) \oplus (R \otimes N/Q) \oplus (R \otimes Q). \tag{8}$$

Durch Ausklammern von R in den letzten beiden Termen folgt Teil b. Da die Summe der drei Terme auf der rechten Seite von (8) direkt ist, folgt Teil a.

QED.

1.2 $\mathbf{Z}[\sigma]$-Moduln

Alle im folgenden betrachteten Moduln seien freie $\mathbf{Z}$-Moduln endlichen Ranges, auf denen zusätzlich die zweielementige Gruppe $\{1, \sigma\}$ operiert. Das heißt, ist M ein Modul und $m \in M$, so gilt $1m = m$ und $\sigma(\sigma(m)) = m$. Es wird dann M zu einem $\mathbf{Z}[\sigma]$-Modul gemäß $(a + b\sigma)m := am + b\sigma m$ für $a, b \in \mathbf{Z}$.

1.2.1 Die Normalzerlegung von $\mathbf{Z}[\sigma]$-Moduln

Operiert σ auf einem Modul M, so gibt es drei Möglichkeiten, wie sich σ auf einem Element $m \in M$ verhält. Gilt $\sigma m = m$ oder $\sigma m = -m$, so ist das $\mathbf{Z}[\sigma]$-Erzeugnis von m isomorph zu $\mathbf{Z}$, und σ operiert auf diesem entweder trivial oder durch Negation. Ist andernfalls $\sigma m = m'$ mit $m' \neq \pm m$, so ist das $\mathbf{Z}[\sigma]$-Erzeugnis von m ein zweidimensionaler, von den Elementen m und σm erzeugter $\mathbf{Z}$-Modul, der isomorph zu $\mathbf{Z}[\sigma]$ ist, auf dem $\mathbf{Z}[\sigma]$ durch Multiplikation operiert.

Das folgende Lemma zeigt, daß sich jeder $\mathbf{Z}[\sigma]$-Modul in eine direkte Summe von zu $\mathbf{Z}$ oder $\mathbf{Z}[\sigma]$ isomorphen Moduln zerlegt, auf denen σ in der oben beschriebenen Art und Weise operiert.

Lemma 1.2.1 *Es sei M ein Modul. Zu M existieren eine Zerlegung gemäß $M = M^0 \oplus M^+ \oplus M^-$ und eindeutig bestimmte Zahlen m^0, m^+ und $m^- \in \mathbf{N}$ mit*

- $M^0 \cong \mathbf{Z}[\sigma]^{m^0}$*, wobei σ auf den einzelnen Komponenten durch Multiplikation operiert,*
- $M^+ \cong \mathbf{Z}^{m^+}$*, wobei σ trivial auf M^+ operiert,*
- $M^- \cong \mathbf{Z}^{m^-}$*, und σ operiert auf den einzelnen Komponenten durch Negation.*

Beweis
In [3], Theorem 74.3, wird die Zerlegung für beliebige $\mathbf{Z}G$-Moduln bewiesen, wobei G eine Gruppe primer Ordnung ist. Wir geben hier eine "Übersetzung" an, wie dieser Satz zum Beweis der Zerlegung in Lemma 1.2.1 anzuwenden ist.

Speziell im Fall $G = \{1, \sigma\}$ ergibt sich mit den dortigen Bezeichnungen eine Zerlegung

$$M \cong (A_1, a_1) \oplus \cdots \oplus (A_r, a_r) \oplus A_{r+1} \oplus \cdots \oplus A_n \oplus Y. \tag{9}$$

Auf den zu $\mathbf{Z}$ isomorphen A_i operiere σ durch Negation. Auf Y operiere σ trivial, und die Moduln (A_i, a_i) mit $a_i \in A_i \setminus 2A_i$ seien von der Form $A_i \oplus y\mathbf{Z}$, auf denen σ gemäß $\sigma y = y + a_i$ operiert.

Es entspricht nun M^+ dem Modul Y und M^- der Summe $A_{r+1} \oplus \cdots \oplus A_n$. Dabei ist $m^+ = \operatorname{rg} Y$ und $m^- = n - r$.

Es bleibt zu zeigen, daß $\mathbf{Z}[\sigma] \cong (A_i, a_i)$ und damit $m^0 = r$ ist. Schreiben wir $A_i = x\mathbf{Z}$ und daher $(A_i, a_i) = x\mathbf{Z} \oplus y\mathbf{Z}$ und $a_i = (2k+1)x$ mit $k \in \mathbf{Z}$, so wird der gewünschte Isomorphismus etabliert durch $\sigma \mapsto kx+y$ und $1 \mapsto (k+1)x+y$.

QED.

Definition 1.2.2 *Eine Zerlegung eines $\mathbf{Z}[\sigma]$-Moduls $M = M^0 \oplus M^+ \oplus M^-$ gemäß Lemma 1.2.1 nennen wir* Normalzerlegung *mit* Invarianten *m^+, m^- und m^0.*

Zunächst stellen wir einige einfache Eigenschaften von Normalzerlegungen fest.

Lemma 1.2.3 *Es sei $M = M^0 \oplus M^+ \oplus M^-$ ein Modul in Normalzerlegung. Dann gilt:*

i) *Ist $\sigma m = m$ für $m \in M^0$, so ist $m \in (1+\sigma)M^0$.*

ii) *Ist $\sigma m = -m$ für $m \in M^0$, so ist $m \in (1-\sigma)M^0$.*

Beweis
Wir zeigen i für $M^0 = \mathbf{Z}[\sigma]$. Dazu sei $g = a + b\sigma \in \mathbf{Z}[\sigma]$ mit $a, b \in \mathbf{Z}$ gegeben. Aus $\sigma(a + b\sigma) = a + b\sigma$ folgt $b + \sigma a = a + \sigma b$, also insbesondere $a = b$. Somit ist $g = (1+\sigma)a$.
Gilt die Behauptung aber für $\mathbf{Z}[\sigma]$, so auch für die direkte Summe von Moduln $\mathbf{Z}[\sigma]$.
Teil ii folgt analog.

QED.

Das nächste Lemma zeigt, daß sich aus einer Normalzerlegung die Struktur der Kohomologiegruppen $H^0(\sigma, M)$ und $H^1(\sigma, M)$ ablesen läßt.

Lemma 1.2.4 *Es sei $M = M^0 \oplus M^+ \oplus M^-$ ein Modul in Normalzerlegung. Dann ist $H^0(\sigma, M) \cong M^+/2M^+$ und $H^1(\sigma, M) \cong M^-/2M^-$.*
Mit anderen Worten $H^0(\sigma, M)$ ist ein $\mathbf{F}_2$-Vektorraum der Dimension m^+, und es ist $H^1(\sigma, M)$ ein $\mathbf{F}_2$-Vektorraum der Dimension m^-.

Beweis
Es ist $H^0(\sigma, M) = \ker_M(1-\sigma)/(\sigma+1)M$ und $H^1(\sigma, M) = H^0(-\sigma, M)$ (zur allgemeinen Definition der Kohomologiegruppen siehe [10], Seite 25).
Aus $\ker_M(1-\sigma) = (1+\sigma)M^0 \oplus M^+$ und $(1+\sigma)M = (1+\sigma)M^0 \oplus 2M^+$ folgt die Behauptung für $H^0(\sigma, M)$.
Ersetzt man σ durch $-\sigma$, so folgt die Behauptung für $H^0(-\sigma, M)$.

QED.

1.2.2 Normalbasen und Quasinormalbasen

Da das eigentliche Interesse dieser Arbeit in der expliziten Konstruktion von Basen liegt, beschäftigen wir uns im weiteren mit den Basen, die eine Normalzerlegung nach sich ziehen, den Normalbasen.

Definition 1.2.5 *Es sei M ein Modul. Eine Basis $B := E^0 \cup \sigma E^0 \cup E^+ \cup E^-$ von M mit*

i) $E^0 \cap \sigma E^0 = \emptyset$,

ii) $\sigma e = e$ *für* $e \in E^+$,

iii) $\sigma e = -e$ *für* $e \in E^-$,

heißt Normalbasis. *Wir schreiben eine solche Basis kurz $B = [E^0, E^+, E^-]$.*

Offensichtlich definiert jede Normalbasis $[E^0, E^+, E^-]$ eines Moduls M eine Normalzerlegung $M^0 \oplus M^+ \oplus M^-$ von M gemäß $M^0 := \langle E^0 \cup \sigma E^0 \rangle$, $M^+ := \langle E^+ \rangle$ und $M^- := \langle E^- \rangle$.
Es sei noch einmal betont, daß die Schreibweise $B = [E^0, E^+, E^-]$ als Abkürzung des Ausdrucks $B = E^0 \cup \sigma E^0 \cup E^+ \cup E^-$ zu verstehen ist, mit der Betonung, daß B eine Normalbasis ist. Das heißt, es kommt zu E^0 noch σE^0 als Teilmenge von B dazu. Die Mächtigkeit von B ist demzufolge $|B| = 2|E^0| + |E^+| + |E^-|$.
Oft reicht eine schwächere Version der Normalbasen aus, die wir wie folgt definieren.

Definition 1.2.6 *Gelten in Definition 1.2.5 statt der Bedingungen ii und iii die schwächeren Bedingungen*

ii') $\sigma e \equiv e \bmod M^0$ *für* $e \in E^+$,

iii') $\sigma e \equiv -e \bmod M^0$ *für* $e \in E^-$,

mit $M^0 = \langle E^0 \cup \sigma E^0 \rangle$, dann heißt $B = [E^0, E^+, E^-]$ Quasinormalbasis.

Natürlich ist jede Normalbasis auch Quasinormalbasis, und jede Quasinormalbasis impliziert eine Zerlegung $M = M^0 \oplus M^*$ mit $M^* = \langle E^+ \cup E^- \rangle$. Außerdem induziert $B = [\emptyset, E^+, E^-]$ eine Normalbasis von M/M^0.
Viele Aussagen über Quasinormalbasen lassen sich einfach auf entsprechende Aussagen über Normalbasen zurückführen. Die Beziehung zwischen Quasinormalbasen und Normalbasen, die dazu ausgenutzt wird, stellt die folgende Definition her.

Definition 1.2.7 *Es sei $C = [F^0, F^+, F^-]$ eine Quasinormalbasis eines Moduls M und $B = [E^0, E^+, E^-]$ eine Normalbasis von M. Es heißt B* assoziiert *zu C, falls $E^0 = F^0$ ist und eine Abbildung $\xi : E^+ \cup E^- \to M^0$ existiert, so daß*

$$F^+ = \{e + \xi(e);\ e \in E^+\} \quad \textit{und} \quad F^- = \{e + \xi(e);\ e \in E^-\}$$

ist.

Lemma 1.2.8 *Jede Quasinormalbasis besitzt eine zu ihr assoziierte Normalbasis.*

Beweis
Es sei die Quasinormalbasis $C = [F^0, F^+, F^-]$ gegeben.

Wir geben explizit an, wie e und $\xi(e)$ zu $f \in F^+$ berechnet werden, so daß $\sigma e = e$ und $\xi(e) \in M^0$ sowie $f = e + \xi(e)$ gelten. (Für F^- argumentiert man analog.)

Man setze $m := \sigma f - f$. Es ist $m \in M^0$, und nach Lemma 1.2.3 ist sogar $m \in (\sigma - 1)M^0$. Daher läßt sich $m = (\sigma - 1)m'$ mit $m' \in M^0$ schreiben. Man setze $e := f - m'$ und $\xi(e) := m'$.

QED.

Die nächste Definition mit dem folgenden Lemma zeigt, wie sich aus Normal- und Quasinormalbasen eines Moduls M Basen gewisser aus M abgeleiteter Moduln ergeben.

Definition 1.2.9 *Ein Modul M definiert die beiden Moduln*

- $M_- := M/\ker_M(1-\sigma)$,
- $M_+ := M/\ker_M(1+\sigma)$.

Lemma 1.2.10 *Für eine Normalbasis $B = [E^0, E^+, E^-]$ eines Moduls M gilt:*

a) i) $E^0 \cup E^+$ *induziert eine Basis von* M_+,
   ii) $E^0 \cup E^-$ *induziert eine Basis von* M_-,

b) i) $(1+\sigma)E^0 \cup E^+$ *ist eine Basis von* $\ker_M(1-\sigma)$,
   ii) $(1-\sigma)E^0 \cup E^-$ *ist eine Basis von* $\ker_M(1+\sigma)$,

c) i) E^- *erzeugt die Torsionsgruppe von* $M/(1-\sigma)M$, *das heißt, die Torsionselemente sind von der Form* $\sum_{e\in E^-} \delta_e e + (1-\sigma)M$ *mit* $\delta_e \in \{0,1\}$. *Der torsionsfreie Anteil von* $M/(1-\sigma)M$ *ist isomorph zu* M_+.
   ii) E^+ *erzeugt die Torsionsgruppe von* $M/(1+\sigma)M$, *das heißt, die Torsionselemente sind von der Form* $\sum_{e\in E^+} \delta_e e + (1+\sigma)M$ *mit* $\delta_e \in \{0,1\}$. *Der torsionsfreie Anteil von* $M/(1+\sigma)M$ *ist isomorph zu* M_-.

Teil a gilt sogar, wenn B bloß eine Quasinormalbasis ist.

Beweis
Wir zeigen jeweils den i-Teil, die Teile ii folgen analog.

Zu a: Die Multiplikation mit $(1+\sigma)$ ist ein Epimorphismus von M nach $(1+\sigma)M$. Direkt durch Multiplikation von B mit $(1+\sigma)$ erhält man, daß $(1+\sigma)E^0 \cup 2E^+$ ein Erzeugendensystem von $(1+\sigma)M$ ist. Offensichtlich ist $(1+\sigma)E^0 \cup 2E^+$ auch linear unabhängig. Durch Herausfaktorisieren des Kerns des Epimorphismus erhält man $M_+ = M/\ker_M(1+\sigma) \cong (1+\sigma)M$, und es folgt Teil a, i.

Zu b: Es seien nun $M^+ = \langle E^+ \rangle$, $M^- = \langle E^- \rangle$ und $M^0 = \langle E^0 \cup \sigma E^0 \rangle$. Unmittelbar ist $M^+ \subseteq \ker_M(1-\sigma)$ und $M^- \cap \ker_M(1-\sigma) = \{0\}$ klar. Mit Lemma 1.2.3 rechnet man $M^0 \cap \ker_M(1-\sigma) = (1+\sigma)M^0$ nach, und zusammengenommen beweist dies den Teil b, i: Schreiben wir nämlich $m \in \ker_M(1-\sigma)$ als $m = a^0 + a^+ + a^-$ mit $a^x \in M^x$ für $x \in \{0,+,-\}$, so folgt aus $(1-\sigma)m = 0$, daß $a^- = 0$ und $a^0 \in (1+\sigma)M^0$ liegt.

Zu c: Aus den Teilen a, i und b, ii erhalten wir nach Bemerkung 1.1.2 die Zerlegung

$$M = \langle E^0 \cup E^+ \rangle \oplus \ker_M(1+\sigma), \tag{10}$$

also $M \cong M_+ \oplus \ker_M(1+\sigma)$. Faktorisieren wir in (10) auf beiden Seiten $(1-\sigma)M$ heraus, so erhalten wir nach dem Beweis von Lemma 1.2.4 den Isomorphismus

$$M/(1-\sigma)M \cong M_+ \oplus M^-/2M^-. \tag{11}$$

Dies beweist Teil c, i.

Für Quasinormalbasen wähle man zunächst eine assoziierte Normalbasis und tausche die Normalbasiselemente dann gegen Quasinormalbasiselemente aus.

QED.

Bemerkung 1.2.11 *Wie im Beweis von Lemma 1.2.10, a schon erwähnt, erhält man aus einer Normalbasis $[E^0, E^+, E^-]$ eines Moduls M zum einen die Basis $(1+\sigma)E^0 \cup 2E^+$ von $(1+\sigma)M$ und zum anderen $(1-\sigma)E^0 \cup 2E^-$ als Basis von $(1-\sigma)M$. Insbesondere impliziert dies die Formel*

$$\operatorname{rg} M = \operatorname{rg}(1+\sigma)M + \operatorname{rg}(1-\sigma)M, \tag{12}$$

zeigt aber auch, daß M im allgemeinen nicht die direkte Summe von $(1+\sigma)M$ und $(1-\sigma)M$ ist.

1.3 $\mathbf{Z}[\sigma]$-Moduln und Tensorprodukte

In diesem Abschnitt betrachten wir die folgende Situation. Auf dem Tensorprodukt $M \otimes L$ zweier Moduln M und L lassen wir $\mathbf{Z}[\sigma]$ diagonal operieren, das heißt, zu $g \in \mathbf{Z}[\sigma]$ sei $g(m \otimes l) := gm \otimes gl$. Wir klären zunächst, wie sich eine Normalzerlegung unter dem Tensorprodukt verhält. Anschließend übertragen wir diese Überlegungen auf Normalbasen.

1.3.1 Normalzerlegung und Tensorprodukte

Wir betrachten als erstes die Situation in den Fällen der einfachsten $\mathbf{Z}[\sigma]$-Moduln.

Lemma 1.3.1 *Es operiere σ auf $\mathbf{Z}[\sigma]$ durch Multiplikation, auf $\mathbf{Z}^+ \cong \mathbf{Z}$ durch Identität und auf $\mathbf{Z}^- \cong \mathbf{Z}$ durch Negation. Dann ist die Normalzerlegung der möglichen Tensorprodukte zwischen jeweils zwei dieser Moduln gegeben durch*

a) $\mathbf{Z}[\sigma] \otimes \mathbf{Z}[\sigma] \cong \mathbf{Z}[\sigma] \oplus \mathbf{Z}[\sigma]$,

b) $\mathbf{Z}[\sigma] \otimes \mathbf{Z}^{\pm} \cong \mathbf{Z}^{\pm} \otimes \mathbf{Z}[\sigma] \cong \mathbf{Z}[\sigma]$,

c) $\mathbf{Z}^+ \otimes \mathbf{Z}^+ \cong \mathbf{Z}^- \otimes \mathbf{Z}^- \cong \mathbf{Z}^+$,

d) $\mathbf{Z}^+ \otimes \mathbf{Z}^- \cong \mathbf{Z}^- \otimes \mathbf{Z}^+ \cong \mathbf{Z}^-$.

Beweis

Zu a: Ist $E^0 = \{1 \otimes 1, 1 \otimes \sigma\}$, so ist $[E^0, \emptyset, \emptyset]$ eine Normalbasis von $\mathbf{Z}[\sigma] \otimes \mathbf{Z}[\sigma]$.

Zu b: Mit $E^0 = \{1 \otimes 1\}$ ist in allen Fällen $[E^0, \emptyset, \emptyset]$ eine Normalbasis.

Zu c: Mit $E^+ = \{1 \otimes 1\}$ ist hier $[\emptyset, E^+, \emptyset]$ eine Normalbasis.

Zu d: Mit $E^- = \{1 \otimes 1\}$ ist $[\emptyset, \emptyset, E^-]$ eine Normalbasis.

QED.

Mit Hilfe von Lemma 1.3.1 läßt sich auf Grund der Distributivität des Tensorproduktes die Normalzerlegung im allgemeinen Fall bestimmen.

Lemma 1.3.2 *Es sei $L = L^0 \oplus L^+ \oplus L^-$ und $M = M^0 \oplus M^+ \oplus M^-$ die Normalzerlegung der beiden Moduln L und M. Dann ist die direkte Summe der drei Moduln*

$$(L \otimes M)^0 := (L^0 \otimes M) + (L \otimes M^0),$$

$$(L \otimes M)^+ := (L^+ \otimes M^+) \oplus (L^- \otimes M^-),$$

$$(L \otimes M)^- := (L^- \otimes M^+) \oplus (L^+ \otimes M^-)$$

eine Normalzerlegung von $L \otimes M$.

Beweis
Man schreibe $L^0 \cong \mathbf{Z}[\sigma]^{m^0(L)}$, $M^0 \cong \mathbf{Z}[\sigma]^{m^0(M)}$, $L^+ \cong (\mathbf{Z}^+)^{m^+(L)}$, $M^+ \cong (\mathbf{Z}^+)^{m^+(M)}$, $L^- \cong (\mathbf{Z}^-)^{m^-(L)}$ und $M^- \cong (\mathbf{Z}^-)^{m^-(M)}$, multipliziere die direkten Summen distributiv aus, und wende Lemma 1.3.1 an.
Insbesondere Für $(L \otimes M)^0$ erhält man den länglichen Ausdruck

$$(L \otimes M)^0 = (L^0 \otimes M^0) \oplus (L^0 \otimes M^+) \oplus (L^0 \otimes M^-) \oplus (L^+ \otimes M^0) \oplus (L^- \otimes M^0), \quad (13)$$

der sich zur (nicht direkten) Summe $(L^0 \otimes M) + (L \otimes M^0)$ zusammenfassen läßt.

QED.

Lemma 1.3.2 impliziert einfache Formeln für die Invarianten m^+ und m^- eines $\mathbf{Z}[\sigma]$-Moduls.

Korollar 1.3.3 *Für zwei Moduln L und M gilt*

a) $m^+(L \otimes M) = m^+(L)m^+(M) + m^-(L)m^-(M)$,

b) $m^-(L \otimes M) = m^-(L)m^+(M) + m^+(L)m^-(M)$.

Der Satz für Normalzerlegungen weist den Weg für Normalbasen.

1.3.2 Normalbasen unter Tensorprodukten

Wir zeigen zunächst, wie sich Normalbasen unter Tensorproduktbildung verhalten. Später werden wir einen entsprechenden Satz für Quasinormalbasen aufstellen.

Satz 1.3.4 *Es sei $[E^0, E^+, E^-]$ eine Normalbasis eines Moduls L, und es sei $[F^0, F^+, F^-]$ eine Normalbasis eines Moduls M. Es sei ferner $E^* := E^+ \cup E^-$ und $F^* := F^+ \cup F^-$. Definieren wir*

i) $G^0 := (E^0 \times F^0) \cup (E^0 \times \sigma F^0) \cup (E^0 \times F^*) \cup (E^* \times F^0)$,

ii) $G^+ := (E^+ \times F^+) \cup (E^- \times F^-)$,

iii) $G^- := (E^+ \times F^-) \cup (E^- \times F^+)$,

dann induziert $[G^0, G^+, G^-]$ eine Normalbasis von $L \otimes M$.
Mit anderen Worten, das Bild von $G^0 \cup \sigma G^0 \cup G^+ \cup G^-$ unter der Abbildung $L \times M \to L \otimes M$ ist eine Normalbasis von $L \otimes M$.

Beweis
Der Satz ist eine Übertragung von Lemma 1.3.2 auf Basen. Wir zeigen, wie dies im einzelnen aussieht. Schreiben wir

$$L^0 := \langle E^0 \cup \sigma E^0 \rangle, \quad L^+ := \langle E^+ \rangle, \quad L^- := \langle E^- \rangle,$$

und

$$M^0 := \langle F^0 \cup \sigma F^0 \rangle, \quad M^+ := \langle F^+ \rangle, \quad M^- := \langle F^- \rangle,$$

so sieht man mit Lemma 1.3.2 und Lemma 1.1.5, daß zum einen G^+ eine Basis von $(L \otimes M)^+$ und zum anderen G^- eine Basis von $(L \otimes M)^-$ induziert.
Daß $G^0 \cup \sigma G^0$ eine Basis von $(L \otimes M)^0$ induziert, sieht man beispielsweise mit Hilfe der Zerlegung von $(L \otimes M)^0$ gemäß (13) ein: Wir stellen dazu die folgende Tabelle auf. Die Vereinigung der paarweise disjunkten Mengen in der linken Spalte ergibt $G^0 \cup \sigma G^0$, die rechte Spalte ist eine direkte Summenzerlegung

von $(L \otimes M)^0$ nach (13). Dabei induziert die jeweils linke Seite eine Basis des Moduls auf der rechten Seite.

$$\begin{array}{ll} (E^0 \cup \sigma E^0) \times (F^0 \cup \sigma F^0) & L^0 \otimes M^0 \\ (E^0 \cup \sigma E^0) \times F^+ & L^0 \otimes M^+ \\ E^+ \times (F^0 \cup \sigma F^0) & L^+ \otimes M^0 \\ (E^0 \times F^-) \cup (\sigma E^0 \times \sigma F^-) & L^0 \otimes M^- \\ (E^- \times F^0) \cup (\sigma E^- \times \sigma F^0) & L^- \otimes M^0 \end{array} \tag{14}$$

Nur die letzten beiden Zeilen folgen nicht direkt aus Lemma 1.1.5. Es gilt aber beispielsweise in der vorletzten Zeile $\sigma F^- = \{-f;\ f \in F^-\}$, also erzeugen $\sigma E^0 \times \sigma F^-$ und $\sigma E^0 \times F^-$ den gleichen Modul, und es gilt

$$\langle (E^0 \times F^-) \cup (\sigma E^0 \times \sigma F^-) \rangle = \langle (E^0 \cup \sigma E^0) \times F^- \rangle = L^0 \otimes M^-. \tag{15}$$

Für die letzte Zeile argumentiert man analog.

QED.

Bemerkung 1.3.5 *Nach der Konstruktion in Satz 1.3.4 liegt $E^0 \times \sigma F^0$ in G^0, jedoch nicht $\sigma E^0 \times F^0$. Dadurch wird die Konstruktion unsymmetrisch in L und M. Dies läßt sich letztendlich nicht vermeiden, da eine und nur eine der Mengen $\sigma E^0 \times F^0$ oder $E^0 \times \sigma F^0$ in G^0 aufgenommen werden muß, um eine Normalbasis zu erhalten.*

Satz 1.3.6 *Satz 1.3.4 gilt genauso, wenn man "Normalbasis" durch "Quasinormalbasis" ersetzt.*

Beweis
Wir zeigen zuerst ähnlich wie im Beweis zu Satz 1.3.4, daß $[G^0, G^+, G^-]$ Basis ist, anschließend rechnen wir die Quasinormalbasiseigenschaften explizit nach. Wie in Satz 1.3.4 seien $E^* := E^+ \cup E^-$ und $F^* := F^+ \cup F^-$. Wir definieren

$$L^0 = \langle E^0 \cup \sigma E^0 \rangle, \quad L^* = \langle E^* \rangle,$$

und

$$M^0 = \langle F^0 \cup \sigma F^0 \rangle, \quad M^* = \langle F^* \rangle,$$

und erhalten die Zerlegungen $L = L^0 \oplus L^*$ und $M = M^0 \oplus M^*$.

Im Unterschied zum Beweis für Normalbasen sind nun allerdings nicht mehr notwendig $\sigma E^* \subseteq L^*$ und $\sigma F^* \subseteq M^*$. Es ist aber immerhin σE^* eine Basis von L^* modulo L^0 und σF^* eine Basis von M^* modulo M^0. Dies führt zu der folgenden Tabelle: Die Mengen der linken Spalte sind paarweise disjunkt, und vereinigen sich zu $G^0 \cup \sigma G^0 \cup G^+ \cup G^-$, die mittlere Spalte ist eine direkte Summenzerlegung von $L \otimes M$. Die Menge in der linken Spalte induziert eine Basis des Moduls in der mittleren Spalte modulo dem Modul in der rechten Spalte.

$$\begin{array}{lll} (E^0 \cup \sigma E^0) \times (F^0 \cup \sigma F^0) & L^0 \otimes M^0 & \\ (E^0 \times F^*) \cup (\sigma E^0 \times \sigma F^*) & L^0 \otimes M^* & \text{modulo } L^0 \otimes M^0 \\ (E^* \times F^0) \cup (\sigma E^* \times F^0) & L^* \otimes M^0 & \text{modulo } L^0 \otimes M^0 \\ E^* \times F^* & L^* \otimes M^* & \end{array} \tag{16}$$

Es bleiben noch die Quasinormalbasiseigenschaften zu zeigen. Das heißt, es ist zu zeigen, daß $\sigma g \equiv g \bmod (L \otimes M)^0$ für $g \in G^+$ und $\sigma g \equiv -g \bmod (L \otimes M)^0$ für $g \in G^-$ gilt. Sei also beispielsweise $g \in G^+$ und insbesondere $g = e \otimes f$ mit $e \in E^+$ und $f \in F^+$ (die anderen Fälle behandelt man analog). Dann gilt

$$\begin{aligned} \sigma(e \otimes f) &= \sigma e \otimes \sigma f \equiv e \otimes \sigma f \mod L^0 \otimes M \\ &\equiv e \otimes f \mod L \otimes M^0. \end{aligned} \tag{17}$$

QED.

1.3.3 Mehrfache Tensorprodukte von $\mathbf{Z}[\sigma]$-Moduln

In den letzten Abschnitten wurde das Verhalten von jeweils zwei Moduln L und M untersucht. Hat man mehrere Moduln $L_1, \ldots, L_r$, die tensoriert werden, so erhält man eine Normalbasis von $L := L_1 \otimes \cdots \otimes L_r$ induktiv aus der Konstruktion für zwei Moduln. Wir wollen im folgenden diese Situation näher untersuchen.

Definieren wir $L_i^* := L_i^+ \oplus L_i^-$, so folgt mit $x = (x_1, \ldots, x_r)$ aus der Distributivität des Tensorproduktes

$$L = \bigotimes_{i=1}^{r} (L_i^0 \oplus L_i^*) = \bigoplus_{x \in \{0,*\}^r} (L_1^{x_1} \otimes \cdots \otimes L_r^{x_r}). \tag{18}$$

Wir untersuchen nun L^0 und L^* näher.

Zu L^*: Zunächst erhält man induktiv aus Lemma 1.3.2, daß $L^* = (L_1^* \otimes \cdots \otimes L_r^*)$ ist. Enthält $W \subseteq \{+,-\}^r$ genau die Vorzeichentupel, in denen das Minuszeichen in gerader Anzahl vorkommt, und ist $W^c := \{+,-\}^r \setminus W$, so gilt

$$L^+ = \bigoplus_{x \in W} (L_1^{x_1} \otimes \cdots \otimes L_r^{x_r}) \quad \text{und} \quad L^- = \bigoplus_{x \in W^c} (L_1^{x_1} \otimes \cdots \otimes L_r^{x_r}). \tag{19}$$

Wir formulieren zwei Spezialfälle, die später im Zusammenhang mit Kreiseinheiten auftreten werden, als Lemma.

Lemma 1.3.7 *Es sei $L = L_1 \otimes \cdots \otimes L_r$.*

a) *Ist $L_i^* = 0$ für mindestens ein $i \in \{1, \ldots, r\}$, dann ist $L^+ = L^- = 0$.*

b) *Ist $L_i^+ = 0$ für alle $i \in \{1, \ldots, r\}$, so ist*

- *im Fall, daß r gerade ist: $L^+ = L_1^- \otimes \cdots \otimes L_r^-$ und $L^- = 0$,*
- *im Fall, daß r ungerade ist: $L^- = L_1^- \otimes \cdots \otimes L_r^-$ und $L^+ = 0$.*

Beweis
Teil a folgt sofort aus $L^* = L_1^* \otimes \cdots \otimes L_r^*$ und Teil b aus Gleichung (19).

QED.

Zu L^0: In der rechten Seite von (18) gehören alle Summanden bis auf einen, nämlich $L^* = L_1^* \otimes \cdots \otimes L_r^*$ zum L^0-Teil. Man kann die Summanden beispielsweise auf folgende Weise zusammenfassen:

$$L^0 = \bigoplus_{i=1}^{r} (L_1^* \otimes \cdots \otimes L_{i-1}^* \otimes L_i^0 \otimes L_{i+1} \otimes \cdots \otimes L_r). \tag{20}$$

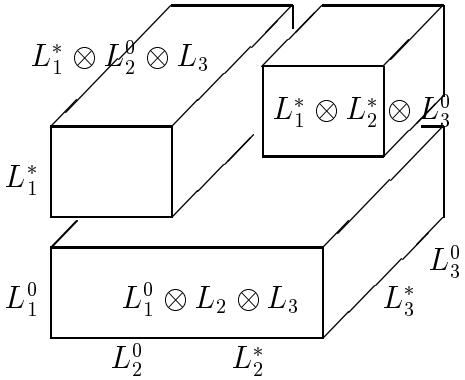
Die direkte Summe, aus der L^0 zusammengesetzt ist, besteht dann nur noch aus r Summanden und nicht mehr aus $2^r - 1$ Summanden wie in (18).

Formal zeigt man (20) durch Induktion nach r. Bezeichnen wir mit M_r die rechte Seite von (20), so folgt aus der Distributivität des Tensorprodukts mit der direkten Summe

$$\begin{aligned} M_r &= \left(\bigoplus_{i=1}^{r-1} (L_1^* \otimes \cdots \otimes L_{i-1}^* \otimes L_i^0 \otimes L_{i+1} \otimes \cdots \otimes L_{r-1}) \right) \otimes L_r \\ &\qquad \oplus (L_1^* \otimes \cdots \otimes L_{r-1}^* \otimes L_r^0) \\ &= (M_{r-1} \otimes L_r) \oplus (L_1^* \otimes \cdots \otimes L_{r-1}^* \otimes L_r^0). \end{aligned} \tag{21}$$

Nach Induktionsannahme ist M_{r-1} gleich der rechten Seite von (18) (mit $r-1$ statt r), wobei jedoch der Summand $L^* = L_1^* \otimes \cdots \otimes L_{r-1}^*$ fehlt. Damit erhält man (20).

Die Zusammenfassung der Summanden aus (18) zu finden läßt sich zumindest für $r \leq 3$ geometrisch interpretieren: Man überdecke einen r-dimensionalen Würfel (den Modul $L = L_1 \otimes \cdots \otimes L_r$), aus dem ein kleinerer Würfel (der Teilmodul $L^* = L_1^* \otimes \cdots \otimes L_r^*$) entfernt wurde, durch (möglichst große) Quader. Im Falle $r = 3$ sähe die Zerlegung wie folgt aus.



Im folgenden Satz zeigen wir, wie die obigen Überlegungen für (Quasi-)Normalbasen aussehen.

Satz 1.3.8 *Gegeben seien die Moduln $L_1, \ldots, L_r$, jeweils mit (Quasi-)Normalbasen*

$$B_i = [E_i^0, E_i^+, E_i^-] = E_i^0 \cup \sigma E_i^0 \cup E_i^+ \cup E_i^- \tag{22}$$

für $i = 1, \ldots, r$, und wir definieren $E_i^* := E_i^+ \cup E_i^-$. Weiter sei $W \subseteq \{+,-\}^r$ die Menge der Vorzeichentupel $x = (x_1, \ldots, x_r)$, in denen das Minuszeichen in gerader Anzahl vorkommt und $W^c := \{+,-\}^r \setminus W$.

Unter diesen Voraussetzungen induziert $[F^0, F^+, F^-]$ mit

i) $F^0 = \bigcup_{i=1}^{r} E_1^* \times \cdots \times E_{i-1}^* \times E_i^0 \times B_{i+1} \times \cdots \times B_r$,

ii) $F^+ = \bigcup_{x \in W} E_1^{x_1} \times \cdots \times E_r^{x_r}$,

iii) $F^- = \bigcup_{x \in W^c} E_1^{x_1} \times \cdots \times E_r^{x_r}$,

eine (Quasi-)Normalbasis von $L = \bigotimes_{i=1}^{r} L_i$.

Beweis
Die Teile i-iii sind eine Übersetzung der Zerlegungen (19) und (20) in Normalbasen. Alternativ kann man Satz 1.3.8 auch direkt über Induktion nach r, und dann mit Satz 1.3.4 beziehungsweise Satz 1.3.6 beweisen.

QED.

Für zwei Spezialfälle, die später im Zusammenhang mit Kreiseinheiten auftreten werden, formulieren wir das dem Lemma 1.3.7 für Normalbasen entsprechende Korollar zu Satz 1.3.8.

Korollar 1.3.9 *In Satz 1.3.8 gilt insbesondere:*

a) *Existiert ein* $i \in \{1, \ldots, r\}$ *mit* $E_i^* = \emptyset$, *beispielsweise* $i = 1$, *so ist* $F^+ = F^- = \emptyset$ *und* $F^0 = E_1^0 \times B_2 \times \cdots \times B_r$.

b) *Ist* $E_i^+ = \emptyset$ *für alle* $i = 1, \ldots, r$, *so ist*

   - *im Fall, daß* r *gerade ist:* $F^+ = E_1^- \times \cdots \times E_r^-$ *und* $F^- = \emptyset$,
   - *im Fall, daß* r *ungerade ist:* $F^- = E_1^- \times \cdots \times E_r^-$ *und* $F^+ = \emptyset$.

   F^0 *ist dabei wie in Satz 1.3.8, iii definiert.*

1.4 Zeilenfaktormoduln

Der Zeilenfaktormodul entsteht als freier Modul über einer Produktmenge $A_1 \times \cdots \times A_r$ modulo dem Erzeugnis der Summen über einzelne Komponenten A_i, die wir als Zeilensummen bezeichnen. Eine exakte Definition wird im ersten Abschnitt gegeben. Anschließend zeigen wir, daß sich ein Zeilenfaktormodul als Tensorprodukt von einfach aufgebauten, sogenannten elementaren Zeilenfaktormoduln auffassen läßt.

Operiert zusätzlich σ auf dem Zeilenfaktormodul, so stellt sich die Frage nach der Konstruktion von Normalbasen und Quasinormalbasen von Zeilenfaktormoduln. Dazu reicht es aus, diese zunächst nur für elementare Zeilenfaktormoduln zu konstruieren und dann die Ergebnisse über Normalbasen und Tensorprodukte anzuwenden.

Die Zeilensummen sind untereinander nicht frei von Relationen. Im letzten Abschnitt werden wir daher die Relationen, die zwischen den Zeilensummen bestehen, genau untersuchen und sogar eine Basis von dem von den Zeilensummen erzeugten Modul angeben.

1.4.1 Definition und Eigenschaften

Definition 1.4.1 *Zu $r \in \mathbf{N}$ sei $A = \prod_{i=1}^{r} A_i$ das endliche Produkt endlicher Mengen und $J \subseteq \{1, \ldots, r\}$.*
Definieren wir $M := \langle A \rangle$ als freies Erzeugnis von A und $R \leq M$ als Erzeugnis der Zeilensummen

$$s_{A_i}(a) := s_{A_i}(a_1, \ldots, a_r) = \sum_{b \in A_i} (a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_r), \tag{23}$$

mit $a \in A$ und $i \in J$, so heißt $Z := M/R$ der Zeilenfaktormodul zu A und J.
Die Mengen A_i heißen Faktoren *von Z, und diejenigen Faktoren A_i mit $i \in J$ nennen wir* echte *Faktoren.*
Ist $r = 1$ so nennen wir Z elementar.

Üblicherweise geben wir bei der Definition eines Zeilenfaktormoduls zu A und J nicht die Menge J an, sondern erklären, welche Faktoren echt sind. Beispielsweise sprechen wir vom Zeilenfaktormodul zu $A \times B$, wobei A echter Faktor und B kein echter Faktor ist.

Bemerkung 1.4.2 *Ist ein Zeilenfaktormodul Z zu einer Menge A elementar, so gibt es genau zwei Möglichkeiten:*

- *A ist kein echter Faktor. Dann ist $Z = \langle A \rangle$, und wir nennen Z* trivialen *elementaren Zeilenfaktormodul zu A.*

  In diesem Fall ist A selbst auch eine Basis von Z.

- *A ist echter Faktor. Dann ist $Z = \langle A \rangle / \langle \sum_{a \in A} a \rangle$, und wir nennen Z den* nichttrivialen *elementaren Zeilenfaktormodul zu A.*

  Ist $a^\sharp \in A$, so ist in diesem Fall $A^\flat := A \setminus \{a^\sharp\}$ eine Basis von Z.

Beispiele für Zeilenfaktormoduln finden sich in Abschnitt 2.1. Die dort definierten Zeilenfaktormoduln werden zu den Kreiseinheiten in Beziehung gesetzt, wobei die Zeilensummen den durch Relativnormen erzeugten Relationen entsprechen.

Von entscheidender Bedeutung ist der folgende Satz, der es erlaubt von elementaren Zeilenfaktormoduln auf beliebige Zeilenfaktormoduln zu schließen.

Satz 1.4.3 *Es sei X ein Zeilenfaktormodul zu $A = A_1 \times \cdots \times A_r$ und Y ein Zeilenfaktormodul zu $B = B_1 \times \cdots \times B_s$. Ist Z der Zeilenfaktormodul mit Faktoren $A_1, \ldots, A_r, B_1, \ldots, B_s$, wobei genau die Faktoren echt sind, die auch schon in X und Y echt waren, dann gilt $Z \cong X \otimes Y$.*

Beweis
Es seien $L = \langle A \rangle$, $M = \langle B \rangle$ und $N = \langle A \times B \rangle$. Weiter seien Q, R und S als Erzeugnis der entsprechenden Zeilensummen definiert, so daß $X = L/Q$, $Y = M/R$ und $Z = N/S$ gilt.

Wir zeigen die Behauptung zunächst unter der Annahme, daß X und Y frei sind. Nach Lemma 1.1.6 ist dann $L/Q \otimes M/R \cong (L \otimes M)/(Q \otimes M + L \otimes R)$.

Wir zeigen $L \otimes M \cong N$ und $Q \otimes M + L \otimes R \cong S$, wobei jeweils $a \otimes b \in L \otimes M$ auf $(a, b) \in N$ abgebildet wird. Der Isomorphismus $L \otimes M \cong N$ folgt sofort mit Lemma 1.1.5.

Ist q eine Zeilensumme aus Q und $m \in M$, so wird $q \otimes m$ auf eine Zeilensumme aus S abgebildet. Also wird $Q \otimes M$ auf S abgebildet. Analog wird auch $L \otimes R$ auf S abgebildet. Somit ist der Homomorphismus $Q \otimes M + L \otimes R \stackrel{\psi}{\to} S$ wohldefiniert. Die Injektivität von ψ ist gegeben, da ψ eine Einschränkung des Isomorphismus $L \otimes M \cong N$ ist. Es bleibt die Surjektivität zu zeigen. Ein Urbild einer Zeilensumme aus S ist aber entweder von der Form $q \otimes m \in Q \otimes M$ oder von der Form $l \otimes r \in L \otimes R$. Da S von Zeilensummen erzeugt wird, folgt die Behauptung.

Bisher wurde gezeigt: Gelten die Voraussetzungen von Satz 1.4.3 und sind X und Y frei, so gilt $Z \cong X \otimes Y$.

Wir zeigen nun durch Induktion nach r, daß X frei ist. Daß Y frei ist, folgt analog durch Induktion nach s. Ist $r = 1$, so ist X elementar und daher offensichtlich frei. Für $r > 1$ sei X' der Zeilenfaktormodul zu $A_1 \times \cdots \times A_{r-1}$ und X'' der elementare Zeilenfaktormodul zu A_r. Nach Induktionsannahme sind X' und X'' frei, also erhalten wir nach dem bisher bewiesenen den Isomorphismus $X \cong X' \otimes X''$. Da das Tensorprodukt zweier freier Moduln nach Lemma 1.1.5 wieder frei ist, ist X frei.

QED.

Durch mehrmalige Anwendung von Satz 1.4.3 erhalten wir das folgende Korollar.

Korollar 1.4.4 *Jeder Zeilenfaktormodul ist das Tensorprodukt elementarer Zeilenfaktormoduln.*

Damit können wir insbesondere eine Basis des Zeilenfaktormoduls angeben.

Lemma 1.4.5 *Es sei Z ein Zeilenfaktormodul zu $A = A_1 \times \cdots \times A_r$. Weiter sei $A_i^\flat := A_i$, falls A_i kein echter Faktor ist, und $A_i^\flat := A_i \setminus \{a_i^\sharp\}$, falls A_i echter Faktor ist mit $a_i^\sharp \in A_i$ jeweils für $i = 1, \ldots, r$. Dann ist Z frei, und*

$$B := A_1^\flat \times \cdots \times A_r^\flat \tag{24}$$

induziert eine Basis von Z.

Beweis
Nach Korollar 1.4.4 ist Z das Tensorprodukt von offensichtlich freien elementaren Zeilenfaktormoduln, deren Basen in Bemerkung 1.4.2 angegeben sind. Durch wiederholte Anwendung von Lemma 1.1.5 folgt, daß B in der Tat Basis ist.

QED.

1.4.2 Normalbasen elementarer Zeilenfaktormoduln

Operiert auf jedem Faktor A_i eines Zeilenfaktormoduls Z zu $A = \prod_{i=1}^{r} A_i$ die zweielementige Gruppe $\{1, \sigma\}$, so setzen wir diese komponentenweise fort auf A. Homomorphes Fortsetzen auf $M = \langle A \rangle$ und anschließendes Herausfaktorisieren des von den Zeilensummen erzeugten Moduls R macht Z zum $\mathbf{Z}[\sigma]$-Modul. Damit stellt sich die Frage nach Normalbasen von Zeilenfaktormoduln.

Da wir jeden Zeilenfaktormodul als Tensorprodukt elementarer Zeilenfaktormoduln identifiziert haben, kann man sich bei der Konstruktion von Normalbasen von Zeilenfaktormoduln auf elementare Zeilenfaktormoduln zurückziehen, dort Normalbasen konstruieren und die Aussagen über Tensorprodukte und Normalbasen aus Abschnitt 1.3 anwenden, um eine Normalbasis eines beliebigen Zeilenfaktormoduls zu erhalten. In diesem Abschnitt bestimmen wir daher Normalbasen und Quasinormalbasen für die elementaren Zeilenfaktormoduln.

Operiert $\{1, \sigma\}$ auf einer Menge A, so besitzt diese eine Zerlegung

$$A = E^0 \cup \sigma E^0 \cup E^+ \tag{25}$$

in paarweise disjunkte Mengen mit $\sigma e = e$ für $e \in E^+$, die wir im folgenden *Normalzerlegung* nennen, und mit $[E^0, E^+]$ bezeichnen. Für den trivialen elementaren Zeilenfaktormodul $\langle A \rangle$ ist dann schon $[E^0, E^+, \emptyset]$ eine Normalbasis. Den nichttrivialen elementaren Zeilenfaktormodul beschreibt das folgende Lemma.

Lemma 1.4.6 *Aus einer Normalzerlegung $[E^0, E^+]$ einer Menge A erhält man eine in $\langle A \rangle$ lebende Normalbasis $[F^0, F^+, F^-]$ des nichttrivialen elementaren Zeilenfaktormoduls $\langle A \rangle / \langle \sum_{a \in A} a \rangle$ durch die folgenden Definitionen.*

1. *Fall: $E^+ \neq \emptyset$. Zu einem $e \in E^+$ sei*
   $$F^0 := E^0, \qquad F^+ := E^+ \setminus \{e\}, \qquad F^- := \emptyset.$$
2. *Fall: $E^+ = \emptyset$. Zu einem $e \in E^0$ sei*
   $$F^0 := E^0 \setminus \{e\}, \qquad F^+ := \emptyset, \qquad F^- := \{\textstyle\sum_{d \in E^0} d\}.$$

Ersetzt man im 2. Fall F^- durch $\widetilde{F^-} := \{e\}$, so ist $[F^0, F^+, \widetilde{F^-}]$ eine Quasinormalbasis.

Beweis
Es sei $B = [F^0, F^+, F^-]$. Offensichtlich ist $|B| = |A| - 1$, also gleich dem Rang des Zeilenfaktormoduls $\langle A\rangle/\langle\sum_{a\in A} a\rangle$.

Es reicht daher zu zeigen, daß B Erzeugendensystem von Z ist, was im 1. Fall trivial ist. Im 2. Fall ist zu zeigen, daß die Elemente e und σe von B erzeugt werden. Schreiben wir $f := \sum_{d\in E^0} d$, so folgt dies aus den beiden Relationen $e = f - \sum_{d\in F^0} d$ und $\sigma e = -f - \sum_{d\in\sigma F^0} d$. Daß B nicht nur Basis, sondern sogar Normalbasis ist, rechnet man direkt nach. Ebenso rechnet man den Zusatz zum zweiten Fall, daß $B = [F^0, F^+, \widetilde{F^-}]$ eine Quasinormalbasis ist, nach.

QED.

Der Vorteil der Quasinormalbasis im Gegensatz zur Normalbasis liegt darin, daß die Basis ganz aus Elementen des Erzeugendensystems A gewählt werden kann.

Da ein beliebiger Zeilenfaktormodul nach Korollar 1.4.4 als Tensorprodukt elementarer Zeilenfaktormoduln identifiziert werden kann, läßt sich nun auch mit Hilfe der Maschinerie aus Abschnitt 1.3 eine Basis eines beliebigen Zeilenfaktormoduls konstruieren. In Abschnitt 2.1 wird dies am Beispiel des Kreismoduls ausführlich vorgeführt.

1.4.3 Die Relationen der Zeilensummen

Es sei $Z = M/R$ ein Zeilenfaktormodul zu $A = \prod_{i=1}^r A_i$. Wir nehmen im folgenden an, daß alle Faktoren echt sind (unechte Faktoren stören die folgenden Überlegungen nicht, erschweren aber die Lesbarkeit). Um Doppelindizes zu vermeiden schreiben wir im folgenden $s_i(a)$ für die Zeilensumme $s_{A_i}(a)$ für $i = 1, \ldots, r$ und $a \in A$. Die Zeilensummen genügen für beliebige $a_i \in A_i$ und $1 \le i, j \le r$ offensichtlich der Relation

$$\sum_{b\in A_i} s_j(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_r) = \sum_{c\in A_j} s_i(a_1, \ldots, a_{j-1}, c, a_{j+1}, \ldots, a_r). \quad (26)$$

Dies ist in der Tat die einzige Relation, die zwischen den Zeilensummen besteht.

Um dies zu zeigen, geben wir eine Basis der Zeilensummen an, und zeigen dabei, daß zur Erzeugung der Zeilensummen, die nicht in der Basis liegen, ausschließlich Relationen aus (26) benutzt werden. Im Anschluß an den folgenden Satz zeigen wir dann, wie dieses Ergebnis in die Darstellbarkeit der Zeilenfaktormoduln als Tensorprodukt elementarer Zeilenfaktormoduln hineinpaßt.

Satz 1.4.7 *Zu $i = 1, \ldots, r$ sei jeweils $a_i^\sharp \in A_i$ fest gewählt. Dann ist*

$$C := \bigcup_{i=1}^r \{s_i(a_1, \ldots, a_r);\ (a_1, \ldots, a_r) \in A,\ a_j \ne a_j^\sharp \text{ für } i < j \le r\} \quad (27)$$

eine Basis von R, und diejenigen Zeilensummen, die nicht in der Basis C liegen, werden mit Hilfe von Relationen vom Typ (26) von C erzeugt.

Beweis
R ist als Teilmodul von M torsionsfrei. Um zu zeigen, daß C Basis ist, reicht es zu zeigen, daß C ein Erzeugendensystem und $|C| = \operatorname{rg} R$ ist. Dabei verwenden wir im Beweis nur die Relationen vom Typ (26). Für $i = 1, \ldots, r$ sei im folgenden $A_i^\flat := A_i \setminus \{a^\sharp\}$.

C ist Erzeugendensystem: Wir ordnen jeder Zeilensumme $\xi := s_i(a_1, \ldots, a_r)$ den Wert $\tau(\xi) := \max(\{0\} \cup \{j;\ a_j = a_j^\sharp\})$ zu, und wenden Induktion nach $\tau(\xi)$ an. Ist $\tau(\xi) = 0$, so liegt ξ in C. Nehmen wir nun an, daß alle Zeilensummen ξ' mit $\tau(\xi') < \tau(\xi)$ von C erzeugt werden.

Relation (26) liefert

$$\xi = s_i(a_1, \ldots, a_r) = \sum_{b \in A_i} s_{\tau(\xi)}(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_r) - \sum_{c \in A^\flat_{\tau(\xi)}} s_i(a_1, \ldots, a_{\tau(\xi)-1}, c, a_{\tau(\xi)+1}, \ldots, a_r) \tag{28}$$

Die Summanden $s_{\tau(\xi)}(a_1, \ldots, a_r)$, jeweils mit $a_i = b$ in der ersten Summe, liegen alle in C, denn es ist $a_{\tau(\xi)+1} \neq a^\sharp_{\tau(\xi)+1}$, $\ldots$, $a_r \neq a_r^\sharp$ nach der Definition von $\tau(\xi)$.

Die Summanden $\xi' := s_i(a_1, \ldots, a_r)$, jeweils mit $a_{\tau(\xi)} = c$ aus der zweiten Summe werden nach der Induktionsannahme von C erzeugt: Es ist $a_{\tau(\xi)} \neq a^\sharp_{\tau(\xi)}$, und daher $\tau(\xi') < \tau(\xi)$.

$\operatorname{rg} R = |C|$: Interpretieren wir Z als Tensorprodukt elementarer Zeilenfaktormoduln, so erhalten wir $\operatorname{rg} Z = \prod_{i=1}^r (|A_i| - 1)$. Es ist weiter $\operatorname{rg} M = \prod_{i=1}^r |A_i|$, und wir erhalten $\operatorname{rg} R = \operatorname{rg} M - \operatorname{rg} Z$.

Definieren wir $B := A_1^\flat \times \cdots \times A_r^\flat$, so ist $H := A \setminus B$ eine Menge der Mächtigkeit $\operatorname{rg} R$. Wir geben eine Bijektion von C nach H an.

Es besteht H aus genau den r-Tupeln $(a_1, \ldots, a_r)$, die in mindestens einer der Komponenten ein Element $a_i = a_i^\sharp$ stehen haben. Eine Bijektion $C \to H$ ist gegeben durch

$$s_i(a_1, \ldots, a_r) \mapsto (a_1, \ldots, a_{i-1}, a_i^\sharp, a_{i+1}, \ldots, a_r). \tag{29}$$

Die Umkehrabbildung ordnet dabei jedem $a = (a_1, \ldots, a_r)$ diejenige Summe $s_i(a)$ zu, für die i maximal ist mit $a_i = a_i^\sharp$.

QED.

Wir wollen im folgenden noch ohne Beweis erläutern, wie die Doppelsummen im Zusammenhang mit der Interpretation der Zeilenfaktormoduln als Tensorprodukte zu verstehen sind.

Haben wir $Z \cong X \otimes Y$ mit Zeilenfaktormoduln X, Y und Z, und schreiben wir $X = L/Q$ und $Y = M/R$, so ist, wie im Beweis zu Satz 1.4.3 gezeigt,

$Z \cong (L \otimes M)/(Q \otimes M + L \otimes R)$. Die Summe in $Q \otimes M + L \otimes R$ ist nicht direkt, sondern es gilt $(Q \otimes M) \cap (L \otimes R) = Q \otimes R$. Da sowohl Q als auch R von Zeilensummen erzeugt werden, wird $Q \otimes R$ von Tensorprodukten jeweils zweier Zeilensummen erzeugt. Dies entspricht gerade den Doppelsummen.

Zum Schluß dieses Abschnittes sei noch angemerkt, daß sich zeigen läßt, daß die Relationen, die zwischen den Doppelsummen bestehen, gerade die Dreifachsummen sind usw, das heißt, die Relationen, die innerhalb der n-fach-Summen bestehen, werden gerade von den $(n+1)$-fach-Summen gebildet.

1.5 Differenzenmoduln

Bei der Behandlung von Gruppenringen RG einer Gruppe G über einem Ring R spielt der Augmentationshomomorphismus eine besondere Rolle. Dieser ordnet einem Element $\sum a_g g$ aus RG die Summe $\sum a_g \in R$ zu (siehe Abschnitt 1.1.5 in [2]). Der Kern dieses Homomorphismus bildet einen Teilmodul ΔRG, der beispielsweise von $\{g - g';\ g, g' \in G\}$ erzeugt wird.

Dies läßt sich in offensichtlicher Weise auf beliebige Moduln N verallgemeinern. Zu einer Menge $E \subseteq N$ betrachte man den Teilmodul

$$\Delta_E N := \langle e - e';\ e, e' \in E \rangle \leq N. \tag{30}$$

In den nächsten Abschnitten untersuchen wir solche Moduln $\Delta_E N$. Dabei betrachten wir zunächst den "klassischen" Fall, daß E eine Basis von N ist und daran anschließend den Fall, daß E nur ein Erzeugendensystem von N ist. Im darauffolgenden Abschnitt übertragen wir die für $\mathbf{Z}$-Moduln erhaltenen Ergebnisse auf $\mathbf{Z}[\sigma]$-Moduln.

Abschließend behandeln wir dann den Fall, daß N ein gewisser Zeilenfaktormodul ist, der später im Zusammenhang mit Kreiseinheiten wichtig ist.

1.5.1 Der Augmentationshomomorphismus

Der Augmentationshomomorphismus taucht in der Regel im Zusammenhang mit Gruppenringen auf und wird dann auf diesen auch definiert. Zur vernünftigen Definition der Augmentation reichen jedoch schon ein Modul und eine Basis dieses Moduls aus.

Definition 1.5.1 *Es sei M ein Modul mit Basis B. Dann heißt der Homomorphismus*

$$\mathrm{aug}\colon M \to \mathbf{Z},\ \sum_{b \in B} \alpha_b b \mapsto \sum_{b \in B} \alpha_b \tag{31}$$

Augmentationshomomorphismus.

Der Teilmodul $\ker_M \mathrm{aug}$ *aller Elemente von M mit Augmentation Null wird mit ΔM bezeichnet.*

Es sei angemerkt, daß aug und Δ wesentlich von der Basis B abhängen, so daß eigentlich aug_B und Δ_B zu schreiben wäre. Im folgenden ist aber immer klar, welche Basis gemeint ist, so daß wir Δ und aug nicht mit der Basis indizieren.
Eine Basis von ΔM ist wie folgt gegeben.

Lemma 1.5.2 *Es sei M ein Modul mit Basis B. Weiter sei $b^\sharp \in B$ und $B^\flat := B \setminus \{b^\sharp\}$. Dann ist*

$$B' := \{b - b^\sharp;\ b \in B^\flat\} \tag{32}$$

eine Basis von ΔM.

<u>*Beweis*</u>
Offensichtlich ist $B' \cup \{b^\sharp\}$ eine Basis von M. Schreiben wir $m \in \Delta M$ als

$$m = \alpha_{b^\sharp} b^\sharp + \sum_{b \in B^\flat} \alpha_b (b - b^\sharp) \tag{33}$$

mit $\alpha_b \in \mathbf{Z}$, so zeigt die Anwendung von aug auf (33), daß $\alpha_{b^\sharp} = 0$ ist.

QED.

Insbesondere folgt aus Lemma 1.5.2, daß der Index $[M : \Delta M] = \infty$ ist.

Im nächsten Abschnitt 1.5.2 brauchen wir den größten gemeinsamen Teiler über alle Augmentationen der Elemente eines Teilmoduls $R \leq M$. Wir untersuchen diesen Wert im folgenden genauer.

Lemma 1.5.3 *Es sei M ein Modul mit Basis B und $R \leq M$ ein Teilmodul von M, und R besitze zumindest ein Element, das nicht in ΔM liegt. Dann existiert $r \in R$ mit* $\mathrm{aug}(r) = \gcd \mathrm{aug}(R)$.

<u>*Beweis*</u>
Es sei $r \in R$ ein Element mit minimaler positiver Augmentation. Da $r \in R$ liegt, ist $\gcd \mathrm{aug}(R)$ ein Teiler von $\mathrm{aug}(r)$.

Es ist noch zu zeigen, daß $\mathrm{aug}(r) | \mathrm{aug}(r')$ für alle $r' \in R$ gilt. Denn dann gilt auch, daß $\mathrm{aug}(r)$ den größten gemeinsamen Teiler über alle Augmentationen von R teilt. Somit ist $\mathrm{aug}(r)$ gleich diesem.

Existiert $r' \in R$ mit $\mathrm{aug}(r) \nmid \mathrm{aug}(r')$, dann hat $\rho = \gcd(\mathrm{aug}(r), \mathrm{aug}(r'))$ eine Darstellung $\rho = \alpha\,\mathrm{aug}(r) + \beta\,\mathrm{aug}(r')$ mit $\alpha, \beta \in \mathbf{Z}$. Damit ist aber $\alpha r + \beta r' \in R$ ein Element mit positiver Augmentation $\rho < \mathrm{aug}(r)$, was ein Widerspruch zur Minimalität von $\mathrm{aug}(r)$ ist.

QED.

Explizit berechnen kann man $\gcd \mathrm{aug}(R)$ über ein Erzeugendensystem von R.

Lemma 1.5.4 *Ist $E \subseteq R$ ein Erzeugendensystem von R, so gilt* $\gcd \mathrm{aug}(R) = \gcd \mathrm{aug}(E)$.

Beweis
Ist $r \in R$ ein Element mit $\operatorname{aug}(r) = \gcd \operatorname{aug}(R)$, so kann man $r = \sum_{e \in E} \alpha_e e$ schreiben und erhält $\operatorname{aug}(r) = \sum_{e \in E} \alpha_e \operatorname{aug}(e)$. Für den größten gemeinsamen Teiler von Zahlen $a_1, \ldots, a_r$ und b gilt $\gcd(a_1, \ldots, a_r, b) = \gcd(a_1, \ldots, a_r)$, wenn b eine Linearkombination der a_i ist. Damit erhalten wir

$$\gcd \operatorname{aug}(R) = \operatorname{aug}(r) = \gcd(\operatorname{aug}(E) \cup \{\operatorname{aug}(r)\}) = \gcd \operatorname{aug}(E). \tag{34}$$

QED.

1.5.2 Konstruktion von Basen

Es sei M ein Modul mit Basis B. Weiter sei $R \leq M$ ein Teilmodul, so daß $N = M/R$ frei ist.

Im letzten Abschnitt definierten und untersuchten wir den Augmentationshomomorphismus $\operatorname{aug} : M \to \mathbf{Z}$, $\sum \alpha_b b \mapsto \sum \alpha_b$, dessen Kern ΔM von der Menge $\{b - b';\ b, b' \in B\}$ erzeugt wird. (Dabei kann b' auch fest gewählt werden.) In Analogie dazu definieren wir den Teilmodul ΔN von N.

Definition 1.5.5 *Es sei M ein Modul, $R \leq M$ ein Teilmodul und $N = M/R$ frei. Ist B eine Basis von M, dann heißt der Modul*

$$\Delta N := \langle (b - b') + R;\ b, b' \in B \rangle = (\Delta M + R)/R \tag{35}$$

Differenzenmodul *von $N = M/R$ zu B.*

Hier sei wie in Definition 1.5.1 angemerkt, daß ΔN jeweils von der Basis B abhängt. In der Regel ist aber eindeutig, welche Basis gemeint ist.

Der Index von ΔM in M ist unendlich. Wir beantworten im folgenden diese Frage für $[N : \Delta N]$.

Lemma 1.5.6 *Es sei M ein Modul mit Basis B. Es sei weiter $R \leq M$ Teilmodul, so daß $N = M/R$ frei ist, und es sei ΔN der Differenzenmodul von N zu B. Dann gilt*

$$[N : \Delta N] = \gcd \operatorname{aug}(R), \tag{36}$$

wobei $\gcd\{0\} = \infty$ *zu definieren ist.*

Beweis
Es sei $b_0 \in B$. Da $b \equiv b_0 \bmod \Delta M$ für alle $b \in B$ ist, ist $N/\Delta N$ zyklisch mit Erzeugendem b_0, und der Index $[N : \Delta N]$ ist die kleinste positive Zahl m mit $mb_0 \in R + \Delta M$.

Ist $R \subseteq \Delta M$, das heißt, haben alle Elemente aus R Augmentation Null, so liegt wegen $\mathrm{aug}(mb_0) = m$ kein mb_0 mit $m \neq 0$ in $\Delta M + R$. Der Index ist dann unendlich.

Ansonsten zeigt Lemma 1.5.3, daß $r \in R$ mit Augmentation $\rho := \mathrm{aug}(r) = \gcd \mathrm{aug}(R)$ existiert. Für dieses $r \in R$ gilt $\rho b_0 \equiv r \bmod \Delta M$, somit folgt, daß $\rho b_0 + R \in \Delta N$ ist.

Wäre umgekehrt $\beta b_0 + R \in \Delta N$ mit $0 < \beta < \rho$, so existierte $r' \in R$ mit $r' - \beta b_0 \in \Delta M$. Somit wäre $\mathrm{aug}(r') = \beta < \gcd \mathrm{aug}(R)$, was nicht sein kann.

QED.

Als nächstes betrachten wir die Konstruktion einer Basis von ΔN. Fixieren wir $b^\sharp \in B$, so ist bekanntlich $B' = \{b - b^\sharp;\ b \in B, b \neq b^\sharp\}$ eine Basis von ΔM. Zumindest im Fall $[N : \Delta N] < \infty$ kann schon aus Ranggründen diese Basisbildung nicht zu einer Basis von ΔN führen, da B' ein Element weniger enthält als B. Für ΔN kann man aber zumindest eine ähnliche Konstruktion durchführen, wie wir in den folgenden Lemmata und im Algorithmus zeigen werden.

In den nächsten beiden Lemmata konstruieren wir eine in M lebende Basis von ΔN aus einer in M lebenden Basis C von N unter der auf den ersten Blick starken Voraussetzung, daß alle Elemente aus C gleiche Augmentation haben. Im Anschluß an diese Lemmata stellen wir einen Algorithmus vor, der, von einer beliebigen Basis ausgehend, eine solche spezielle Basis konstruiert.

Lemma 1.5.7 *Es seien M ein Modul mit Basis B und $R \leq M$ Teilmodul, so daß $N = M/R$ frei ist. Weiter induziere $C \subseteq M$ eine Basis von N, wobei alle Elemente $c \in C$ die gleiche Augmentation γ besitzen. Wir fixieren ein Element $c^\sharp \in C$, und es sei $C^\flat := C \setminus \{c^\sharp\}$. Schließlich sei $\rho := \gcd \mathrm{aug}(R)$. Es gilt:*

a) *Ist $\rho = \infty$, dann induziert $C' := \{c - c^\sharp;\ c \in C^\flat\}$ eine Basis von ΔN.*

b) *Ist $\rho \neq \infty$, dann induziert $C' := \{c - c^\sharp;\ c \in C^\flat\} \cup \{\rho c^\sharp\}$ eine Basis von ΔN.*

Beweis

Wir zeigen zunächst, daß $\gcd(\gamma, \rho) = 1$ ist. Da C eine Basis von M/R induziert, gibt es zu $b \in B$ sicher $c \in \langle C \rangle$ und $r \in R$ mit $b = c + r$. Augmentationsbildung ergibt $1 = \mathrm{aug}(c) + \mathrm{aug}(r)$. Ein gemeinsamer Teiler p von γ und ρ würde auch $\mathrm{aug}(c)$ und $\mathrm{aug}(r)$ teilen, was nicht gleichzeitig sein kann für $p \neq 1$.

Da C' die richtige Anzahl an Elementen besitzt, reicht es zu zeigen, daß C' Erzeugendensystem ist. Da C eine Basis von M/R induziert, induziert auch $\{c^\sharp\} \cup \{c - c^\sharp;\ c \in C^\flat\}$ eine Basis von M/R. Es existieren demnach zu jeden b und $b' \in B$ ganze Zahlen $\alpha_c, \beta \in \mathbf{Z}$ und $r \in R$ mit

$$b - b' = r + \beta c^\sharp + \sum_{c \in C^\flat} \alpha_c (c - c^\sharp). \tag{37}$$

In Teil b hat r Augmentation $k\rho$ mit $k \in \mathbf{Z}$. Die Anwendung von aug auf (37) ergibt $0 = k\rho + \beta\gamma$. Da γ und ρ teilerfremd sind, folgt $\rho|\beta$, das heißt, C' erzeugt in der Tat $b - b'$ modulo R.

Teil a folgt ebenfalls mit (37). In diesem Fall ergibt Augmentationsbildung $\beta = 0$.

QED.

Bemerkung 1.5.8 *Ebenso wie ΔM läß sich ΔN als Kern einer "Augmentation" interpretieren. Mit $\rho = [N : \Delta N]$ für endlichen und $\rho = 0$ für unendlichen Index erhält man einen Homomorphismus*

$$\overline{\mathrm{aug}} : N \to \mathbf{Z}/\rho\mathbf{Z},\ a + R \mapsto \mathrm{aug}(a) + \rho\mathbf{Z}, \tag{38}$$

und es gilt $\Delta N = \ker_N \overline{\mathrm{aug}}$, was wie folgt einzusehen ist.

Offensichtlich ist $\Delta N \subseteq \ker_N \overline{\mathrm{aug}}$. Die andere Inklusion erhält man mit dem gleichen Ansatz wie in (37). Ist $a \in \ker_N \overline{\mathrm{aug}}$, so folgt aus einer Relation

$$a = r + \beta c^\sharp + \sum_{c \in C^\flat} \alpha_c (c - c^\sharp) \tag{39}$$

mit $\alpha_c, \beta \in \mathbf{Z}$ und $r \in R$ durch Augmentationsbildung wie im Beweis zu Lemma 1.5.7 $\rho|\beta$ und damit $a \in \Delta N$.

Im Fall b in Lemma 1.5.7 erhält man ein Element $\rho c^\sharp$ als Basiselement, das nicht in ΔM liegt. Diesen Schönheitsfehler kann man direkt dadurch beheben, daß man $\rho c^\sharp$ durch $\rho c^\sharp - \gamma r$ ersetzt, wobei r ein Element aus R mit Augmentation ρ ist, was nach Lemma 1.5.3 existiert. Die folgende Konstruktion erzeugt ebenfalls eine in ΔM lebende Basis von ΔN, die sogar vollständig aus Elementen der Form $\{c - \check{c}\}$ zu einem festen $\check{c}$ besteht.

Lemma 1.5.9 *Es sei M ein Modul mit Basis B und $R \leq M$ ein Teilmodul, so daß $N = M/R$ frei ist. Weiter induziere $C \subseteq M$ eine Basis von N, wobei alle Elemente $c \in C$ die gleiche Augmentation γ besitzen.*

Ist $\rho := \gcd \mathrm{aug}(R) < \infty$, dann existiert ein Element $\check{c} \in M$ mit $\mathrm{aug}(\check{c}) = \gamma$, so daß

$$\check{C} := \{c - \check{c};\ c \in C\} \tag{40}$$

eine Basis von ΔN induziert.

Man erhält $\check{c}$ explizit als Differenz $\check{c} = r - \tilde{c}$, mit $r \in R$ und $\tilde{c} \in \langle C \rangle$, wobei $\mathrm{aug}(r) = \gamma\rho$ und $\mathrm{aug}(\tilde{c}) = (\rho - 1)\gamma$ ist.

Beweis

Wir beweisen das Lemma dadurch, daß wir von einer Basis gemäß Lemma 1.5.7 ausgehen, und dann sukzessive Elemente austauschen, bis wir die Basis $\check{C}$ erhalten. Ist C' wie in Lemma 1.5.7 gegeben, so tauschen wir zunächst $\rho c^\sharp$

gegen $c^\sharp - \check{c}$ aus, und anschließend $c - c^\sharp$ gegen $c - \check{c}$. Wir zeigen nun im einzelnen, wie das möglich ist.

Es sei $c^\sharp \in C$, und es sei $C^\flat := C \setminus \{c^\sharp\}$. Nach Lemma 1.5.7 induziert $\{\rho c^\sharp\} \cup C'$ mit $C' = \{c - c^\sharp;\ c \in C^\flat\}$ eine Basis von ΔN.

Wir wählen nun $\tilde{c} \in \langle C \rangle$ mit $\mathrm{aug}(\tilde{c}) = (\rho - 1)\gamma$. Für dieses gilt dann $\tilde{c} \equiv (\rho - 1)c^\sharp \bmod \langle C' \rangle$. Mit $\check{c} \equiv -\tilde{c} \bmod R$ folgt $c^\sharp - \check{c} \equiv \rho c^\sharp \bmod (R + \langle C' \rangle)$. Damit können wir $\rho c^\sharp$ gegen $c^\sharp - \check{c}$ austauschen und erhalten $C' \cup \{c^\sharp - \check{c}\}$ als eine in M lebende Basis von ΔN.

Wegen $c - \check{c} = c - c^\sharp + (c^\sharp - \check{c})$ lassen sich nun die Elemente $c - c^\sharp$ aus C' tauschen zu $c - \check{c}$, und wir erhalten $\check{C}$ als in M lebende Basis von ΔN.

Bisher ist also gezeigt, daß $\check{C}$ eine Basis ist, wenn $\tilde{c} \in \langle C \rangle$ existiert, für das $\mathrm{aug}(\tilde{c}) = (\rho - 1)\gamma$ ist. Beispielsweise ist $\tilde{c} := (\rho - 1)c^\sharp$ eine geeignete Wahl.

Um $\mathrm{aug}(\check{c}) = \gamma$ zu erreichen, brauchen wir noch $r \in R$ mit $\mathrm{aug}(r) = \rho\gamma$. Sicher existiert aber, wie in Lemma 1.5.3 gezeigt, $r' \in R$ mit $\mathrm{aug}(r') = \rho$. Dann ist $r := \gamma r'$ geeignet.

QED.

Der folgende Algorithmus konstruiert aus einer beliebigen Basis C von ΔN eine Basis $\check{C}$, die die Voraussetzungen der Lemmata 1.5.7 und 1.5.9 erfüllt.

Algorithmus 1.5.10 *Es seien M ein Modul mit Basis B und $R \leq M$ ein Teilmodul, so daß $N = M/R$ frei ist. Weiter induziere $C \subseteq M$ eine Basis von N. Der folgende Algorithmus berechnet eine in M lebende Basis $\check{C}$ von N, deren Elemente alle die gleiche Augmentation γ besitzen.*

1. (Normieren) *Ersetze die $c \in C$ mit* $\mathrm{aug}(c) < 0$ *jeweils durch $\check{c} := -c$. Es gilt nun für alle $c \in C$, daß* $0 \leq \mathrm{aug}(\check{c})$ *ist.*

2. (Augmentation Null eliminieren) *Haben alle Elemente aus C Augmentation Null, so setze $\check{C} := C$ und beende den Algorithmus. Sonst existiert $c^\sharp \in C$ mit* $\mathrm{aug}(c^\sharp) > 0$. *Ersetze nun die $c \in C$ mit* $\mathrm{aug}(c) = 0$ *jeweils durch $\check{c} := c + c^\sharp$. Nach diesem Schritt haben alle Elemente aus C positive Augmentation.*

3. (Überprüfen) *Haben alle Elemente aus C gleiche Augmentation, so setze $\check{C} := C$ und beende den Algorithmus.*

4. (Austauschen) *Wähle c und $c' \in C$ mit* $\mathrm{aug}(c) < \mathrm{aug}(c')$, *tausche c' durch $c' - c$ aus, und mache bei Schritt 3 weiter.*

Lemma 1.5.11 *Algorithmus 1.5.10 arbeitet korrekt.*

Beweis
Offensichtlich liefert Algorithmus 1.5.10, wenn er denn terminiert, ein korrektes Ergebnis, da C nach jedem Schritt eine Basis von M/R induziert.

Der Algorithmus terminiert, da in jedem Durchlauf von Schritt 4 die Summe der Augmentationen der Elemente c aus C um mindestens 1 verringert wird, diese aber, da positiv, nach unten beschränkt ist.

QED.

Zur Effizienz von Algorithmus 1.5.10 sei an dieser Stelle angemerkt, daß hier nur die prinzipielle Berechenbarkeit einer geeigneten Basis demonstriert werden soll. Der Algorithmus ist angelehnt an die Berechnung eines größten gemeinsamen Teilers mehrerer Zahlen, und demzufolge würde man in einer realen Implementierung die Subtraktion in Schritt 4 durch eine geeignete Division mit Rest ersetzen.

Bemerkung 1.5.12 *Bei der Anwendung in Bezug auf die Gruppe der Kreiseinheiten besitzen alle $c \in C$ jeweils Augmentation 1. Dies ist nicht zwingend so, wie das Beispiel $M = \langle a, b\rangle$, $R = \langle 2a + b\rangle$ und $C = \{a + b\}$ demonstriert.*

1.5.3 $\mathbf{Z}[\sigma]$-Moduln

Bei den Anwendungen auf Kreismoduln tritt der Fall auf, daß σ auf dem $\mathbf{Z}$-Modul M und damit auf $N = M/R$ operiert. Wir betrachten im folgenden nur solche Basen, für die der Augmentationshomomorphismus mit σ verträglich ist, das heißt, daß $\mathrm{aug}(\sigma m) = \mathrm{aug}(m)$ für $m \in M$ gilt.

Wir betrachten die beiden von N abgeleiteten Moduln $N_+ = N/\ker_N(1+\sigma)$ und $N_- = N/\ker_N(1-\sigma)$ und definieren zunächst, wie $\Delta N_\pm$ zu verstehen ist.

Definition 1.5.13 *Es sei B eine Basis eines Moduls M, auf dem σ operiere. Weiter sei $R \leq M$ Teilmodul und $N = M/R$ frei. Die Operation von σ führt dann gemäß Definition 1.2.9 auf die Moduln N_+ und N_-. Wir erhalten damit die Folge von kanonischen Homomorphismen*

$$M \overset{\kappa}{\to} M/R = N \overset{\lambda_\pm}{\to} N_\pm. \tag{41}$$

Mit diesen Bezeichnungen sei $\Delta N_\pm := \lambda_\pm \kappa \Delta M$.

Den Zusammenhang mit der Basiskonstruktion aus Abschnitt 1.5.2 liefert das folgenden Lemma.

Lemma 1.5.14 *Es sei M ein Modul, $R \leq M$ ein Teilmodul und $N = M/R$ frei, verbunden durch den kanonischen Homomorphismus $\kappa : M \to M/R$. Wir definieren die Teilmoduln Q_+ und Q_- von M durch*

$$Q_+ := \kappa^{-1}(\ker_N(1+\sigma)) \qquad \textit{und} \qquad Q_- := \kappa^{-1}(\ker_N(1-\sigma)).$$

Dann ist $M/Q_+ \cong N_+$ und $M/Q_- \cong N_-$. Insbesondere induziert eine in M lebende Basis von $\Delta(M/Q_+)$ eine Basis von ΔN_+, und eine in M lebende Basis von $\Delta(M/Q_-)$ induziert eine Basis von ΔN_-.

Beweis
Die Behauptung folgt direkt aus der Kommutativität des Diagramms

$$\begin{array}{ccc} M & \to & M/R \\ \downarrow & & \downarrow \\ M/Q_x & \cong & N_x \end{array} \tag{42}$$

wobei x eines der Symbole $+$ oder $-$ ist.

QED.

Bemerkung 1.5.15 *Konkret erhält man $Q_+ = R + (1-\sigma)M + \langle E^- \rangle$, wenn $[E^0, E^+, E^-]$ eine Normalbasis von N induziert. Ist darüber hinaus $E^- = \emptyset$, das heißt, gilt $m^-(N) = 0$, so folgt* $\gcd\operatorname{aug}(Q_+) = \gcd\operatorname{aug}(R)$.

Im allgemeinen ist $\gcd\operatorname{aug}(Q_-) \neq \gcd\operatorname{aug}(R)$, *denn es ist $(1+\sigma)M \subseteq Q_-$, und $(1+\sigma)M$ enthält Elemente mit Augmentation 2, woraus direkt die Abschätzung* $\gcd\operatorname{aug}(Q_-) \leq 2$ *folgt.*

1.5.4 Differenzenmodul und Zeilenfaktormoduln

In diesem Abschnitt betrachten wir den Differenzenmodul zu gewissen Zeilenfaktormoduln, die später im Zusammenhang mit dem Kreiseinheiten wichtig sind.

Es sei $\mathcal{N}(\Lambda, A)$ der Zeilenfaktormodul zu $\Lambda \times A$, wobei nur A echter Faktor ist. Ist also R das Erzeugnis der Zeilensummen $s(\lambda, *) = \sum_{a \in A}(\lambda \otimes a)$ mit $\lambda \in \Lambda$, dann ist $\mathcal{N}(\Lambda, A) = \langle \Lambda \times A \rangle / R$.

Im Vorgriff auf die Bezeichnungen im zweiten Kapitel sei an dieser Stelle bereits angemerkt, daß dann $Z(q) = \mathcal{N}(G_{q/p}, \{0, \ldots, p-1\})$ gilt, wobei $q = p^\alpha$ eine Primzahlpotenz, $Z(q)$ der Kreismodul und $G_d = \{1 \leq a < d;\ \gcd(a,d) = 1\}$ ist.

Basen für $\Delta\mathcal{N}(\Lambda, A)$ und $\Delta\mathcal{N}(\Lambda, A)_+$ ergeben sich folgendermaßen.

Satz 1.5.16 *Es seien A und Λ endliche Mengen und $\mathcal{N}(\Lambda, A)$ der Zeilenfaktormodul zu $\Lambda \times A$, wobei nur A echter Faktor ist. Weiter sei $c^\sharp := \lambda^\sharp \otimes a^\sharp \in \Lambda \times A$ ein ausgezeichnetes Element und $A^\flat := A \setminus \{a^\sharp\}$.*

a) *Unter diesen Voraussetzungen induziert*

$$B := \{c - c^\sharp;\ c \in \Lambda \times A^\flat\} \tag{43}$$

eine Basis von $\Delta\mathcal{N}(\Lambda, A)$.

b) *Ist* $[\Gamma, \emptyset]$ *eine Normalzerlegung von* Λ *mit* $\lambda^\sharp \in \Gamma$*, dann induziert*

$$B_+ := \{c - c^\sharp;\ c \in \Gamma \times A^\flat\} \tag{44}$$

eine Basis von $\Delta\mathcal{N}(\Lambda, A)_+$.

Beweis

Nach Lemma 1.4.5 induziert $\Lambda \times A^\flat$ eine Basis von $\mathcal{N}(\Lambda, A)$. Korollar 1.3.9, a liefert $\Gamma \times A^\flat$ als Basis von $\mathcal{N}(\Lambda, A)_+$. Dabei ist $\gamma = \mathrm{aug}(\Lambda \times A^\flat) = 1$.

Wir schreiben $\mathcal{N}(\Lambda, A) = M/R$, wobei $M = \langle \Lambda \times A \rangle$ ist und R von den Zeilensummen $s(\lambda, *)$ für $\lambda \in \Lambda$ erzeugt wird.

Wir wollen Lemma 1.5.9 anwenden. Dazu sind gemäß $\gamma = 1$ ein $r \in R$ und ein $\tilde{c} \in \langle \Lambda \times A^\flat \rangle$ zu bestimmen, so daß $c^\sharp = r - \tilde{c}$ ist, wobei $\rho = \mathrm{aug}(r) = \gcd \mathrm{aug}(R) = |A|$ und $\mathrm{aug}(\tilde{c}) = \rho - 1$ ist. Diese sind für $r = s(\lambda^\sharp, *)$ und $\tilde{c} := \sum_{a \in A^\flat} \lambda^\sharp \otimes a$ gegeben, und es folgt Teil a.

Zum Beweis von Teil b seien $\mathcal{N}(\Lambda, A)_+ = M/Q_+$ mit $M = \langle \Lambda \times A \rangle$ und Q_+ wie in Lemma 1.5.14. Da $m^-(\mathcal{N}(\Lambda, A)) = 0$ ist, gilt, wie in Bemerkung 1.5.15 festgestellt, daß $\gcd \mathrm{aug}(Q_+) = \gcd \mathrm{aug}(R)$ ist. Genau wie im Beweis von Fall a, folgt die Behauptung mit Lemma 1.5.9 (man schreibe im vorangegangenen Abschnitt "Γ" anstelle von "Λ").

QED.

Den Fall $\Delta\mathcal{N}(\Lambda, A)_-$ haben wir im vorangegangenen Satz nicht behandelt. Es gilt im allgemeinen $\gcd \mathrm{aug}(Q_-) \neq \gcd \mathrm{aug}(R)$, so daß der Beweis nicht analog zu führen ist. In Bezug auf die Anwendung auf Kreiseinheiten ist dieser Fall auch irrelevant. Grundsätzlich kann man aber mit den Mechanismen von Abschnitt 1.5.2 auch Basen von $\mathcal{N}(\Lambda, A)_-$ konstruieren.

Zum Schluß geben wir noch explizit an, wie die Elemente $\lambda \otimes a^\sharp - \lambda^\sharp \otimes a^\sharp \in \Delta\mathcal{N}(\Lambda, A)$ von der Basis B aus (43) modulo der Relationen aus R erzeugt werden. Es gilt:

$$\lambda \otimes a^\sharp - \lambda^\sharp \otimes a^\sharp \equiv - \sum_{a \neq a^\sharp} \left((\underbrace{\lambda \otimes a - \lambda^\sharp \otimes a^\sharp}_{\in B}) - (\underbrace{\lambda^\sharp \otimes a - \lambda^\sharp \otimes a^\sharp}_{\in B}) \right) \mod R. \tag{45}$$

1.6 Exakte Sequenzen und Basen

In Abschnitt 1.3 wurden aus Eigenschaften von zwei Moduln Informationen über einen dritten Modul gewonnen, wobei der dritte Modul das Tensorprodukt der beiden anderen Moduln ist. In diesem Abschnitt betrachten wir eine ähnliche Situation. Wir gehen von kurzen exakten Sequenzen $0 \to N \to L \to K \to 0$ aus und gewinnen Informationen über L durch das, was von N und K bekannt ist. Anschließend verallgemeinern wir diese Vorgehensweise auf Systeme von Moduln, die implizit durch exakte Sequenzen miteinander verbunden sind.

1.6.1 Exakte Sequenzen

Ist eine exakte Sequenz $0 \to N \xrightarrow{\iota} L \to K \to 0$ gegeben, so gilt definitionsgemäß $N \cong \iota(N)$ und $K \cong L/\iota(N)$. Wir können daher N immer als Teilmodul von L und K als Faktormodul von L auffassen.

Ausgangspunkt unserer Überlegungen zur Konstruktion von Basen ist das folgende Lemma.

Lemma 1.6.1 *Es sei $0 \to N \to L \to K \to 0$ eine exakte Sequenz von Moduln, wobei N und K frei sind. Ist B eine Basis von N und induziert $C \subseteq L$ eine Basis von K, so ist L frei und $B \cup C$ eine Basis von L.*

Beweis
Es sei $S = \langle C \rangle$. Da L von C modulo N erzeugt wird, gilt $L = S + N$. Aus der linearen Unabhängigkeit von C als Basis von L/N folgt, daß $S \cap N = \{0\}$ gilt, somit ist die Summe von S und N direkt, und die Behauptung folgt.

QED.

Lemma 1.6.1 läßt sich verallgemeinern auf eine aufsteigende Folge von Moduln:

Lemma 1.6.2 *Es sei $0 = L^{(0)} \leq L^{(1)} \leq \cdots \leq L^{(i)} \leq \cdots \leq L$ mit $L = \bigcup_{i=0}^{\infty} L^{(i)}$ eine aufsteigende Folge von Moduln, und es seien zu $i \in \mathbf{N}$ freie Moduln $N^{(i)}$ gegeben, derart daß die Sequenz*

$$0 \to L^{(i-1)} \to L^{(i)} \to N^{(i)} \to 0 \tag{46}$$

exakt ist.
Induziert $B^{(i)} \subseteq L^{(i)}$ eine Basis von $N^{(i)}$ für alle $i \in \mathbf{N}$, so ist L frei und $B := \bigcup_{i=1}^{\infty} B^{(i)}$ eine Basis von L.

Beweis
Durch Induktion zeigt man unter Zuhilfenahme von Lemma 1.6.1, daß $L^{(n)}$ für jedes $n \in \mathbf{N}$ frei und die Menge $C^{(n)} := \bigcup_{i=1}^{n} B^{(i)}$ eine Basis von $L^{(n)}$ ist. Dadurch ist das Lemma für endliche Folgen von Moduln $L^{(i)}$ gesichert.

Da jedes Element aus L in einer der Mengen $L^{(n)}$ liegt, ist offensichtlich B ein Erzeugendensystem von L. Darüber hinaus liegt aber auch jede endliche Kombination von Elementen aus B in $L^{(n)}$, für genügend großes n, so daß man sich zum Beweis der linearen Unabhängigkeit von B ebenfalls auf die lineare Unabhängigkeit der einzelnen $C^{(n)}$ zurückziehen kann.

QED.

1.6.2 Normalität

Im folgenden betrachten wir nur jene exakte Sequenzen $0 \to N \xrightarrow{\iota} L \xrightarrow{\psi} K \to 0$, für die N und K (und damit auch L) frei und die Homomorphismen ι und ψ mit σ verträglich sind.

Die Lemmata 1.6.1 und 1.6.2 gelten im allgemeinen nicht für Normalbasen, wie das folgende Beispiel zeigt. Es sei $L = \langle x, \sigma x\rangle$. Weiter definieren wir $N = \langle x - \sigma x\rangle$ und $K = \langle x + N\rangle$. Die Sequenz $0 \to N \to L \to K \to 0$ ist exakt, es ist $B := [\emptyset, \emptyset, \{x - \sigma x\}]$ eine Normalbasis von N, und $C := [\emptyset, \{x\}, \emptyset]$ induziert eine Normalbasis von K, jedoch ist $B \cup C$ keine Normalbasis, noch nicht einmal eine Quasinormalbasis von L. Es ist in diesem Beispiel auch nicht möglich die Basen B und C geschickter zu wählen, um vielleicht doch aus ihrer Vereinigung eine Normalbasis zu erhalten.

Dennoch ist nicht alles verloren. Im folgenden werden wir einen Algorithmus erarbeiten, der zu einer gegebenen exakten Sequenz

$$0 \to N \to L \to K \to 0 \tag{47}$$

und Normalbasen B von N und C von K eine Normalbasis von L herstellt.

Die geschieht dadurch, daß wir ausgehend von (47) eine Folge von exakten Sequenzen

$$0 \to N_i \to L \to K_i \to 0 \tag{48}$$

jeweils mit Normalbasen B_i von N_i und C_i von K_i für $i = 0, 1, 2, \ldots$ konstruieren, wobei in jedem Schritt der Rang von K_i verkleinert und entsprechend der Rang von N_i vergrößert wird, bis wir für ein s eine exakte Sequenz $0 \to N_s \to L \to 0 \to 0$ erhalten. In dem Fall ist $N_s = L$ und eine Normalbasis von N_s ist auch eine Normalbasis von L. Wir erklären im folgenden die einzelnen Schritte.

Lemma 1.6.3 *Es sei $0 \to N \to L \to K \to 0$ exakt, $B = [F^0, F^+, F^-]$ eine Normalbasis von N, und $C = [E^0, E^+, E^-] \subseteq L$ induziere eine Normalbasis von K.*

Ist $B_0 := [F^0 \cup E^0, F^+, F^-]$ und $C_0 := [\emptyset, E^+, E^-]$, dann ist mit $N_0 := \langle B_0\rangle$ und $K_0 := \langle C_0\rangle$ die Sequenz

$$0 \to N_0 \to L \to K_0 \to 0 \tag{49}$$

exakt. Es gilt weiter, daß B_0 Normalbasis von N_0 und C_0 eine Normalbasis von K_0 ist.

<u>*Beweis*</u>
Es sei $K^0 := \langle E^0 \cup \sigma E^0\rangle$. Dann ist $N_0 = N \oplus K^0$ und $K \cong K^0 \oplus K_0$. Damit folgt die Exaktheit von (49) direkt aus der Exaktheit von $0 \to N \to L \to K \to 0$.

Daß B_0 und C_0 sogar Normalbasen sind, kann direkt nachgerechnet werden.

QED.

Lemma 1.6.3 ermöglicht es, aus K den "K^0-Teil" zu entfernen. Im folgenden kümmern wir uns um den von E^+ und E^- erzeugten Teil von K.

Der folgende Algorithmus konstruiert aus Normalbasen B und C Mengen B' und C', die wir im anschließenden Lemma als Normalbasen geeigneter Moduln identifizieren werden.

Algorithmus 1.6.4 *Es sei $0 \to N \to L \to K \to 0$ eine exakte Sequenz. Es sei weiter $B = [F^0, F^+, F^-]$ eine Normalbasis von N und $C = [E^0, E^+, E^-] \subseteq L$ induziere eine Normalbasis von K, wobei $E^+ \cup E^- \neq \emptyset$ gilt. Wir konstruieren auf die folgende Art $B' := G^0 \cup \sigma G^0 \cup G^+ \cup G^-$ und C' mit $|C'| < |C|$.*

I. Fall: $c \in E^+$. In diesem Fall sei $C' := [E^0, E^+ \setminus \{c\}, E^-]$. Es ist $c - \sigma c \in \ker_N(1+\sigma) \subseteq N$. Nach Lemma 1.2.10, b, ii existieren $a \in N$ und $F' \subseteq F^-$ mit $c - \sigma c = (1-\sigma)a + \sum_{b \in F'} b$. Wir definieren $f := c - a \in L$ und unterscheiden zwei Fälle.

- ⌣ *Ist $F' = \emptyset$, so ist $\sigma f = f$, und dementsprechend setzen wir*
  $$G^0 := F^0, \qquad G^+ := F^+ \cup \{f\}, \quad G^- := F^-.$$
- ⌢̈ *Ist $F' \neq \emptyset$, dann wählen wir ein $f' \in F'$ und setzen*
  $$G^0 := F^0 \cup \{f\}, \quad G^+ := F^+, \qquad G^- := F^- \setminus \{f'\}.$$

II. Fall: $c \in E^-$. Wir setzen zunächst $C' := [E^0, E^+, E^- \setminus \{c\}]$. Analog zum ersten Fall existieren $a \in N$ und $F' \subseteq F^+$ mit $c + \sigma c = (1+\sigma)a + \sum_{b \in F'} b$. Wir definieren wieder $f := c - a \in L$ und unterscheiden zwei Fälle.

- ⌣ *Ist $F' = \emptyset$, so ist $\sigma f = -f$, und dementsprechend setzen wir*
  $$G^0 := F^0, \qquad G^+ := F^+, \qquad G^- := F^- \cup \{f\}.$$
- ⌢̈ *Ist $F' \neq \emptyset$, dann wählen wir ein $f' \in F'$ und setzen*
  $$G^0 := F^0 \cup \{f\}, \quad G^+ := F^+ \setminus \{f'\}, \quad G^- := F^-.$$

Lemma 1.6.5 *Es seien die Voraussetzungen und Bezeichnungen wie in Algorithmus 1.6.4 gewählt. Weiter definieren wir $N' := \langle B' \rangle$ und $K' := \langle C' \rangle$. Dann ist B' eine Normalbasis von N' und C' eine Normalbasis von K', und die Sequenz*

$$0 \to N' \to L \to K' \to 0 \tag{50}$$

ist exakt.

<u>*Beweis*</u>
Daß B' und C' Normalbasen sind ergibt sich direkt aus deren Definition, wobei man in Algorithmus 1.6.4 die einzelnen Fälle unterscheidet. Es ist zu zeigen, daß die Sequenz (50) exakt ist.

Wir übernehmen im folgenden die Bezeichnungen von Algorithmus 1.6.4. Definieren wir $\widetilde{B} := B \cup \{c\}$ und $\widetilde{N} := \langle \widetilde{B} \rangle$, so folgt aus der Exaktheit von $0 \to N \to L \to K \to 0$ wie im Beweis von Lemma 1.6.3 die Exaktheit von

$$0 \to \widetilde{N} \to L \to K' \to 0, \tag{51}$$

indem man bei $L \to K'$ das Element $c \in L$ auf 0 abbildet.

Wir zeigen $\widetilde{N} = N'$, das heißt, wir zeigen, daß B' und $\widetilde{B}$ den gleichen Modul erzeugen. Wir nehmen $c \in E^+$ an. Ist $c \in E^-$, so argumentiert man analog.

Ist der ⌣-Unterfall eingetreten, so ist

$$B' = B \cup \{f\} \quad \text{und} \quad \widetilde{B} = B \cup \{c\}.$$

Da $f \equiv c \bmod \langle B \rangle$ ist, gilt $\langle B' \rangle = \langle \widetilde{B} \rangle$.
Im $\dot{-}$-Unterfall sei $B^\flat := B \setminus \{f'\}$, und es gilt

$$B' = B^\flat \cup \{f, \sigma f\} \quad \text{und} \quad \widetilde{B} = B^\flat \cup \{f', c\} = B \cup \{c\}.$$

$B' \subseteq \langle \widetilde{B} \rangle$ folgt mit $f \equiv c \bmod \langle B \rangle$ und $\sigma f \equiv c \bmod \langle B \rangle$. Um $\widetilde{B} \subseteq \langle B' \rangle$ zu zeigen, benutzt man zunächst die direkt aus der Definition von f folgende Beziehung

$$f' = f - \sigma f - \sum_{\substack{b \in F' \\ b \neq f'}} b, \tag{52}$$

so daß also $f' \in \langle B' \rangle$ folgt, und dann die Beziehung $c = f + a$ mit $a \in N \subseteq \langle B' \cup \{f'\} \rangle = \langle B' \rangle$, aus der sich $c \in \langle B' \rangle$ ergibt.

QED.

Mit diesen Vorarbeiten können wir nun einen Algorithmus zur Konstruktion einer Normalbasis von L formulieren.

Algorithmus 1.6.6 *Gegeben sei eine exakte Sequenz $0 \to N \to L \to K \to 0$. Auf die folgende Art und Weise konstruiert man aus einer Normalbasis von N und einer in L lebenden Normalbasis von K eine Normalbasis von L.*

(1) Konstruiere eine exakte Sequenz $0 \to N_0 \to L \to K_0 \to 0$ mit Normalbasen von N_0 und K_0, gemäß Lemma 1.6.3, so daß also $m^0(K_0) = 0$ ist.

(2) Konstruiere mit Algorithmus 1.6.4 sukzessive die Modulpaare (K_0, N_0), (K_1, N_1), ..., (K_s, N_s) mit Normalbasen von K_i und N_i, wobei jeweils nach Lemma 1.6.5 die Sequenz $0 \to N_i \to L \to K_i \to 0$ für $i = 1, \ldots, s$ exakt ist, und zwar solange, bis $K_s = \{0\}$ ist. Die Normalbasis von N_s ist dann gleichzeitig eine Normalbasis von $L = N_s$.

Bemerkung 1.6.7 *Es sei $x \in \{+, -\}$ und $m^{0x} := m^0 + m^x$. Dann gilt in Algorithmus 1.6.6:*

a) $m^x(N) + m^x(K) = m^x(N_0) + m^x(K_0) \geq m^x(N_1) + m^x(K_1) \geq \cdots \geq m^x(N_s) + m^x(K_s) = m^x(L)$,

b) $m^{0x}(N) + m^{0x}(K) = m^{0x}(N_0) + m^{0x}(K_0) = m^{0x}(N_1) + m^{0x}(K_1) = \cdots = m^{0x}(N_s) + m^{0x}(K_s) = m^{0x}(L)$.

Tritt bei der Anwendung von Algorithmus 1.6.4 nur der $\dot{\smile}$-Fall auf, so liegt eine besonders einfache Situation vor, die wir im folgenden durch äquivalente Aussagen charakterisieren können.

Satz 1.6.8 *Ist die Sequenz*

$$0 \to N \xrightarrow{\iota} L \xrightarrow{\psi} K \to 0 \tag{53}$$

exakt, dann sind die folgenden Aussagen äquivalent.

(i) *In Algorithmus 1.6.6 tritt bei jeder Anwendung von Algorithmus 1.6.4 der $\smile$-Fall auf.*

(ii,a) *Für alle $x \in \{+,-,0\}$ gilt $m^x(L) = m^x(N) + m^x(K)$.*

(ii,b) *Für mindestens ein $x \in \{+,-,0\}$ gilt $m^x(L) = m^x(N) + m^x(K)$.*

(iii,a) *Die Sequenz $0 \to H^0(\sigma, N) \to H^0(\sigma, L) \to H^0(\sigma, K) \to 0$ von $\mathbf{F}_2$-Vektorräumen ist exakt.*

(iii,b) *Die Sequenz $0 \to H^0(-\sigma, N) \to H^0(-\sigma, L) \to H^0(-\sigma, K) \to 0$ von $\mathbf{F}_2$-Vektorräumen ist exakt.*

(iv) *Die beiden Sequenzen $0 \to N_+ \to L_+ \to K_+ \to 0$ und $0 \to N_- \to L_- \to K_- \to 0$ sind exakt.*

(v) *Die Sequenz (53) zerfällt als Sequenz von $\mathbf{Z}[\sigma]$-Moduln.*

Beweis
Wir zeigen zunächst, daß die a-Teile jeweils äquivalent zu dem entsprechendem b-Teil sind.

(ii,a) $\Leftrightarrow$ (ii,b): Es sei $x \in \{+,-\}$. Wie in Bemerkung 1.6.7 festgehalten, gilt $m^{0x}(N) + m^{0x}(K) = m^{0x}(L)$. Daraus erhalten wir sofort

$$-(m^x(L) - m^x(N) - m^x(K)) = m^0(L) - m^0(N) - m^0(K). \tag{54}$$

Ist also nach Voraussetzung eine Seite Null, so verschwindet die andere ebenfalls.

(iii,a) $\Leftrightarrow$ (iii,b): Da $\{1, \sigma\}$ zyklisch ist, existiert das Diagramm

$$\begin{array}{ccccc} H^0(\sigma,N) & \to & H^0(\sigma,L) & \to & H^0(\sigma,K) \\ \uparrow & & & & \downarrow \\ H^1(\sigma,K) & \leftarrow & H^1(\sigma,L) & \leftarrow & H^1(\sigma,N) \end{array} \tag{55}$$

und ist exakt (vergleiche [10], Seite 83). Daher ist insbesondere die Injektivität von $H^0(\sigma, N) \to H^0(\sigma, L)$ äquivalent zur Surjektivität von $H^1(\sigma, L) \to H^1(\sigma, K)$, und die Surjektivität von $H^0(\sigma, L) \to H^0(\sigma, K)$ ist äquivalent zur Injektivität von $H^1(\sigma, N) \to H^1(\sigma, L)$.

Da $H^0(-\sigma, M) = H^1(\sigma, M)$ für jeden Modul M ist, folgt die Äquivalenz von (iii,a) und (iii,b).

Wir zeigen nun im folgenden die Äquivalenzen (i) $\Leftrightarrow$ (ii,a/b) $\Leftrightarrow$ (iii,a/b) $\Leftrightarrow$ (iv), und anschließend die Implikationen (i) $\Rightarrow$ (v) $\Rightarrow$ (ii,a/b).

(i) $\Leftrightarrow$ (ii,a/b): Tritt einmal der $\frown$-Unterfall auf, so ist eine der Ungleichungen in Bemerkung 1.6.7, a echt, und es gilt $m^+(N) + m^+(K) > m^+(L)$.

Tritt umgekehrt nur der $\smile$-Unterfall auf, so gilt in Bemerkung 1.6.7 überall Gleichheit.

(ii,a/b) $\Leftrightarrow$ (iii,a/b): Für jeden Modul M ist $m^+(M)$ nach Lemma 1.2.4 die Dimension des $\mathbf{F}_2$-Vektorraums $H^0(\sigma, M)$ und $m^-(M)$ die Dimension von $H^0(-\sigma, M) = H^1(\sigma, M)$. Da die mittlere Exaktheit in (iii,a/b) immer gilt, folgt die behauptete Äquivalenz durch eine einfache Dimensionsbetrachtung.

(iii,a/b) $\Leftrightarrow$ (iv): Wir zeigen beide Richtungen getrennt.

"$\Rightarrow$" Die Sequenz $0 \to N_+ \to L_+ \to K_+ \to 0$ ist nach Definition 1.2.9 kanonisch isomorph zu $0 \to (1+\sigma)N \to (1+\sigma)L \xrightarrow{\psi} (1+\sigma)K \to 0$. Dabei ist nur die mittlere Exaktheit, nämlich $\ker_{(1+\sigma)L} \psi \subseteq (1+\sigma)N$ fraglich. Aus der Exaktheit von $0 \to N \to L \to K \to 0$ folgt zumindest $\ker_{(1+\sigma)L} \psi \subseteq N$. Ist $y := (1+\sigma)x \in \ker_{(1+\sigma)L} \psi$ mit $x \in L$, so definiert y ein Element aus $H^0(\sigma, N)$, das in $H^0(\sigma, L)$ trivial wird. Damit ist gezeigt, daß die Injektivität von $H^0(\sigma, N) \to H^0(\sigma, L)$ die Exaktheit von $0 \to N_+ \to L_+ \to K_+ \to 0$ impliziert.

Die gleiche Überlegung für $-\sigma$ statt σ zeigt die Exaktheit von $0 \to N_- \to L_- \to K_- \to 0$ mit Hilfe der Injektivität der Abbildung $H^0(-\sigma, N) \to H^0(-\sigma, L)$.

"$\Leftarrow$" Wir zeigen die Injektivität der beiden Abbildungen $H^0(\sigma, N) \to H^0(\sigma, L)$ und $H^0(-\sigma, N) \to H^0(-\sigma, L)$. Mit dem Diagramm aus (55) folgt dann die Exaktheit der Sequenzen in (iii,a) und (iii,b).

Ist $0 \to N_+ \to L_+ \to K_+ \to 0$ exakt, so auch

$$0 \to (1+\sigma)N \to (1+\sigma)L \xrightarrow{\psi} (1+\sigma)K \to 0. \tag{56}$$

Ist $y + (1+\sigma)N \in H^0(\sigma, N)$ mit $y \in N$ in $H^0(\sigma, L)$ trivial, so ist $y \in (1+\sigma)L$. Aus $y \in N$ folgt mittels (53) $y \in \ker_L \psi$, insgesamt erhalten wir $y \in \ker_{(1+\sigma)L} \psi$ und die Exaktheit von (56) liefert $y \in (1+\sigma)N$. Somit ist $y + (1+\sigma)N$ bereits in $H^0(\sigma, N)$ trivial, und die Injektivität von $H^0(\sigma, N) \to H^0(\sigma, L)$ folgt.

Die gleiche Überlegung für $-\sigma$ statt σ liefert die Injektivität von $H^0(-\sigma, N) \to H^0(-\sigma, L)$.

(i) $\Rightarrow$ (v): Nach [6], Theorem 1.18, ii zerfällt (53) als Sequenz von $\mathbf{Z}[\sigma]$-Moduln genau dann, wenn ein $\mathbf{Z}[\sigma]$-Homomorphismus $\lambda : L \to N$ existiert, mit $\lambda\iota = \mathrm{id}_N$. Tritt in Algorithmus 1.6.6 bei jeder Anwendung

von Algorithmus 1.6.4 nur der $\smile$-Unterfall auf, so besitzt L eine Normalbasis der Form $B \cup C$, wobei B eine Normalbasis von N ist. Der $\mathbf{Z}[\sigma]$-Homomorphismus λ wird definiert durch die Festlegung, daß λ die Elemente aus B identisch und diejenigen aus C trivial abbildet.

(v) $\Rightarrow$ (ii,a/b): Aus [6], Theorem 1.18, iii erhalten wir $L = N \oplus K$ als direkte Summenzerlegung von $\mathbf{Z}[\sigma]$-Moduln. Unmittelbar aus der Definition der Invarianten m^+, m^- und m^0 aus Definition 1.2.2 und Lemma 1.2.1 folgt damit die Additivität der Invarianten in (ii,a/b).

QED.

Definition 1.6.9 *Eine exakte Sequenz* $0 \to N \to L \to K \to 0$ *heißt* gutartig, *falls sie eine (und damit alle) der äquivalenten Bedingungen (i)-(v) aus Satz 1.6.8 erfüllt.*

Zusammenfassend läßt sich sagen, daß sich unglücklicherweise zu einer gegebenen exakten Sequenz $0 \to N \to L \to K \to 0$ eine Normalbasis von L nicht einfach in Analogie zu Lemma 1.6.1 aus der Vereinigung einer Basis von N und einer auf L lebenden Basis von K ergibt. Es läßt sich jedoch ein einfacher Algorithmus, nämlich Algorithmus 1.6.6, angeben, der eine Normalbasis von L konstruiert.

Normalbasen von L implizieren nach Lemma 1.2.10, a unter anderem Basen von L_+ und L_-. Ist die Sequenz als gutartig erkannt, so läßt sich eine Basis von beispielsweise L_+ einfacher erhalten: Mit Hilfe der Normalbasen B von N und C von K bestimme man Basen B_+ von N_+ und C_+ von K_+. Die Sequenz $0 \to N_+ \to L_+ \to K_+ \to 0$ ist nach Satz 1.6.8 exakt. Also induziert $B_+ \cup C_+$ nach Lemma 1.6.1 eine Basis von L_+.

Mit diesem vereinfachten Verfahren (Normalbasen von N und K liefern Basen von N_+ und K_+. Diese liefern eine Basis von L_+) erhält man zwar keine Normalbasis mehr von L aber immerhin Basen von L_+ und L_-. Wir zeigen im folgenden, wie dieses Konstruktionsverfahren für eine aufsteigenden Folge von Moduln aussieht.

Satz 1.6.10 *Es sei* $0 = L^{(0)} \leq L^{(1)} \leq \cdots \leq L^{(i)} \leq \cdots \leq L$ *mit* $L = \bigcup_{i=0}^{\infty} L^{(i)}$ *eine aufsteigende Folge von Moduln, und es seien zu* $i \in \mathbf{N}$ *Moduln* $N^{(i)}$ *gegeben, derart daß für alle* $i \in \mathbf{N}$ *die Sequenz*

$$0 \to L^{(i-1)} \to L^{(i)} \to N^{(i)} \to 0 \tag{57}$$

exakt und gutartig ist.

i) Induziert $B_+^{(i)} \subseteq L^{(i)}$ *eine Basis von* $N_+^{(i)}$ *für alle* $i \in \mathbf{N}$, *so induziert* $\bigcup_{i=1}^{\infty} B_+^{(i)}$ *eine Basis von* L_+.

ii) Induziert $B_-^{(i)} \subseteq L^{(i)}$ *eine Basis von* $N_-^{(i)}$ *für alle* $i \in \mathbf{N}$, *so induziert* $\bigcup_{i=1}^{\infty} B_-^{(i)}$ *eine Basis von* L_-.

Beweis
Wir zeigen Teil i, Teil ii folgt analog.
Dazu beweisen wir zunächst durch Induktion, daß $C_+^{(n)} := \bigcup_{i=1}^{n} B_+^{(i)} \subseteq L^{(n)}$ eine Basis von $L_+^{(n)}$ induziert. Wir betrachten das kommutative Diagramm

$$\begin{array}{ccccccccc} 0 & \to & L^{(n-1)} & \to & L^{(n)} & \to & N^{(n)} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & L_+^{(n-1)} & \to & L_+^{(n)} & \to & N_+^{(n)} & \to & 0, \end{array} \tag{58}$$

in dem nach Voraussetzung die obere und untere Sequenz beide exakt sind.
Induziert nun $B_+^{(n)} \subseteq L^{(n)}$ eine Basis von $N_+^{(n)}$, so induziert auch

$$\widetilde{B_+^{(n)}} := \{b + \ker_{L^{(n)}}(\sigma + 1);\ b \in B_+^{(n)}\} \subseteq L_+^{(n)} \tag{59}$$

eine Basis von $N_+^{(n)}$.
Nach Induktionsannahme induziert $C_+^{(n-1)} \subseteq L^{(n-1)}$ eine Basis von $L_+^{(n-1)}$. Betten wir $L_+^{(n-1)}$ in $L_+^{(n)}$ ein, dann ist

$$\widetilde{C_+^{(n-1)}} := \{c + \ker_{L^{(n)}}(\sigma + 1);\ c \in C_+^{(n-1)}\} \subseteq L_+^{(n)} \tag{60}$$

eine Basis von $L_+^{(n-1)}$.
Dies sind aber genau die Voraussetzungen für Lemma 1.6.1, und mit diesem ist

$$\widetilde{B_+^{(n)}} \cup \widetilde{C_+^{(n-1)}} = \{b + \ker_{L^{(n)}}(\sigma + 1);\ b \in B_+^{(n)} \cup C_+^{(n-1)}\} \tag{61}$$

eine Basis von $L_+^{(n)}$. Diese Basis wird aber gerade von $C_+^{(n)}$ induziert.
Den Schritt von $L_+^{(n)}$ auf L_+ führt man wie im Beweis von Lemma 1.6.2 durch, indem man sich auf endliche Stücke zurückzieht.

QED.

1.6.3 Kombinierte Moduln

In diesem Abschnitt diskutieren wir die Kombination eines Systems von Moduln zu einem größeren Modul. Durch Anwendung der Ergebnisse des vorhergehenden Abschnitts konstruieren wir eine Basis dieses größeren Moduls aus Basen der Ausgangsmoduln.

Für den Rest des Abschnitts sei Δ eine endliche oder abzählbare, partiell geordnete Menge, deren Ordnung sich vervollständigen läßt. Zusätzlich verlangen wir von Δ, daß es zu jeder endlichen Teilmenge $\Delta' \subseteq \Delta$ eine obere Schranke, das heißt, ein Element $d \in \Delta$ mit $t \leq d$ für alle $t \in \Delta'$, gibt. Beispiele für solche Indexmengen Δ sind alle Teiler einer Zahl n oder auch die Menge $\mathbf{N}$ selbst, jeweils geordnet durch die Teilbarkeitsbeziehung.

Es ist also Δ a priori nicht vollständig geordnet. Schreiben wir daher im folgenden $t < d$ für $t, d \in \Delta$, so ist die partielle Ordnung gemeint. Vervollständigen

wir die Ordnung auf Δ, so können wir, da Δ endlich oder abzählbar ist, durch Umbenennung $\Delta = \{1, \ldots, n\}$ beziehungsweise $\Delta = \mathbf{N}$ annehmen. Auf einen formalen Beweis hierzu sei an dieser Stelle verzichtet, da in den hier interessierenden Anwendungen (Δ eine Teilmenge von $\mathbf{N}$, durch Teilbarkeit geordnet) die Vervollständigung offensichtlich durch die natürliche Ordnung von $\mathbf{N}$ möglich ist.

Definition 1.6.11 *Zu jedem $d \in \Delta$ sei ein Modul M_d, eine Teilmenge $\mathcal{E}_d$ von M_d und eine Abbildung $\mathfrak{n}_d : \mathcal{E}_d \to \bigoplus_{t<d} M_t$ gegeben. Ein solches System von Tripeln $(M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d\in\Delta}$ nennen wir ein M$\mathcal{E}\mathfrak{n}$-*System.

Ist $N = \bigoplus_{t\in\Delta} M_t$, so existiert für $d \in \Delta$ eine natürliche Einbettung $M_d \hookrightarrow N$. Um die Lesbarkeit der folgenden Definitionen und Sätze zu erhöhen, geben wir im folgenden diese Einbettung nicht explizit an, sondern fassen $a \in M_d$ automatisch auch als in N liegend auf.

Definition 1.6.12 *Zu einem M$\mathcal{E}\mathfrak{n}$-System $\Gamma = (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d\in\Delta}$ und zu $d \in \Delta$ seien $N'_d := \bigoplus_{t<d} M_t$ und $Q'_d := \sum_{t<d}\langle r + \mathfrak{n}_t(r);\ r \in \mathcal{E}_t\rangle \subseteq N'_d$ definiert.*
Das M$\mathcal{E}\mathfrak{n}$-System Γ heißt kombinierbar*, wenn sich die $\mathfrak{n}_d$, aufgefaßt als Abbildungen nach N'_d/Q'_d, fortsetzen lassen zu $\mathbf{Z}[\sigma]$-Homomorphismen*

$$\bar{\mathfrak{n}}_d : \langle \mathcal{E}_d\rangle \to N'_d/Q'_d. \tag{62}$$

In diesem Fall nennen wir den Modul $L = N/Q$ mit $N := \bigoplus_{t\in\Delta} M_t$ und $Q := \sum_{t\in\Delta}\langle r + \mathfrak{n}_t(r);\ r \in \mathcal{E}_t\rangle$ das Kombinat *des M$\mathcal{E}\mathfrak{n}$-Systems Γ.*

Definition 1.6.13 *Es sei das M$\mathcal{E}\mathfrak{n}$-System $\Gamma = (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d\in\Delta}$ kombinierbar und das Kombinat L von Γ frei.*

a) *Ist Δ eine endliche Menge, so heißt Γ* gutartig*, wenn*

$$m^+(L) = \sum_{d\in\Delta} m^+(M_d/\langle \mathcal{E}_d\rangle) \tag{63}$$

erfüllt ist.

b) *Ist Δ eine unendliche Menge, so heißt Γ* gutartig*, wenn für alle $d \in \Delta$ das M$\mathcal{E}\mathfrak{n}$-System $(M_t, \mathcal{E}_t, \mathfrak{n}_t)_{t\le d}$ gutartig ist.*

Die Festlegung auf m^+ in obiger Definition (statt m^- oder m^0) ist willkürlich. Ohne Beweis sei angemerkt, daß Bedingung (63) äquivalent ist zu den entsprechenden Aussagen für m^0 oder m^-. Diese Äquivalenz ist letztendlich auf die Äquivalenz (ii,a) $\Leftrightarrow$ (ii,b) in Satz 1.6.8 zurückzuführen. Wir wollen darauf an dieser Stelle jedoch nicht weiter eingehen und uns der Konstruktion von Basen zuwenden.

Satz 1.6.14 *Es sei $\Gamma = (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d\in\Delta}$ ein kombinierbares M$\mathfrak{E}\mathfrak{n}$-System und L das Kombinat von Γ. Ist $M_d/\langle\mathcal{E}_d\rangle$ frei für jedes $d \in \Delta$, dann ist L ebenfalls frei, und es gilt:*

a) *Induziert $B^{(d)} \subseteq M_d$ für $d \in \Delta$ eine Basis von $M_d/\langle\mathcal{E}_d\rangle$, dann induziert $B := \bigcup_{d\in\Delta} B^{(d)} \subseteq \bigoplus_{d\in\Delta} M_d$ eine Basis von L.*

   Mit anderen Worten: zerlegen wir jedes M_d gemäß $M_d = C_d \oplus \langle\mathcal{E}_d\rangle$, so ist $L \cong \bigoplus_{d\in\Delta} C_d$.

b) *Ist Γ darüber hinaus gutartig, so gilt:*

   i) *Induziert $B_+^{(d)} \subseteq M_d$ für $d \in \Delta$ eine Basis von $(M_d/\langle\mathcal{E}_d\rangle)_+$, dann induziert $B_+ := \bigcup_{d\in\Delta} B_+^{(d)} \subseteq \bigoplus_{d\in\Delta} M_d$ eine Basis von L_+.*

   ii) *Induziert $B_-^{(d)} \subseteq M_d$ für $d \in \Delta$ eine Basis von $(M_d/\langle\mathcal{E}_d\rangle)_-$, dann induziert $B_- := \bigcup_{d\in\Delta} B_-^{(d)} \subseteq \bigoplus_{d\in\Delta} M_d$ eine Basis von L_-.*

Beweis
Teil a:
Wir setzen die Ordnung von Δ zu einer vollständigen Ordnung fort, können also $\Delta = \mathbf{N}$ oder $\Delta = \{1, \ldots, n\}$ der Größe nach geordnet annehmen. Für $i \in \Delta$ definieren wir $N_i := M_1 \oplus \cdots \oplus M_i$ und

$$Q_i := \sum_{j=1}^{i} \langle r + \mathfrak{n}_j(r);\ r \in \mathcal{E}_j\rangle \leq N_i. \tag{64}$$

Dazu sei angemerkt, daß mit den Bezeichnungen aus Definition 1.6.12 dann $Q_i' \leq Q_{i-1}$ und $N_i' \leq N_{i-1}$ gilt, mit Gleichheit, wenn die Ordnung in Definition 1.6.12 bereits vollständig war.
Wir zeigen zunächst $Q_i \cap N_{i-1} = Q_{i-1}$ und schreiben dazu $q \in Q_i$ als

$$q = \sum_{e\in\mathcal{E}_i} \alpha_e(e + \mathfrak{n}_i(e)) + q', \tag{65}$$

mit $\alpha_e \in \mathbf{Z}$, nur endlich viele $\alpha_e \neq 0$ und $q' \in Q_{i-1}$.
Da $\mathfrak{n}_i$ modulo Q_i' und damit auch modulo Q_{i-1} Homomorphismus ist, ist

$$q \equiv r + \mathfrak{n}_i(r) \bmod Q_{i-1} \tag{66}$$

mit $r = \sum_{e\in\mathcal{E}_i} \alpha_e e \in M_i$. Reduzieren wir (66) modulo N_{i-1}, so folgt, wenn q auch in N_{i-1} liegt, $0 \equiv r \bmod N_{i-1}$, und daher $r \in N_{i-1} \cap M_i = \{0\}$, also $r = 0$. Setzen wir dies in (66) ein, so folgt $q \in Q_{i-1}$. Damit ist $Q_i \cap N_{i-1} = Q_{i-1}$ gezeigt, weil die umgekehrte Inklusion offensichtlich gilt.
Induktiv folgt $Q_k \cap N_{i-1} = Q_{i-1}$ für $k \geq i$ aus

$$Q_k \cap N_{i-1} = (\cdots((Q_k \cap N_{k-1}) \cap N_{k-2}) \cap \cdots N_i) \cap N_{i-1}. \tag{67}$$

Mit $Q = \bigcup_{i\in\Delta} Q_i$ folgt dann, daß $Q \cap N_i = Q_i$ für alle $i \in \Delta$ gilt, denn jedes $q \in Q$ muß in irgendeinem der Q_k liegen. Wir können daher N_i/Q_i als Teilmodul von N/Q auffassen und erhalten eine aufsteigende Folge von Moduln

$$0 = N_0/Q_0 \leq N_1/Q_1 \leq N_2/Q_2 \leq \cdots \leq N/Q. \tag{68}$$

Die offensichtlich exakte Sequenz

$$0 \to N_{i-1} \to N_i \xrightarrow{\pi} M_i \to 0 \tag{69}$$

führt durch Faktorisieren mit Q_i zu der exakten Sequenz

$$0 \to N_{i-1}/(Q_i \cap N_{i-1}) \to N_i/Q_i \to M_i/\pi(Q_i) \to 0. \tag{70}$$

Nach dem oben Gezeigten ist $Q_i \cap N_{i-1} = Q_{i-1}$.

Weiter ist π die Projektion auf M_i. Das bedeutet, daß die Elemente $r + \mathfrak{n}_i(r)$ mit $r \in \mathcal{E}_i$ auf r abgebildet werden, somit ist $\pi(Q_i) = \langle \mathcal{E}_i \rangle$. Wir erhalten die exakte Sequenz

$$0 \to N_{i-1}/Q_{i-1} \to N_i/Q_i \to M_i/\langle \mathcal{E}_i \rangle \to 0. \tag{71}$$

Die in M_i definierte Basis $B^{(i)}$ von $M_i/\langle \mathcal{E}_i \rangle$ können wir vermöge der Abbildung $b \mapsto b + Q_i$ für $b \in B^{(i)}$ als in N_i/Q_i liegend auffassen. Mit der Folge (68) und der exakten Sequenz (71) sind wir dann genau in der Situation von Lemma 1.6.2. Mit diesem folgt, daß L frei ist und die Behauptung in Teil a.

Teil b:

Sind die exakten Sequenzen in (71) für alle $i \in \Delta$ gutartig, so läßt sich direkt Satz 1.6.10 anwenden, um die Behauptung zu erhalten.

Wir zeigen also, daß die Gutartigkeit von Γ die Gutartigkeit der exakten Sequenzen aus (71) impliziert. Zunächst definieren wir die folgenden Zahlen. Zu $i \in \Delta$ sei $x_i := m^+(N_i/Q_i)$ und $y_i := m^+(M_i/\langle \mathcal{E}_i \rangle)$. Zusätzlich sei $x_0 = 0$.

Für exakte Sequenzen, also insbesondere für die Sequenz in (71) mit $i \in \Delta$, gilt nach Bemerkung 1.6.7, a die Ungleichung $x_i \leq x_{i-1} + y_i$, nach Satz 1.6.8 mit Gleichheit genau dann, wenn die Sequenz gutartig ist. Per Induktion zeigt man, daß $x_k \leq \sum_{i=1}^{k} y_i$ mit Gleichheit genau dann gilt, wenn $x_i = x_{i-1} + y_i$ für alle $i \leq k$ ist.

Wir unterscheiden nun die Fälle, ob Δ endlich oder unendlich ist.

I. Fall, $\Delta = \{1, \ldots, n\}$:

In diesem Fall ist das Kombinat L von Γ gleich N_n/Q_n. Die Gutartigkeitsbedingung an Γ ergibt die Gleichung $x_n = \sum_{i=1}^{n} y_i$. Für alle $i \leq n$ folgt dann nach dem oben Bewiesenen $x_i = x_{i-1} + y_i$. Dies ist aber gleichbedeutend zur Gutartigkeit aller Sequenzen in (71).

II. Fall, $\Delta = \mathbf{N}$:

Zu $i \in \mathbf{N}$ sei $d(i) \in \mathbf{N}$ eine obere Schranke bezüglich der ursprünglichen Ordnung von $\{1, \ldots, i\}$. Es soll also gelten, daß $j < d(i)$ gilt für alle $j \in$

$\{1, \ldots, i\}$. (Zur Erinnerung: Die Existenz einer solchen oberen Schranke war eine Forderung an Δ.)

Wir betrachten das $M\mathcal{E}\mathfrak{n}$-System $\Gamma_i = (M_t, \mathcal{E}_t, \mathfrak{n}_t)_{t \leq d(i)}$. Für dieses endliche System ist die Sequenz in (71) ebenfalls definiert. Dieses endliche System Γ_i ist gutartig, und aus dem I. Fall folgt die Gutartigkeit von (71).

QED.

Ist also L das Kombinat eines $M\mathcal{E}\mathfrak{n}$-Systems $\Gamma = (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d \in \Delta}$, so zeigt Satz 1.6.14, wie man Basen von L, L_+ und L_- erhält. Noch offen ist die Frage nach Normalbasen von L. Ist Δ endlich, so läßt sich eine Normalbasis durch sukzessive Anwendung von Algorithmus 1.6.6 erhalten. Wir beschreiben dies im folgenden genauer.

Algorithmus 1.6.15 *Es sei $\Gamma = (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d \in \Delta}$ ein kombinierbares $M\mathcal{E}\mathfrak{n}$-System mit $|\Delta| < \infty$ und L das Kombinat von Γ.*

Der folgende Algorithmus konstruiert eine Normalbasis von L aus in M_d lebenden Normalbasen von $M_d/\langle \mathcal{E}_d \rangle$.

1. (Ordnung vervollständigen) *Wie im Beweis zu Satz 1.6.14 setzen wir die Ordnung von Δ zu einer vollständigen Ordnung fort. Ohne Einschränkung sei dann $\Delta = \{1, \ldots, n\}$. Für $i = 0, \ldots, n$ seien $N_i := M_1 \oplus \cdots \oplus M_i$ und $Q_i := \sum_{j=1}^{i} \langle r + \mathfrak{n}_j(r);\ r \in \mathcal{E}_j \rangle$. Wir erhalten (wie im Beweis von Satz 1.6.14 gezeigt) die exakten Sequenzen*

$$0 \to N_{i-1}/Q_{i-1} \to N_i/Q_i \to M_i/\langle \mathcal{E}_i \rangle \to 0 \tag{72}$$

   für $i = 1, \ldots, n$.

2. (sukzessive Normalbasen konstruieren) *Für $i = 1, \ldots, n$ konstruiere man nun mittels Algorithmus 1.6.6 eine Normalbasis von N_i/Q_i aus Normalbasen von N_{i-1}/Q_{i-1} und $M_i/\langle \mathcal{E}_i \rangle$.*

   Nach Definition des Kombinates ist $L = N_n/Q_n$, daher ist eine Normalbasis von N_n/Q_n die gewünschte Normalbasis von L.

Algorithmus 1.6.15 funktioniert unabhängig davon, ob das $M\mathcal{E}\mathfrak{n}$-System gutartig ist oder nicht. Es sei dazu noch angemerkt, daß sich eine eventuelle Gutartigkeit des $M\mathcal{E}\mathfrak{n}$-Systems im Sinne von Definition 1.6.13 dadurch bemerkbar macht, daß bei der Anwendung von Algorithmus 1.6.4 (der von Algorithmus 1.6.6 benutzt wird) jedesmal der $\smile$-Unterfall eintritt.

Im Beweis von Satz 1.6.14 wurde gezeigt, daß aus der Gutartigkeit des $M\mathcal{E}\mathfrak{n}$-Systems Γ die Gutartigkeit der Sequenzen in (72) folgt. Insbesondere gilt dies für $i = n$, wenn $\Delta = \{1, \ldots, n\}$ ist. Wir halten dies in einer Bemerkung fest.

Bemerkung 1.6.16 *Es sei $\Gamma = (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d \leq n}$ ein kombinierbares, gutartiges $M\mathcal{E}\mathfrak{n}$-System mit Kombinat L.*

Darüber hinaus sei $N' := \bigoplus_{d<n} M_d$ und $Q' := \sum_{d<n} \langle r + \mathfrak{n}_d(r);\ r \in \mathcal{E}_d \rangle$.

Unter diesen Voraussetzungen ist die Sequenz

$$0 \to N'/Q' \to L \to M_n/\langle \mathcal{E}_n \rangle \to 0 \tag{73}$$

exakt und gutartig.

Satz 1.6.14 zeigt, wie man auf einfache Weise, nämlich durch Vereinigung, Basen eines Kombinates L eines kombinierbaren $M\mathcal{E}\mathfrak{n}$-Systems Γ konstruieren kann. Darüber hinaus kann man Basen von L_+ und L_- konstruieren, wenn Γ gutartig ist. Ist Γ nicht gutartig, so bietet sich noch für $|\Delta| < \infty$ der Ausweg eine Normalbasis von L mittels Algorithmus 1.6.15 zu konstruieren und von dieser Basen für L_+ und L_- nach Lemma 1.2.10 abzuleiten.

Möglicherweise ist aber Γ nur "teilweise", das heißt, bis zu einem gewissen Index D nicht gutartig. In diesem Fall gibt es noch die Möglichkeit, daß man Basen von L_+ und L_- zumindest ab D durch Vereinigen konstruieren kann. Die nächste Definition und der darauffolgende Satz zeigen, wie das gemeint ist.

Im folgenden vereinbaren wir, daß $0 \notin \Delta$ ist und die Ordnung von Δ auf $\Delta \cup \{0\}$ erweitert wird durch $0 < d$ für alle $d \in \Delta$.

Definition 1.6.17 *Es sei $\Gamma = (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d\in\Delta}$ ein kombinierbares $M\mathcal{E}\mathfrak{n}$-System und $D \in \Delta$. Dann definieren wir durch*

- $M_0 := \bigoplus_{t\le D} M_t$,
- $\mathcal{E}_0 := \bigcup_{t\le D}\{r + \mathfrak{n}_t(r);\ r \in \mathcal{E}_t\}$,
- $\mathfrak{n}_0 \equiv 0$

und $\Delta^D := \{0\} \cup \{t \in \Delta;\ t \not\le D\}$ das von Γ abgeleitete $M\mathcal{E}\mathfrak{n}$-System $\Gamma^D = (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d\in\Delta^D}$.

Bemerkung 1.6.18 *Es sei angemerkt, daß mit den obigen Bezeichnungen $M_0/\langle\mathcal{E}_0\rangle$ das Kombinat des $M\mathcal{E}\mathfrak{n}$-System $(M_t, \mathcal{E}_t, \mathfrak{n}_t)_{t\le D}$ ist, wie man direkt aus Definition 1.6.12 ablesen kann.*

Satz 1.6.19 *Ist Γ ein kombinierbares $M\mathcal{E}\mathfrak{n}$-System und $D \in \Delta$, dann ist das abgeleitete $M\mathcal{E}\mathfrak{n}$-System Γ^D kombinierbar, und die Kombinate von Γ und Γ^D sind gleich.*

Beweis
Die Behauptung ist offensichtlich, wenn man die Definition des Kombinates explizit hinschreibt: Ist $N'_d := \bigoplus_{t<d} M_t$ und $Q'_d := \sum_{t<d}\langle r + \mathfrak{n}_t(r);\ r \in \mathcal{E}_t\rangle$ für $d \in \Delta$, so ist die Eigenschaft, daß Γ kombinierbar ist, dadurch definiert, daß die Abbildungen $\mathfrak{n}_d : \mathcal{E}_d \to N'_d$ sich fortsetzen lassen zu Homomorphismen von $\langle\mathcal{E}_d\rangle$ nach N'_d/Q'_d.

Definieren wir diese Moduln entsprechend für Γ^D, so erhalten wir für $d \in \Delta^D$ mit $d \neq 0$, daß

$$N_d'^D = M_0 \oplus \bigoplus_{\substack{t<d \\ t \not\leq D}} M_t = \bigoplus_{t \leq D} M_t \oplus \bigoplus_{\substack{t<d \\ t \not\leq D}} M_t = N_d' \tag{74}$$

ist, und wenn wir $S_t := \langle r + \mathfrak{n}_t(r);\ r \in \mathcal{E}_t \rangle$ setzen, gilt

$$Q_d'^D = S_0 + \sum_{\substack{t<d \\ t \not\leq D}} S_t = \sum_{t \leq D} S_t + \sum_{\substack{t<d \\ t \not\leq D}} S_t = Q_d'. \tag{75}$$

Somit ist für alle $d \in \Delta^D$ mit $d \neq 0$ der Modul N_d'/Q_d' gleich dem Modul $N_d'^D/Q_d'^D$, und die $\mathfrak{n}_d$ sind zu Homomorphismen nach $N_d'^D/Q_d'^D$ fortsetzbar.
Es bleibt zu zeigen, daß die Kombinate gleich sind. Definieren wir aber $N := \bigoplus_{t \in \Delta} M_t$, $Q := \sum_{t \in \Delta} \langle r + \mathfrak{n}_t(r);\ r \in \mathcal{E}_t \rangle$, und entsprechend N^D und Q^D, so zeigt man genauso wie in (74) und (75), daß $N = N^D$ und $Q = Q^D$ ist. Insbesondere ist also das Kombinat N/Q gleich dem Kombinat N^D/Q^D.

QED.

Satz 1.6.19 erlaubt es im Fall, daß ein $M\mathcal{E}\mathfrak{n}$-System Γ nicht gutartig ist, eine Basis doch noch zu konstruieren, wenn man ein $D \in \Delta$ findet, so daß zumindest das abgeleitete $M\mathcal{E}\mathfrak{n}$-System Γ^D gutartig ist.

Dies wollen wir im folgenden durch ein Beispiel verdeutlichen. Im zweiten Kapitel werden zu jedem $n \in \mathbf{N}$ sogenannte Kreissysteme definiert und untersucht. Als Beispiel an dieser Stelle betrachten wir das 12-te Kreissystem. Die Definition des 12-ten Kreissystems wird im folgenden explizit angegeben. Zum Nachweis der Kombinierbarkeit und auch zum Verständnis der Sinnhaftigkeit der einzelnen Definitionen, insbesondere der der $\mathcal{E}_d$ und $\mathfrak{n}_d$, sei aber auf das zweite Kapitel verwiesen.

Beispiel
Es sei $\Delta = \{1, 2, 3, 4, 6, 12\}$ die Menge aller Teiler von 12, partiell geordnet durch Teilbarkeit. Wir definieren ein $M\mathcal{E}\mathfrak{n}$-System, indem wir zu jedem $d \in \Delta$ angeben, wie M_d, $\mathcal{E}_d$ und $\mathfrak{n}_d$ definiert sind.

- Es sei $G_d := \{1 \leq a < d;\ \gcd(a, d) = 1\}$ und $M_d := \langle G_d \rangle$ (mit $M_1 = 0$). Auf G_d, und damit auf M_d, operiere σ durch Negation modulo d. Wir schreiben, um die Elemente aus G_d von Zahlen aus $\mathbf{Z}$ zu unterscheiden, $a \in G_d$ als $[d, a]$. Es ist also beispielsweise $M_{12} = \langle [12, 1], [12, 5], [12, 7], [12, 11] \rangle$.

- Es seien $\mathcal{E}_1 := \mathcal{E}_2 := \mathcal{E}_3 := \emptyset$. Weiter seien

$$\begin{aligned} \mathcal{E}_4 := &\ \{[4,1] + [4,3]\}, \\ \mathcal{E}_6 := &\ \{[6,1], [6,5], [6,1] + [6,5]\}, \\ \mathcal{E}_{12} := &\ \{[12,1] + [12,7], [12,5] + [12,11], [12,1] + [12,5], \\ &\ [12,7] + [12,11]\}. \end{aligned}$$

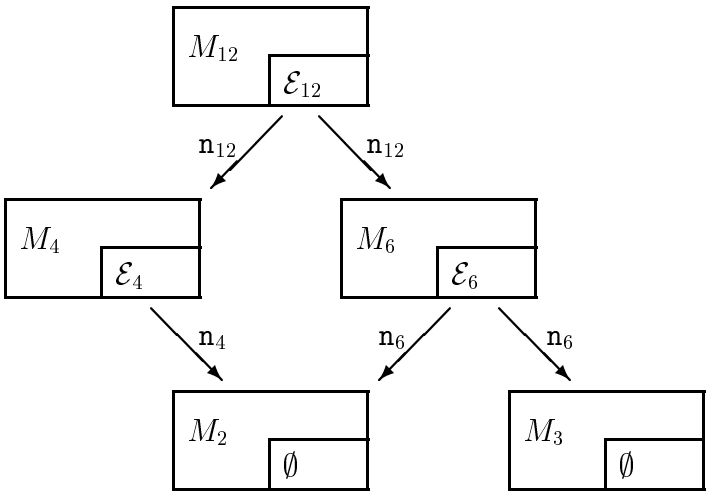
- Die Abbildungen $\mathfrak{n}_d : \mathcal{E}_d \to \bigoplus_{t|d,t\neq d} M_t$ sind folgendermaßen definiert. Zunächst sei $\mathfrak{n}_4([4,1]+[4,3]) = -[2,1]$, und $\mathfrak{n}_6$ und $\mathfrak{n}_{12}$ seien definiert durch

$$\begin{array}{rrcl} \mathfrak{n}_6 : & [6,1] & \mapsto & [3,2]-[3,1] \\ & [6,5] & \mapsto & [3,1]-[3,2] \\ & [6,1]+[6,5] & \mapsto & [2,1]-[2,1] \end{array} \tag{76}$$

und

$$\begin{array}{rrcl} \mathfrak{n}_{12} : & [12,1]+[12,7] & \mapsto & -[6,1] \\ & [12,5]+[12,11] & \mapsto & -[6,5] \\ & [12,1]+[12,5] & \mapsto & [4,3]-[4,1] \\ & [12,7]+[12,11] & \mapsto & [4,1]-[4,3]. \end{array} \tag{77}$$

Das dadurch definierte $M\mathcal{E}\mathfrak{n}$-System sieht dann schematisch wie folgt aus.

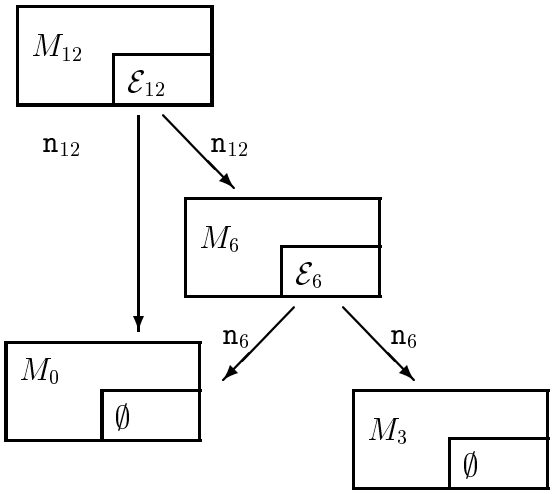


Den Nullmodul M_1 haben wir dabei weggelassen. Die Pfeile sind so zu verstehen, daß beispielsweise $\mathfrak{n}_{12}$ teilweise nach M_4 und teilweise nach M_6 abbildet. In (76) wurde dazu absichtlich suggestiv $[2,1]-[2,1]$ statt 0 geschrieben. Im allgemeinen bilden die $\mathfrak{n}_d$ beim Kreissystem in die Moduln $M_{d/p}$ ab, wobei p eine Primzahl ist, die d teilt (vergleiche Definition 2.2.1 im nächsten Kapitel). Die Kombinierbarkeit dieses $M\mathcal{E}\mathfrak{n}$-Systems $(M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d|12}$, das wir im folgenden mit $\Gamma(12)$ bezeichnen, wird im zweiten Kapitel in Lemma 2.2.3 bewiesen. Jedoch ist $\Gamma(12)$ nicht gutartig, da das Teilsystem $\Gamma(4) := (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d|4}$ schon nicht gutartig ist. Dies folgt aus der Nichtgutartigkeit der Sequenz

$$0 \to M_2 \to (M_2 \oplus M_4)/Q_4 \to M_4/\langle \mathcal{E}_4 \rangle \to 0 \tag{78}$$

mit $Q_4 = \langle [4,1]+[4,3]-[2,1] \rangle$. Man versuche beispielsweise eine Normalbasis von $(M_2 \oplus M_4)/Q_4$ aus der Normalbasis $[\emptyset,[2,1],\emptyset]$ von M_2 und der Normalbasis $[\emptyset,\emptyset,[4,1]]$ von $M_4/\langle \mathcal{E}_4 \rangle$ mit Hilfe von Algorithmus 1.6.6 zu konstruieren. Dabei tritt bei der Anwendung von Algorithmus 1.6.4, II. Fall der $\dot{-}$-Unterfall auf.

Abhilfe schafft das abgeleitete $M\mathfrak{En}$-System $\Gamma(12)^{(4)}$. Definieren wir $M_0 := M_2 \oplus M_4$ und $\mathcal{E}_0 := \{[4,1]+[4,3]-[2,1]\}$, so sieht das abgeleitete $M\mathfrak{En}$-System $\Gamma(12)^{(4)}$ so aus:



Dieses System ist nun in der Tat gutartig (was im zweiten Kapitel ausführlich nachgewiesen wird). Bezeichnet $\mathcal{L}(12)$ das Kombinat von $\Gamma(12)$, so erhalten wir Basen von $\mathcal{L}(12)_\pm$ durch Vereinigung von in M_d lebenden Basen der Moduln $(Y_d)_\pm := M_d/\langle\mathcal{E}_d\rangle_\pm$. Von den Y_d konstruieren wir jeweils eine Normalbasis (die Y_d sind alle als Zeilenfaktormoduln auffassbar, wobei $\mathcal{E}_d$ jeweils die Zeilensummen enthält), und fassen diese tabellarisch zusammen:

d:	0	3	6	12
Normalbasis von Y_d:	$[[4,1],\emptyset,\emptyset]$	$[[3,1],\emptyset,\emptyset]$	$[\emptyset,\emptyset,\emptyset]$	$[\emptyset,[12,1],\emptyset]$
Basis von $(Y_d)_+$:	$\{[4,1]\}$	$\{[3,1]\}$	$\emptyset$	$\{[12,1]\}$
Basis von $(Y_d)_-$:	$\{[4,1]\}$	$\{[3,1]\}$	$\emptyset$	$\emptyset$

Daraus lesen wir ab, daß $\{[4,1],[3,1],[12,1]\}$ eine Basis von $\mathcal{L}(12)_+$ ist und $\{[4,1],[3,1]\}$ eine Basis von $\mathcal{L}(12)_-$ ist.

2 Kreismoduln und Kreissysteme

In diesem Kapitel behandeln wir Kreissysteme, die definiert sind als $M\mathfrak{En}$-Systeme und im wesentlichen aus Kreismoduln gebildet werden. Diese Kreismoduln werden im ersten Abschnitt eingeführt und ausführlich untersucht. Insbesondere berechnen wir von diesen Normalbasen und Quasinormalbasen.

Im anschließenden zweiten Abschnitt definieren wir das Kreissystem $\Gamma(n)$, ein spezielles $M\mathfrak{En}$-System $(M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d\in\Delta}$, wobei die Moduln $M_d/\langle\mathcal{E}_d\rangle$ bis auf einige wenige Ausnahmen aus Kreismoduln bestehen. Um die Gutartigkeit des Systems zu untersuchen, benötigen wir den Wert von $m^+(\mathcal{L}(n))$, wobei $\mathcal{L}(n)$ das Kombinat von $\Gamma(n)$ ist. Dazu berechnen wir die σ-Kohomologie des Kombinates von $\mathcal{L}(n)$.

Das Kreissystem wird motiviert durch den Zusammenhang mit Kreiseinheiten. In Abschnitt 2.3 wird zunächst der offensichtliche Zusammenhang zu der Gruppe der Kreiszahlen, einer Gruppe, die die Gruppe der Kreiseinheiten als Untergruppe enthält, herausgearbeitet.

Abschließend wird im vierten Abschnitt das P-Kreissystem $\acute{\Gamma}(n)$ eingeführt und untersucht. Dieses bietet einen anderen Zugang zu den Kreiszahlen an als $\Gamma(n)$. Die Unterschiede zwischen $\Gamma(n)$ und $\acute{\Gamma}(n)$ werden ausführlich diskutiert.

In diesem Kapitel bezeichnen wir durchgängig mit G_d die Menge

$$G_d := \{1 \le a < d;\ \gcd(a,d) = 1\}. \tag{79}$$

Da im folgenden oft mit $\langle G_d\rangle$, also dem $\mathbf{Z}$-Erzeugnis von G_d, gearbeitet wird, gibt es zwei Möglichkeiten, den Ausdruck $a+b$ mit $a, b \in G_d$ zu interpretieren. Einmal als "normale" Addition zweier ganzer Zahlen, und einmal als Addition innerhalb des Moduls $\langle G_d\rangle$. Daher schreiben wir dort, wo es zu Mißverständnissen kommen kann, $a \in G_d$ auch als $[a]$ oder sogar als $[d, a]$ wie im Beispiel am Ende des ersten Kapitels, und meinen damit das Element im Modul $\langle G_d\rangle$. Wir halten also fest:

- Ausdrücke wie $\sum_{a\in G_d}[a]$ oder $[a]+[b]$ mit $a, b \in G_d$ bedeuten die Moduladdition in $\langle G_d\rangle$.
- Ausdrücke wie $\sum_{a\in G_d} a$ und $a + b$ mit $a, b \in G_d$ bedeuten die Addition in $\mathbf{Z}$.

2.1 Der Kreismodul

In diesem Abschnitt definieren wir zu $n \in \mathbf{N}$ den Kreismodul $Z(n)$, der als Tensorprodukt gewisser Zeilenfaktormoduln erklärt ist. Nach der Definition im ersten Abschnitt geben wir im zweiten Abschnitt Normalbasen und Quasinormalbasen von $Z(n)$ an.

Im dritten Abschnitt zeigen wir einen anderen Zugang zu $Z(n)$ auf, indem wir $Z(n)$ als Modul der Form $\langle G_n\rangle/\langle\mathcal{E}_n\rangle$ interpretieren, wobei $\mathcal{E}_n$ den Zeilensummen entspricht.

2.1.1 Definition des Kreismoduls

Definition 2.1.1 *Zu $n \in \mathbf{N}$ definieren wir den Kreismodul $Z(n)$ wie folgt:*

a) Ist $n = p$ Primzahl, dann sei $Z(p) := \langle G_p \rangle / \langle \sum_{a \in G_p} [a] \rangle$.
Auf G_p (und damit auf $Z(p)$) operiere σ durch $\sigma a := p - a$.

b) Ist $n = q = p^\alpha$ die Potenz einer Primzahl mit $\alpha > 1$, so setzen wir $\Lambda_q := G_{q/p}$ und $A_p := \{0, \ldots, p-1\}$. Wir definieren

$$Z(q) := \langle \Lambda_q \rangle \otimes \langle A_p \rangle / \langle \sum_{a \in A_p} [a] \rangle. \tag{80}$$

Auf A_p operiere σ durch $\sigma a := p - 1 - a$, auf Λ_q operiere σ durch $\sigma \lambda := q/p - \lambda$, und auf $Z(q)$ operiere σ diagonal.

c) Ist $n = q_1 \cdots q_r$ das Produkt von paarweise teilerfremden Primzahlpotenzen, so definieren wir $Z(n) := Z(q_1) \otimes \cdots \otimes Z(q_r)$. Auf $Z(n)$ operiere σ diagonal.

Die Kreismoduln sind also gewisse Zeilenfaktormoduln, wie sie in Abschnitt 1.4 behandelt wurden. Insbesondere ist $Z(p)$ in Fall a der nichttriviale elementare Zeilenfaktormodul zu G_p, und $Z(q)$ in Fall b ist der Zeilenfaktormodul zu $\Lambda_q \times A_p$, wobei nur A_p echter Faktor ist. Da das Tensorprodukt von Zeilenfaktormoduln wieder ein Zeilenfaktormodul ist, sind auch die $Z(n)$ in Teil c Zeilenfaktormoduln.

Lemma 2.1.2 *Der Rang von $Z(n)$ ist gleich*

$$\prod_{p|n} (\varphi(p^{\alpha_p}) - \varphi(p^{\alpha_p - 1})), \tag{81}$$

wobei p alle Primteiler von n durchläuft und α_p der Exponent von p in n ist.

Beweis
Bei der Tensorproduktbildung multiplizieren sich die Ränge, somit ist nur zu zeigen, daß der Rang von $Z(p^{\alpha_p})$ gleich $\varphi(p^{\alpha_p}) - \varphi(p^{\alpha_p - 1})$ ist.
Für $\alpha_p = 1$ hat $Z(p)$ den Rang $|G_p| - 1 = \varphi(p) - 1$. Ist $\alpha_p > 1$ und $q = p^{\alpha_p}$, so hat Λ_q den Rang $\varphi(p^{\alpha_p - 1})$ und A_p den Rang $p - 1$, womit die Behauptung folgt.

QED.

2.1.2 Normalbasen des Kreismoduls

Grundsätzlich ist die Konstruktion einer Normalbasis des Kreismoduls geklärt, denn Elementarzerlegungen von G_q, Λ_q und A_p sind einfach zu erhalten (wir

werden sie später angeben). Eine Basis erhält man daher mit den im ersten Kapitel hergeleiteten Mechanismen. In diesem Sinne ist dieser Abschnitt nur eine Zusammenfassung von Anwendungen dieser Mechanismen. Dabei treten in Abhängigkeit von n jedoch wesentlich verschiedene Fälle auf, die im folgenden einzeln abgehandelt werden.

$n \equiv 2 \bmod 4$
Dieser Fall ist besonders einfach. Da $Z(2) = 0$ ist, und $Z(2)$ als Faktor des Tensorproduktes von $Z(n)$ auftritt ist $Z(n) = 0$, die Basis ist somit leer.

n quadratfrei und ungerade
Wir geben den Konstruktionsprozeß in mehreren Schritten an.

- Für eine Primzahl p ist eine Normalzerlegung $[E_p^0, E_p^+]$ von G_p gegeben durch $E_p^+ := \emptyset$ und beispielsweise $E_p^0 := \{1, \ldots, \lfloor p/2 \rfloor\}$.

- Lemma 1.4.6 zeigt, wie man für Zeilenfaktormoduln aus einer Normalzerlegung eine Normalbasis erhält. Beispielsweise ist $[F_p^0, F_p^+, F_p^-]$ mit

$$F_p^0 := \{2, \ldots, \lfloor p/2 \rfloor\}, \quad F_p^+ := \emptyset, \quad F_p^- := \{ \sum_{a=1}^{\lfloor p/2 \rfloor} [a] \}$$

  eine Normalbasis von $Z(p)$.

  Unschön an dieser Normalbasis ist die Summe in F_p^-. Einen Ausweg bietet die Quasinormalbasis $[G_p^0, G_p^+, G_p^-]$ mit

$$G_p^0 := F_p^0, \quad G_p^+ := \emptyset, \quad G_p^- := \{1\}.$$

- $Z(n)$ ist als Tensorprodukt von Kreismoduln $Z(p)$ definiert, wobei p die Primzahlen durchläuft, die n teilen. Daher können wir aus Korollar 1.3.9, b eine Normalbasis und eine Quasinormalbasis von $Z(n)$ explizit ablesen. Ist $n = p_1 \cdots p_r$, so sieht die Quasinormalbasis $[G^0, G^+, G^-]$ wie folgt aus:

$$G^0 := \bigcup_{i=1}^{r} \{(1, \ldots, 1, a_i, \ldots, a_r) \in G_{p_1} \times \cdots \times G_{p_r};\ 1 < a_i < p_i/2, \text{ und } 1 \le a_j < p_j - 1 \text{ für } j = i+1, \ldots, r\}$$
$$G^+ := \{(1, \ldots, 1)\}, \text{ falls } r \text{ gerade und } G^+ := \emptyset, \text{ falls } r \text{ ungerade},$$
$$G^- := \{(1, \ldots, 1)\} \setminus G^+.$$

  Eine Normalbasis $[F^0, F^+, F^-]$ ist ähnlich wie die Quasinormalbasis aufgebaut, jedoch muß das Quasinormalbasiselement "1" aus G_{p_i} durch die Summe "$\sum_{a=1}^{\lfloor p_i/2 \rfloor} [a]$" für das entsprechende p_i ersetzt werden, was F^0 recht unübersichtlich macht. F^+ und F^- sind gegeben durch

$$F^+ := \{f\}, \text{ falls } r \text{ gerade und } F^+ := \emptyset, \text{ falls } r \text{ ungerade},$$
$$F^- := \{f\} \setminus F^+,$$

jeweils mit

$$f = \sum_{a_1=1}^{\lfloor p_1/2 \rfloor} \sum_{a_2=1}^{\lfloor p_2/2 \rfloor} \cdots \sum_{a_r=1}^{\lfloor p_r/2 \rfloor} (a_1, a_2, \ldots, a_r). \tag{82}$$

$n = 4u$ mit u quadratfrei und ungerade

Dieser Fall läßt sich wie folgt auf den vorhergehenden Fall zurückführen.

- Es ist $Z(4)$ der Zeilenfaktormodul zu $\Lambda_4 \times A_2 = \{1\} \times \{0, 1\}$, wobei nur A_2 echter Faktor ist. Eine Normalbasis ist gegeben durch $[\emptyset, \emptyset, \{(1, 0)\}]$.
- Nun können wir $Z(n)$ schreiben als $Z(4) \otimes Z(u)$, und entsprechend Normalbasen mit Hilfe des vorigen Abschnitts konstruieren. Beispielsweise sind wie in (82) im Fall n ungerade und quadratfrei F^+ und F^- in Abhängigkeit von r gegeben durch

$$f = \sum_{a_2=1}^{\lfloor p_2/2 \rfloor} \cdots \sum_{a_r=1}^{\lfloor p_r/2 \rfloor} (1, 0, a_2, \ldots, a_r), \tag{83}$$

  wobei $n = 4p_2 \cdots p_r$ ist.

Sonstige n

In der Zerlegung $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = q_1 \cdots q_r$ ist mindestens für ein i sowohl $\alpha_i > 1$ als auch $q_i > 4$. Es sei $p := p_i$ und $q := q_i$.

Eine Normalzerlegung der Menge Λ_q ist gegeben durch $[H_q, \emptyset]$ mit beispielsweise $H_q := \{\lambda \in \Lambda_q;\ 1 \le \lambda < \frac{1}{2}q/p\}$. Wir schreiben $Z(n) = \langle \Lambda_q \rangle \otimes X$, wobei X der Zeilenfaktormodul ist, der die gleichen Faktoren von $Z(n)$ enthält mit der Ausnahme, daß Λ_q fehlt. Explizit ist $X = (A_p / \langle \sum_{a \in A_p} [a] \rangle) \otimes Z(n/q)$.

In Korollar 1.3.9, a zu Satz 1.3.8 wird gezeigt, wie man eine Basis von $\langle \Lambda_q \rangle \otimes X$ konstruiert. Demnach ist $[H_q \times B, \emptyset, \emptyset]$ eine Normalbasis von $Z(n)$, wenn B eine beliebige Basis von X ist, beispielsweise die Basis aus Lemma 1.4.5.

Ordnen wir also die Primfaktoren von n so, daß $p_1 = p$ ist und ein t existiert mit $\alpha_i = 1$ genau dann, wenn $i > t$ ist, das heißt, ist $n = p^\alpha p_2^{\alpha_2} \cdots p_t^{\alpha_t} p_{t+1} \cdots p_r$, so ist eine Normalbasis $[F^0, \emptyset, \emptyset]$ von $Z(n)$ explizit gegeben durch

$$F^0 = H_{q_1} \times A_{p_1}^\flat \times \prod_{i=2}^{t} (\Lambda_{q_i} \times A_{p_i}^\flat) \times \prod_{i=t+1}^{r} G_{p_i}^\flat, \tag{84}$$

wobei $A_{p_i}^\flat$ aus A_{p_i} und $G_{p_i}^\flat$ aus G_{p_i} jeweils durch Entfernen eines (beliebigen) Elements hervorgeht. Beispielsweise kann man $A_{p_i}^\flat := \{1, \ldots, p_i - 1\}$ und $G_{p_i}^\flat := \{2, \ldots, p_i - 1\}$ wählen.

Zusammenfassend läßt sich sagen, daß bei der Konstruktion von Normalbasen von Kreismoduln drei wesentlich unterschiedliche Fälle auftreten, nämlich

- der triviale Fall, daß $n \equiv 2 \bmod 4$ und daher $Z(n) = 0$ ist,

- der Fall, daß $n = u$ oder $n = 4u$ ist, wobei u ungerade und quadratfrei ist. In diesem Fall enthält die Normalzerlegung von $Z(n)$ einen eindimensionalen, je nach Anzahl der Primfaktoren, + oder − Anteil,
- alle anderen Fälle. In diesen Fällen ist $Z(n) = Z(n)^0$, das heißt, in der Normalzerlegung kommen weder + noch − Anteile vor.

2.1.3 Der Kreismodul als Erzeugnis von G_n

Zur Konstruktion einer Basis war es nützlich, $Z(n)$ als Tensorprodukt von anderen Kreismoduln definiert zu haben. Bei der diesem Abschnitt folgenden Konstruktion des Kreissystems ist es praktischer, $Z(n)$ als $\langle G_n\rangle/R_n$ interpretieren zu können, wobei R_n eine geeignete Menge von Relationen ist.
Es gilt der folgende Satz:

Satz 2.1.3 *Es sei $Z(n)$ der n-te Kreismodul. Dann ist $Z(n) \cong \langle G_n\rangle/R_n$, wobei σ auf G_n durch Negation modulo n, also durch $\sigma a := n - a$ für $a \in G_n$ operiert. Dabei wird R_n erzeugt durch*

$$\mathcal{E}_n := \{s(n,p,a);\ p|n \text{ mit } p \text{ prim},\ a \in G_n\} \tag{85}$$

mit

$$s(n,p,a) := \sum_{\substack{x \in G_n \\ x \equiv a \bmod (n/p)}} [x]. \tag{86}$$

Beweis
Die Primfaktoren p_i von n seien so bezeichnet, daß

$$n = p_1^{\alpha_1} \cdots p_t^{\alpha_t} p_{t+1} \cdots p_r \tag{87}$$

mit $\alpha_i > 1$ für $i = 1, \ldots, t$ ist. Weiter sei $q_i = p_i^{\alpha_i}$ für $i = 1, \ldots, t$ und $q_i = p_i$ sonst. Die Mengen Λ_{q_i} und A_{p_i} seien wie in Definition 2.1.1 definiert. Nach Satz 1.4.3 ist dann $Z(n)$ isomorph zum Zeilenfaktormodul Y zu

$$S := \Lambda_{q_1} \times A_{p_1} \times \cdots \times \Lambda_{q_t} \times A_{p_t} \times G_{p_{t+1}} \times \cdots \times G_{p_r}, \tag{88}$$

wobei genau die Faktoren A_{p_i} für $1 \le i \le t$ und G_{p_i} für $t < i \le r$ echt sind. Wir zeigen $Y \cong \langle G_n\rangle/R_n$.
Wir benutzen dazu die mit σ verträgliche Bijektion $\xi := \psi \circ \kappa : G_n \to S$ gemäß

$$G_n \xrightarrow{\psi} G_{q_1} \times \cdots \times G_{q_r} \xrightarrow{\kappa} S, \tag{89}$$

wobei ψ und κ wie folgt definiert sind:

- Es ordne ψ jedem $a \in G_n$ das Tupel $(a_1, \ldots, a_r)$ zu, so daß $a_i \equiv a \bmod q_i$ für $i = 1, \ldots, r$ gilt. Nach dem Chinesischen Restsatz ist ψ wohldefiniert und bijektiv.

- Die Abbildung κ ist folgendermaßen komponentenweise definiert. Schreiben wir $\kappa(a_1,\ldots,a_r)=(\kappa_1(a_1),\ldots,\kappa_r(a_r))$, so sei κ_i für $i=t+1,\ldots,r$ die Identität. Für $i=1,\ldots,t$ und $c\in G_{q_i}$ sei $\kappa_i(c)=(\lambda,b)\in\Lambda_{q_i}\times A_{p_i}$ so definiert, daß $c=bp_i^{\alpha_i-1}+\lambda$ gilt. Konkret ist also $\lambda\equiv c \bmod p_i^{\alpha_i-1}$ und $b:=(c-\lambda)/p_i^{\alpha_i-1}$.

Mit ξ erhält man einen Isomorphismus zwischen $\langle G_n\rangle$ und $\langle S\rangle$. Direkt rechnet man nach, daß dabei die $s(n,p,a)$ aus (86) auf die Zeilensummen von Y abgebildet werden. Für $a\in G_n$ gilt nämlich

$$s(n,p_i,a)\mapsto\begin{cases} s_{A_{p_i}}(\xi(a)) & \text{für } 1\le i\le t,\\ s_{G_{p_i}}(\xi(a)) & \text{für } t<i\le r.\end{cases} \tag{90}$$

Jeder Zeilensumme von Y entspricht also ein $s(n,p_i,a)$ und umgekehrt. Somit ist $\langle G_n\rangle/R_n\cong Y$ gezeigt.

QED.

Motiviert durch (90) bezeichnen wir im folgenden die $s(n,p_i,a)$ aus (86) ebenfalls als *Zeilensummen*.

Bemerkung 2.1.4 *Genaugenommen reicht es in (85) aus, wenn a aus $G_{n/p}$ ist: Die Zuordnung, die jedem Paar (p,a) mit $p|n$ Primzahl und $a\in G_{n/p}$ die Zeilensumme $s(n,p,a)$ zuordnet, ist bijektiv, denn für $a,b\in\mathbf{Z}$ gilt $s(n,p,a)=s(n,p,b)$ genau dann, wenn $a\equiv b \bmod n/p$ ist.*

2.2 Das Kreissystem

2.2.1 Definition

Das Kreissystem ist ein gewisses $M\mathfrak{En}$-System $(M_d,\mathcal{E}_d,\mathfrak{n}_d)_{d\in\Delta}$. Dabei sind die Moduln $M_d/\langle\mathcal{E}_d\rangle$ im wesentlichen die im vorhergehenden Abschnitt ausführlich behandelten Kreismoduln $Z(d)$.

Zunächst führen wir einige Bezeichnungen ein.

- Auf G_d lassen wir die multiplikative Gruppe $V_d:=\{r/s\in\mathbf{Q};\ (r,d)=(s,d)=1\}$ durch Multiplikation modulo d operieren. Damit ist eine Operation des Gruppenrings $\mathbf{Z}V_d$ auf $M_d=\langle G_d\rangle$ definiert. Ist $a\in G_d$ und p teilerfremd zu d, so ist damit beispielsweise $(p^{-1}-1)[a]=[a']-[a]$, wobei für $a'\in G_d$ gilt, daß $pa'\equiv a \bmod d$ ist.

- Gilt $t|d$ für $t,d\in\mathbf{N}$, so bezeichne zu $a\in G_d$ die Schreibweise $b:=a \bmod t$ dasjenige eindeutig bestimmte $b\in G_t$, mit $b\equiv a \bmod t$.

- Die Schreibweise $t||d$ bedeute, daß t ein Teiler von d und ungleich d ist.

- Im folgenden treten im wesentlichen zwei Typen von Indexmengen Δ auf. Einerseits ist Δ die endliche Menge aller Teiler d einer natürlichen Zahl

n. Andererseits ist Δ die Menge $\mathbf{N}$ der natürlichen Zahlen. In einigen Fällen bietet es sich an, den endlichen und unendlichen Fall gemeinsam zu behandeln. Wir vereinbaren dafür die folgende Sprechweise. Wir fügen ein neues Symbol ∞ zu $\mathbf{N}$ hinzu, und es sei $\mathbf{N}_\infty := \mathbf{N} \cup \{\infty\}$. Die Menge aller Teiler von ∞ sei gleich $\mathbf{N}$ (und nicht etwa $\mathbf{N}_\infty$). Ein Ausdruck wie $\bigcup_{d|\infty} B_d$ ist damit gleichbedeutend mit $\bigcup_{d\in\mathbf{N}} B_d$.

Es folgt nun die Definition des kombinierten Kreismoduls $\mathcal{L}(n)$. Dieser entsteht als Kombinat eines gewissen $M\mathfrak{En}$-Systems $\Gamma(n)$. Wir definieren zunächst dieses System, und zeigen anschließend, daß es auch in der Tat kombinierbar ist.

Definition 2.2.1 *Zu $d \in \mathbf{N}$ sei $M_d := \langle G_d \rangle$, und ist d keine Primzahl, dann sei $\mathcal{E}_d \subseteq M_d$ die Menge aller Zeilensummen $s(d,p,a)$ mit $a \in G_d$ und $p|d$ Primzahl gemäß (86).*

Ist d Primzahl, dann sei $\mathcal{E}_d$ leer.

Weiter seien auf den Zeilensummen Abbildungen $\mathfrak{n}_d : \mathcal{E}_d \to \bigoplus_{t||d} M_t$ gegeben, indem wir $s(d,p,a) \in \mathcal{E}_d$ das Element $g_{p,d}[a \bmod d/p] \in M_{d/p}$ zuordnen, wobei $g_{p,d} \in \mathbf{Z}V_{d/p}$ definiert ist durch

$$g_{p,d} := \begin{cases} -1 & \text{falls } p^2|d, \\ p^{-1} - 1 & \text{falls } p^2 \nmid d. \end{cases} \tag{91}$$

Zu $n \in \mathbf{N}_\infty$ heißt das $M\mathfrak{En}$-System $\Gamma(n) := (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d|n}$ das n-te Kreissystem. *Die Menge aller Teiler von n sei dabei durch Teilbarkeit geordnet.*

Bemerkung 2.2.2 *Explizit ist also*

$$\mathfrak{n}_d(s(d,p,a)) = g_{p,d}[a \bmod d/p] = \begin{cases} -[a \bmod d/p] & \text{falls } p^2|d, \\ [a' \bmod d/p] - [a \bmod d/p] & \text{falls } p^2 \nmid d, \end{cases} \tag{92}$$

mit $a' \in G_{d/p}$ so, daß $pa' \equiv a \bmod d/p$ gilt.

Lemma 2.2.3 *Es sei $n \in \mathbf{N}_\infty$. Dann ist das n-te Kreissystem $\Gamma(n)$ kombinierbar.*

Beweis

Zu $d|n$ seien $N'_d := \bigoplus_{t||d} M_t$ und $Q'_d := \sum_{t||d} \langle r + \mathfrak{n}_t(r);\ r \in \mathcal{E}_t \rangle$. Es ist zu zeigen, daß sich die Abbildungen $\mathfrak{n}_d$ fortsetzen lassen zu $\mathbf{Z}[\sigma]$-Homomorphismen $\bar{\mathfrak{n}}_d : \langle \mathcal{E}_d \rangle \to N'_d/Q'_d$.

Alle Relationen innerhalb der Zeilensummen entstehen nach Satz 1.4.7 durch Doppelsummen. Wir bezeichnen die Doppelsummen als $s(d,p,q,a)$ mit zwei Primzahlen $q \neq p$, die d teilen. Explizit sind diese definiert als

$$s(d,p,q,a) = \sum_{\substack{x \in G_d \\ x \equiv a \bmod d/p}} s(d,q,x). \tag{93}$$

Der Doppelsummenrelation (26) entspricht dann die Relation $s(d,q,p,a) = s(d,p,q,a)$, und es ist

$$\sum_{\substack{x\in G_d\\ x\equiv a \bmod d/q}} \mathfrak{n}_d(s(d,p,x)) \equiv \sum_{\substack{x\in G_d\\ x\equiv a \bmod d/p}} \mathfrak{n}_d(s(d,q,x)) \mod Q'_d \tag{94}$$

zu zeigen, um $\bar{\mathfrak{n}}_d$ eindeutig auf $s(d,p,q,a) = s(d,q,p,a)$ definieren zu können.

Ist $d = pq$, so benutzen wir, daß p^{-1} die Menge G_q wieder auf sich selbst abbildet. Die linke Seite von (94) ist gleich

$$\sum_{\substack{x\in G_d\\ x\equiv a \bmod d/q}} (p^{-1}-1)[x \bmod q] = \sum_{b\in G_q}(p^{-1}-1)[b] = \sum_{b\in G_q}[b] - \sum_{b\in G_q}[b] = 0. \tag{95}$$

Vertauschen wir p und q, so zeigt dies, daß auch die rechte Seite von (94) gleich 0 ist.

Es sei $d \neq pq$. Wie in (91) definieren wir $g_{p,d} := -1$ für $p^2|d$ und $g_{p,d} := p^{-1}-1$ sonst. Dann ist die linke Seite von (94) gleich

$$\begin{aligned} \sum_{\substack{x\in G_d\\ x\equiv a \bmod d/q}} g_{p,d}[x \bmod d/p] &= g_{p,d}s(d/p,q,a) \\ &\equiv -g_{p,d/q}\mathfrak{n}_{d/p}(s(d/p,q,a)) \quad \mod Q'_d \\ &= -g_{p,d/q}g_{q,d/p}[a \bmod d/(qp)]. \end{aligned} \tag{96}$$

Die rechte Seite von (94) ist analog gleich $-g_{q,d/p}g_{p,d/q}[a \bmod d/(qp)]$. Da $g_{p,d/q}$ und $g_{q,d/p}$ kommutieren, folgt die Kongruenz in (94), und $\mathfrak{n}_d$ läßt sich modulo Q'_d daher auf die Doppelsummen, und damit auf $\langle\mathcal{E}_d\rangle$ fortsetzen.

Es kommutiert σ mit der Operation von $g_{p,d}$, und direkt aus der Definition der Zeilensummen in (86) folgt $\sigma(s(d,p,a)) = s(d,p,\sigma a)$. Damit gilt $\bar{\mathfrak{n}}_d(\sigma r) = \sigma\bar{\mathfrak{n}}_d(r)$ für $r \in \langle\mathcal{E}\rangle$, das heißt, $\bar{\mathfrak{n}}_d$ ist in der Tat auch $\mathbf{Z}[\sigma]$-Homomorphismus.

QED.

Definition 2.2.4 *Es sei $n \in \mathbf{N}_\infty$. Das Kombinat $\mathcal{L}(n)$ des n-ten Kreissystems $\Gamma(n)$ heißt* n-ter kombinierter Kreismodul.

Lemma 2.2.5 *Das Kombinat $\mathcal{L}(n)$ des n-ten Kreissystems ist frei.*

Beweis

Nach Satz 1.6.14 ist zu zeigen, daß $M_d/\langle\mathcal{E}_d\rangle$ aus Definition 2.2.1 für alle $d|n$ frei ist.

Ist d Primzahl, so ist $\mathcal{E}_d = \emptyset$ und daher $M_d/\langle\mathcal{E}_d\rangle \cong M_d = \langle G_d\rangle$ offensichtlich frei. Sonst ist $M_d/\langle\mathcal{E}_d\rangle$ nach Satz 2.1.3 isomorph zum Kreismodul $Z(d)$, der als Zeilenfaktormodul nach Definition 2.2.1 und Lemma 1.4.5 frei ist.

QED.

2.2.2 Kohomologie

Um die Gutartigkeit des Kreissystems $\Gamma(n)$ zu untersuchen, brauchen wir unter anderen den Wert $m^+(\mathcal{L}(n))$. Nach Lemma 1.2.4 ist $m^+(\mathcal{L}(n))$ die $\mathbf{F}_2$-Dimension der 0-ten Kohomologiegruppe von $\mathcal{L}(n)$. Wir berechnen daher in diesem Abschnitt die σ-Kohomologie von $\mathcal{L}(n)$. Dies geschieht dadurch, daß wir $\mathcal{L}(n)$ als isomorph zu einem von C. G. Schmidt in [12] eingeführten Modul nachweisen, dessen Kohomologie bekannt ist.

Satz 2.2.6 *Zu $n \in \mathbf{N}$ sei r die Anzahl der Primteiler von n. Wir definieren $r' = r$, falls $n \not\equiv 2 \bmod 4$ und $r' = r - 1$ sonst.*
Es sei $n > 2$ und $\mathcal{L}(n)$ der n-te kombinierte Kreismodul. Dann gilt:

i) $H^0(\sigma, \mathcal{L}(n)) \cong \begin{cases} \mathbf{F}_2^{2^{r'-1}-1} & \text{falls } n \not\equiv 2 \bmod 4, \\ \mathbf{F}_2^{2^{r'-1}} & \text{falls } n \equiv 2 \bmod 4. \end{cases}$

ii) $H^1(\sigma, \mathcal{L}(n)) \cong \mathbf{F}_2^{2^{r'-1}-r'}$.

Beweis
Die Behauptung, die hier für $\mathcal{L}(n)$ aufgestellt wird, findet sich in [12], Satz 2, für einen gewissen Modul $A = V/U$, wobei in diesem Fall r' die Anzahl der im n-ten Kreisteilungskörper verzweigenden Primzahlen ist, was (beispielsweise nach [9], Kapitel I, Korollar (10.4)) der hier explizit gegebenen Definition von r' entspricht. Wir zeigen Satz 2.2.6, indem wir einen Isomorphismus zwischen A und $\mathcal{L}(n)$ angeben.
Der Schmidtsche Faktormodul A ist in [12] definiert als freier $\mathbf{Z}$-Modul V über der Menge $(\mathbf{Z}/n\mathbf{Z}) \setminus \{0\}$, die in [12] mit $\{e(1), \ldots, e(n-1)\}$ bezeichnet wird, modulo einem Teilmodul U, der nach (1.7) in [12] von den Elementen der Form

$$a(d, x) := e(dx) - \sum_{\nu=0}^{d-1} e(x + \nu \frac{n}{d}) \tag{97}$$

für $d|n$ und $x = 1, \ldots, n/d - 1$ erzeugt wird.
Es sei also $\Gamma(n) := (M_d, \mathcal{E}_d, \mathtt{n}_d)_{d|n}$ das n-te Kreissystem. Dann ist nach Definition 1.6.12 $\mathcal{L}(n) = N/Q$ mit $N := \bigoplus_{d|n} M_d$ und $Q := \sum_{d|n} \langle r + \mathtt{n}_d(r);\ r \in \mathcal{E}_d \rangle$.
Wir schreiben die Erzeuger von N als $[d, a]$ mit $d|n$ und $a \in G_d$. Die Zeilensummen schreiben wir eindeutig nach Bemerkung 2.1.4 als $s(d, p, a)$ mit $p|d$ und $a \in G_{d/p}$.
Wir beweisen den Isomorphismus zwischen $A = V/U$ und $\mathcal{L}(n) = N/Q$ in zwei Schritten, indem wir zunächst $N \cong V$ und anschließend $Q \cong U$ zeigen.

$N \cong V$: Der Isomorphismus ist gegeben durch die Abbildung $[d, a] \mapsto e(a\frac{n}{d})$.
Die Umkehrabbildung ist gegeben durch $e(x) \mapsto [\frac{n}{t}, \frac{x}{t}]$ mit $t = \gcd(n, x)$.

$\underline{Q \cong U}$: Wir zeigen zur Vorbereitung zunächst ein Lemma, das mit elementarer Kongruenzrechnung bewiesen wird.

Lemma 2.2.7 *Zu $d \in \mathbf{N}$, $p|d$ prim und $b \in G_{d/p}$ seien*

$$\begin{aligned} X &:= \{0 \le x < d;\ x \equiv b \bmod \frac{d}{p}\}, \\ Y &:= \{x \in G_d;\ x \equiv b \bmod \frac{d}{p}\}. \end{aligned} \tag{98}$$

Dann gilt:

a) $X = \{b + \nu\frac{d}{p};\ \nu = 0, \ldots, p-1\}$

b) $X = \begin{cases} Y & \text{falls } p^2|d \\ Y \cup \{pb'\} & \text{falls } p^2 \not| d \end{cases}$

mit $b' \in G_{d/p}$ so, daß $pb' \equiv b \bmod d/p$ gilt.

Beweis von Lemma 2.2.7
Teil a folgt direkt, indem man "$\subseteq$" und "$\supseteq$" nachrechnet. In Teil b ist $Y \subseteq X$ trivial. Wir unterscheiden nun die beiden Fälle $p^2|d$ und $p^2 \not| d$.

$\underline{p^2|d}$: Da $b \in G_{d/p}$ ist, ist x mit $x \equiv b \bmod d/p$ teilerfremd zu d/p und damit auch teilerfremd zu d, also $X = Y$.

$\underline{p^2 \not| d}$: Offensichtlich ist $pb' \in X$ und daher $Y \cup \{pb'\} \subseteq X$. Um "$\supseteq$" zu zeigen, wählen wir $x \in X$. Ist $x \not\equiv 0 \bmod p$, so ist x teilerfremd sowohl zu p als auch zu d/p und daher teilerfremd zu d, und x liegt also in Y. Im anderen Fall erfüllt x das System simultaner Kongruenzen

$$\begin{aligned} x &\equiv 0 \mod p \\ x &\equiv b \mod d/p, \end{aligned} \tag{99}$$

das ebenfalls von $pb' \in X$ gelöst wird. Nach dem Chinesischen Restsatz ist die Lösung von (99) modulo d eindeutig, es gilt also $x = pb'$.

Wir zeigen nun $Q \cong U$. Es wird Q von Elementen der Form $s(d,p,b) + \mathfrak{n}_d(s(d,p,b))$ erzeugt, wobei $s(d,p,b)$ eine Zeilensumme gemäß (86) ist, und U ist das Erzeugnis der $a(d,x)$ aus (97). Mit X,Y und b' aus (98) ist

$$-a(p, \frac{n}{d}b) = -e(\frac{np}{d}b) + \sum_{\nu=0}^{p-1} e(\frac{n}{d}\left(b + \nu\frac{d}{p}\right)) = -e(\frac{np}{d}b) + \sum_{x \in X} e(\frac{n}{d}x), \tag{100}$$

und $s(d,p,b)+\mathfrak{n}_d(s(d,p,b))$ wird nach (86) (Definition von $s(d,p,b)$) und (91) (Definition von $\mathfrak{n}_d$) auf

$$\begin{cases} \sum_{x\in Y} e(\frac{n}{d}x) - e(\frac{np}{d}b) & \text{falls } p^2|d \\ \sum_{x\in Y} e(\frac{n}{d}x) + e(\frac{np}{d}b') - e(\frac{np}{d}b) & \text{falls } p^2 \not| d \end{cases} \tag{101}$$

abgebildet. Mit Lemma 2.2.7 folgt durch Vergleich von (100) und (101), daß $s(d,p,b)+\mathfrak{n}_d(s(d,p,b))$ auf $-a(p,\frac{n}{d}b)$ abgebildet wird.

Umgekehrt hat $-a(p,x)$ mit $p|n$ und $1 \le x < n/p$ als Urbild

$$s(\frac{n}{t},p,\frac{x}{t}) + \mathfrak{n}_d(s(\frac{n}{t},p,\frac{x}{t})) \tag{102}$$

mit $t = \gcd(\frac{n}{p},x)$.

Wir haben also einen Isomorphismus zwischen Q und dem von den Elementen $a(p,x)$ mit $p|n$ Primzahl und $1 \le x < \frac{n}{p}$ erzeugten Teilmodul von U. Daß dieser aber bereits ganz U ist, folgt aus der rekursiven Anwendung der Formel

$$a(dt,x) = a(d,tx) + \sum_{j=0}^{d-1} a(t,x+j\frac{n}{dt}), \tag{103}$$

die für alle Teiler $d>1$, $t>1$ von n und $1 \le x < \frac{n}{dt}$ gültig ist, und direkt mit der Definition in (97) bewiesen wird. Mit anderen Worten, alle Elemente $a(d,x)$ aus (97) können durch Elemente $a(p,\cdot)$, wobei $p|n$ Primzahl ist, dargestellt werden

QED.

2.2.3 Gutartigkeit

Mit den beiden im vorangegangenen Abschnitt berechneten Kohomologiegruppen $H^0(\sigma,\mathcal{L}(n))$ und $H^1(\sigma,\mathcal{L}(n))$ kennen wir nach Lemma 1.2.4 die Werte $m^+(\mathcal{L}(n))$ und $m^-(\mathcal{L}(n))$. Im folgenden diskutieren wir die Gutartigkeit von $\Gamma(n)$.

Zunächst noch einige Vorbemerkungen:

- Zu $d \in \mathbf{N}$ sei $g(d) := \prod_{p|d}(\varphi(p^{\alpha_p}) - \varphi(p^{\alpha_p-1}))$, wobei α_p jeweils der maximale Exponent ist, mit dem d von der Primzahl p geteilt wird, und φ die Eulersche φ-Funktion bezeichnet. Wir zeigen später, daß $\varphi(n) = \sum_{d|n} g(d)$ gilt.
- $\Gamma(n)$ ist als ein $M\mathfrak{En}$-System $(M_d,\mathcal{E}_d,\mathfrak{n}_d)_{d\in\Delta}$ definiert. Wir schreiben $Y_d := M_d/\langle\mathcal{E}_d\rangle$. Basen des Kombinates $\mathcal{L}(n)$ von $\Gamma(n)$ werden also gemäß

Satz 1.6.14 aus in M_d lebenden Basen der Y_d konstruiert. Explizit sehen nach Definition 2.2.1 und Satz 2.1.3 die Y_d wie folgt aus. Es ist

$$Y_d = \begin{cases} 0 & \text{falls } d = 1, \\ \langle G_d \rangle & \text{falls } d \text{ Primzahl}, \\ Z(d) & \text{sonst.} \end{cases} \tag{104}$$

- Um einige Aussagen übersichtlicher zu halten, sparen wir manchmal im folgenden den Fall $n = 2$ aus. In diesem läßt sich aber alles sofort ausrechnen. Es ist $\mathcal{L}(2) \cong Y_2 \cong \langle G_2 \rangle$, somit ist insbesondere $m^+(\mathcal{L}(2)) = m^+(Y_2) = 1$ und $\Gamma(2)$ daher direkt nach Definition 1.6.13 gutartig,

Um die Gutartigkeit von $\Gamma(n)$ nachzuweisen, ist $m^+(\mathcal{L}(n)) = \sum_{d|n} m^+(Y_d)$ zu überprüfen.

Zunächst fassen wir dafür in einer Tabelle die Werte der Invarianten m^x von Y_d zusammen.

Lemma 2.2.8 *Zu $d \in \mathbf{N}$ sei $r(d)$ die Anzahl der Primzahlen, die d teilen. Die Invarianten m^+, m^-, m^0 und der Rang von Y_d ergeben sich aus der folgenden Tabelle.*

		m^+	m^-	*Rang*	m^0
I)	$d = 1$	0	0	$g(d) - 1$	0
II)	$d = 2$	1	0	$g(d) + 1$	0
III)	*$d = p$ ungerade und Primzahl*	0	0	$g(d) + 1$	$\frac{1}{2}(g(d) + 1)$
IV)	*$d = u$ oder $d = 4u$ mit ungeraden quadratfreien u und $2 \mid r(d)$*	1	0	$g(d)$	$\frac{1}{2}(g(d) - 1)$
V)	*d nicht prim, $d = u$ oder $d = 4u$ mit ungeraden quadratfreien u und $2 \nmid r(d)$*	0	1	$g(d)$	$\frac{1}{2}(g(d) - 1)$
VI)	*sonstige d*	0	0	$g(d)$	$\frac{1}{2}g(d)$

Beweis
Die Werte für m^0 ergeben sich aus $m^0 = \frac{1}{2}(\text{Rang} - m^+ - m^-)$.

Der Fall I ist trivial. Es ist $Y_1 = 0$. In den Fällen II und III ist $Y_p = \langle G_p \rangle$ und $g(p) = \varphi(p) - 1$, woraus die Behauptung ebenfalls folgt.

In den restlichen Fällen ist $Y_d = Z(d)$. Die Behauptung für den Rang folgt aus Lemma 2.1.2. Die Werte der Invarianten m^+ und m^- folgen aus der Diskussion des Kreismoduls in Abschnitt 2.1.2.

QED.

Mit der Tabelle aus Lemma 2.2.8 können wir den Rang von $\mathcal{L}(n)$ bestimmen.

Lemma 2.2.9 *Es sei $n \in \mathbf{N}$ und r die Anzahl der Primteiler von n. Dann ist*

$$\operatorname{rg} \mathcal{L}(n) = \varphi(n) + r - 1. \tag{105}$$

Beweis
Die Behauptung folgt, wenn wir die Formel

$$\varphi(n) = \sum_{d|n} g(d) \tag{106}$$

zeigen, denn nach Satz 1.6.14, a ergibt die Vereinigung von Basen von Y_d eine Basis von $\mathcal{L}(n)$, also ist der Rang von $\mathcal{L}(n)$ gleich der Summe der Ränge der Y_d, wobei d alle Teiler von n durchläuft. Insgesamt ergibt sich mit (106) und Lemma 2.2.8 ein Rang von "ungefähr" $\varphi(n)$, nämlich als Summe der einzelnen $g(d)$ mit kleinen Abweichungen, bedingt durch die von $g(d)$ verschiedenen Ränge von Y_d, falls d gleich 1 oder Primzahl ist. Somit ist der Rang von $\mathcal{L}(n)$ gleich $\varphi(n) + r - 1$, wobei r die Anzahl der Primteiler von n ist.

Wir zeigen (106) durch Induktion nach r. Für $r = 0$ ist $g(1) = 1 = \varphi(1)$.

Direkt aus der Definition von $g(d)$ folgen $g(dt) = g(d)g(t)$ falls $(d,t) = 1$ ist und

$$\sum_{i=0}^{\alpha} g(p^i) = \sum_{i=1}^{\alpha} (\varphi(p^i) - \varphi(p^{i-1})) + \varphi(1) = \varphi(p^\alpha) \tag{107}$$

für p Primzahl und $\alpha \in \mathbf{N}$. Sei nun $r > 0$. Wir schreiben $n = tp^\alpha$ mit $(t, p^\alpha) = 1$ und p Primzahl. Wir erhalten

$$\sum_{d|n} g(d) = \sum_{i=0}^{\alpha} \sum_{d|t} g(dp^i) = \sum_{i=0}^{\alpha} g(p^i) \sum_{d|t} g(d) = \varphi(p^\alpha)\varphi(t) = \varphi(n). \tag{108}$$

QED.

Durch Aufsummieren der Invarianten m^+ der einzelnen Y_d erhalten wir schließlich Informationen über die Gutartigkeit von $\Gamma(n)$.

Lemma 2.2.10 *Es seien $n > 2$ und r die Anzahl der Primteiler von n. Dann ist*

$$m^+(\mathcal{L}(n)) = \begin{cases} 2^{r-1} - 1 & \text{falls } n \not\equiv 2 \bmod 4, \\ 2^{r-2} & \text{falls } n \equiv 2 \bmod 4, \end{cases} \tag{109}$$

und

$$m^-(\mathcal{L}(n)) = \begin{cases} 2^{r-1} - r & \text{falls } n \not\equiv 2 \bmod 4, \\ 2^{r-2} - (r-1) & \text{falls } n \equiv 2 \bmod 4. \end{cases} \tag{110}$$

Beweis
Nach Lemma 1.2.4 ist $m^+(\mathcal{L}(n))$ die $\mathbf{F}_2$-Dimension der Kohomologiegruppe $H^0(\sigma, \mathcal{L}(n))$ und $m^-(\mathcal{L}(n))$ die $\mathbf{F}_2$-Dimension von $H^1(\sigma, \mathcal{L}(n))$. Mit $r' = r$, falls $n \not\equiv 2 \bmod 4$, und $r' = r - 1$ sonst, erhalten wir aus Satz 2.2.6

$$m^+(\mathcal{L}(n)) = \begin{cases} 2^{r'-1} - 1 & \text{falls } n \not\equiv 2 \bmod 4, \\ 2^{r'-1} & \text{falls } n \equiv 2 \bmod 4, \end{cases} \tag{111}$$

und $m^-(\mathcal{L}(n)) = 2^{r'-1} - r'$.

Ersetzt man r' entsprechend durch r, so folgt die Behauptung.

QED.

Mit den Invarianten und dem Rang von $\mathcal{L}(n)$ können wir auch die Ränge von $\mathcal{L}(n)_+$ und $\mathcal{L}(n)_-$ ausrechnen.

Lemma 2.2.11 *Es seien $n > 2$, und r die Anzahl der Primteiler von n. Dann ist*

$$\mathrm{rg}\,(\mathcal{L}(n)_+) = \tfrac{1}{2}\varphi(n) + r - 1 \quad \textit{und} \quad \mathrm{rg}\,(\mathcal{L}(n)_-) = \tfrac{1}{2}\varphi(n).$$

Beweis
Wir leiten den Rang von $\mathcal{L}(n)_+$ her. Für $\mathcal{L}(n)_-$ kann man analog vorgehen.

Aus der Formel "Rang $= 2m^0 + m^+ + m^-$" folgt $m^0 + m^+ = \frac{1}{2}(\mathrm{Rang} + m^+ - m^-)$. Nach Lemma 1.2.10, a ist $m^0(\mathcal{L}(n)) + m^+(\mathcal{L}(n))$ der Rang von $\mathcal{L}(n)_+$.

Aus Lemma 2.2.10 lesen wir die Werte für $m^+(\mathcal{L}(n))$ und $m^-(\mathcal{L}(n))$ ab und erhalten $m^+(\mathcal{L}(n)) - m^-(\mathcal{L}(n)) = r - 1$. Der Rang von $\mathcal{L}(n)$ ist nach Lemma 2.2.9 gleich $\varphi(n) + r - 1$. Dies zusammengenommen gibt die Behauptung für den Rang von $\mathcal{L}(n)_+$.

QED.

Lemma 2.2.12 *Es seien $n > 2$ und r die Anzahl der Primteiler von n. Dann ist*

$$\sum_{d|n} m^+(Y_d) = \begin{cases} 2^{r-1} - 1 & \text{falls } n \equiv 1, 3 \bmod 4, \\ 2^{r-1} & \text{falls } n \equiv 0 \bmod 4, \\ 2^{r-2} & \text{falls } n \equiv 2 \bmod 4. \end{cases} \tag{112}$$

Beweis
Die Werte von $m^+(Y_d)$ entnimmt man aus Lemma 2.2.8. Dabei sieht man, daß man nur die Teiler der Form $d = u$ oder $d = 4u$ mit u ungerade und quadratfrei oder $d = 2$ betrachten muß, denn nur für diese ist $m^+(Y_d) \neq 0$.

Im Fall $n \equiv 1, 3 \bmod 4$ ist 2^{r-1} die Anzahl der quadratfreien Teiler von n, die eine gerade Anzahl von Primfaktoren besitzen. Insbesondere wird dabei aber auch 1 als Teiler mit gerader Anzahl von Primfaktoren mitgezählt. Da $m^+(Y_1) = 0$ ist, ist 1 von 2^{r-1} abzuziehen.

Im Fall $n \equiv 0 \bmod 4$ ist 2^{r-1} die Anzahl der Teiler der Form $n = u$ oder $n = 4u$ mit n ungerade und quadratfrei, die eine geraden Anzahl von Primfaktoren besitzen. Außerdem muß beachtet werden, daß $m^+(Y_2) = 1$ ist.

Im Fall $n \equiv 2 \bmod 4$ ist die Summe über alle Teiler von $n/2$ zu bilden, was analog zu den vorherigen Fällen $2^{r-2} - 1$ ergibt, zuzüglich 1, dem Wert von $m^+(Y_2)$.

QED.

Nunmehr können wir die Gutartigkeit von $\Gamma(n)$ überprüfen.

Satz 2.2.13 *Zu $n \in \mathbf{N}_\infty$ sei $\Gamma(n)$ das Kreissystem. Dann gilt:*

a) Es ist $\Gamma(n)$ gutartig genau dann, wenn $n \not\equiv 0 \bmod 4$ ist.

b) Ist $n \equiv 0 \bmod 4$, so ist das abgeleitete Kreissystem $\Gamma(n)^{(4)}$ gutartig.

Beweis
Wir führen den Beweis direkt durch Nachweis von (63) in Definition 1.6.13. Dabei folgt Teil a direkt aus dem Vergleich von (109) und (112).
Da $\Gamma(n)$ und $\Gamma(n)^{(4)}$ das gleiche Kombinat $\mathcal{L}(n)$ haben, verifiziert man die Gutartigkeit von $\Gamma(n)^{(4)}$ mit der Gleichung

$$m^+(\mathcal{L}(n)) = m^+(\mathcal{L}(4)) + \sum_{\substack{d|n \\ d\neq 1,2,4}} m^+(Y_d). \tag{113}$$

Aus den Lemmata 2.2.8, 2.2.10 und 2.2.12 erhält man die entsprechenden Werte, und Teil b des Satzes folgt.

QED.

2.2.4 Basen

Die vorangegangene Diskussion der Gutartigkeit des Kreissystems $\Gamma(n)$ erlaubt es, auf einfache Weise Basen von $\mathcal{L}(n)$, $\mathcal{L}(n)_+$ und $\mathcal{L}(n)_-$ anzugeben, nämlich durch Vereinigung von in M_d lebenden Basen der Moduln $Y_d = M_d/\langle\mathcal{E}_d\rangle$ beziehungsweise der Moduln $(Y_d)_+$ und $(Y_d)_-$. Dabei ist im Fall, daß $n \equiv 0 \bmod 4$ ist, zu beachten, daß das abgeleitete $M\mathfrak{En}$-System $\mathcal{L}(n)^{(4)}$ betrachtet wird.
Wir erhalten den folgenden Satz:

Satz 2.2.14 *Zu $n \in \mathbf{N}_\infty$ sei $\mathcal{L}(n)$ der kombinierte Kreismodul, der als Kombinat des n-ten Kreissystems $\Gamma(n) := (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d|n}$ entsteht, und zu $d|n$ sei $Y_d := M_d/\langle\mathcal{E}_d\rangle$. Dann gilt:*

a) *Eine Basis von $\mathcal{L}(n)$ wird induziert von der Vereinigung von in M_d lebenden Basen der Y_d über alle Teiler d von n.*

b) *Es sei x eines der Symbole $-$ oder $+$. Dann gilt:*

   i) Ist $n \not\equiv 0 \bmod 4$, so wird eine Basis von $\mathcal{L}(n)_x$ induziert von der Vereinigung von in M_d lebenden Basen der $(Y_d)_x$, wobei d alle Teiler von n durchläuft.

   ii) Ist hingegen $n \equiv 0 \bmod 4$, so wird eine Basis von $\mathcal{L}(n)_x$ induziert von der Vereinigung von in M_d lebenden Basen der $(Y_d)_x$, wobei d alle Teiler von n ungleich 2 oder 4 durchläuft, vereinigt mit einer in $M_2 \oplus M_4$ lebenden Basis von $\mathcal{L}(4)_x$.

Beweis
Der Satz ist vollständig eine Anwendung von Satz 1.6.14, der die entsprechenden Aussagen für $M\mathfrak{En}$-Systeme liefert. In Teil b fließen die Ergebnisse aus Satz 2.2.13 über die Gutartigkeit von $\mathcal{L}(n)$ ein.

QED.

Der gerade bewiesene Satz 2.2.14 zeigt auf, was wir an Ausgangsmaterial zur expliziten Konstruktion von Basen von $\mathcal{L}(n)$, $\mathcal{L}(n)_+$ und $\mathcal{L}(n)_-$ benötigen:

a) Basen der Y_d, $(Y_d)_+$ und $(Y_d)_-$ für jeden Teiler d von n,

b) im Falle $n \equiv 0 \bmod 4$ zusätzlich noch Basen von $\mathcal{L}(4)_+$ und $\mathcal{L}(4)_-$.

zu a)
Die Y_d sind in (104) definiert. Ist d keine Primzahl, so ist Y_d der Kreismodul $Z(d)$. Für $Z(d)$ werden in Abschnitt 2.1.2 ausführlich Quasinormalbasen und Normalbasen berechnet, die nach Lemma 1.2.10 Basen von $Z(d)_+$ und $Z(d)_-$ induzieren. Dies soll an dieser Stelle nicht noch einmal wiederholt werden.

Im Fall, daß $d = p$ eine Primzahl ist, ist nach (104) $Y_p = \langle G_p \rangle$. Auf G_p operiert σ durch $\sigma a := p - a$. Daher induziert für $p \neq 2$ beispielsweise $[H_p, \emptyset, \emptyset]$ mit $H_p = \{1, \ldots, \lfloor p/2 \rfloor\}$ eine Normalbasis von Y_p, und entsprechend induziert H_p eine Basis sowohl von $(Y_p)_+$ als auch $(Y_p)_-$.

Was den Fall $d = 2$ angeht, so ist $Y_2 = \langle G_2 \rangle$, und auf G_2 operiert σ trivial. Daher induziert $[\emptyset, G_2, \emptyset]$ eine Normalbasis von Y_2. Somit induziert G_2 eine Basis von $(Y_2)_+$, und es ist $(Y_2)_- = 0$.

zu b)
Wie schon an anderen Stellen schreiben wir $a \in G_d$ als $[d, a]$. Insbesondere ist $G_2 = \{[2,1]\}$ und $G_4 = \{[4,1],[4,3]\}$. Aus dem Beispiel am Ende von Kapitel 1 können wir ablesen, wie das $M\mathcal{E}\mathfrak{n}$-System $\Gamma(4) = (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d=1,2,4}$ explizit aussieht. Insbesondere ist $\mathfrak{n}_4([4,1]+[4,3]) = -[2,1]$, und das Kombinat $\mathcal{L}(4)$ ist explizit gegeben durch

$$\mathcal{L}(4) = \langle [4,1],[4,3],[2,1] \rangle / \langle [4,1]+[4,3]-[2,1] \rangle. \tag{114}$$

Entweder durch Probieren oder mit Hilfe von Algorithmus 1.6.6 erhält man beispielsweise $[\{[4,1]\}, \emptyset, \emptyset]$ als Normalbasis von $\mathcal{L}(4)$, und somit induziert $\{[4,1]\}$ gleichermaßen eine Basis von $\mathcal{L}(4)_+$ wie auch von $\mathcal{L}(4)_-$.

2.3 Der Kreismodul und die Kreiszahlen

Als eine erste echte Anwendung des Kreismoduls betrachten wir im folgenden die Gruppe der Kreiszahlen, das heißt, die Gruppe, die von den Elementen $1-\epsilon$ erzeugt wird, wobei ϵ die Einheitswurzeln ungleich 1 durchläuft. Die Kreiseinheiten, die wir später betrachten, sind eine Untergruppe der Kreiszahlen.

Nach der Definition der Kreiszahlen im ersten Abschnitt stellen wir zwei grundsätzlich verschiedene Möglichkeiten vor, die Kreiszahlen mit dem Kreismodul in Verbindung zu bringen. Einerseits lassen sich alle Kreiszahlen auffassen als isomorph zu dem kombinierten Kreismodul. Das heißt, man stellt einen kombinierten Kreismodul allen Kreiszahlen gegenüber, oder man betrachtet andererseits einen Kreismodul, und stellt ihn als isomorph zu der Gruppe der Kreiszahlen modulo einer geeigneten Untergruppe heraus.

Im folgenden sei zu $n \in \mathbf{N}$ jeweils ϵ_n eine primitive n-te Einheitswurzel. Diese seien zusätzlich so definiert, daß $\epsilon_d = \epsilon_n^{n/d}$ für alle d und n mit $d|n$ gilt. Beispielsweise kann $\epsilon_n := e^{\frac{2\pi i}{n}}$ gewählt werden.

2.3.1 Definition der Kreiszahlen und Eigenschaften

Definition 2.3.1 *Es sei $n \in \mathbf{N}_\infty$, und wir definieren die Gruppe $D^{(n)}$ der Kreiszahlen als die von $\{1 - \epsilon_d^a;\ a \in G_d, 1 < d|n\}$ erzeugte multiplikative Untergruppe von $\mathbf{C}^*$ modulo Torsion, also modulo den Einheitswurzeln.*

Die Kreiszahlen sind eng verwandt mit der Gruppe der Kreiseinheiten, die Gegenstand des dritten Kapitels dieser Arbeit sind. Indem wir Ergebnisse aus dem dritten Kapitel benutzen, können wir den Rang der Gruppe der Kreiszahlen berechnen.

Lemma 2.3.2 *Zu $n \in \mathbf{N}$ sei r die Anzahl der Primteiler von n. Dann ist*

$$\operatorname{rg} D^{(n)} = \tfrac{1}{2}\varphi(n) + r - 1. \tag{115}$$

Beweis
Es sei $C^{(n)}$ die Gruppe der Kreiseinheiten, die definiert ist als Gruppe der in $\mathbf{Z}[\epsilon_n]$ invertierbaren Elemente von $D^{(n)}$. In Lemma 3.1.4, c, wird gezeigt, daß $\operatorname{rg} D^{(n)} = r + \operatorname{rg} C^{(n)}$ ist. Die Gruppe der Kreiseinheiten $C^{(n)}$ hat nach Lemma 3.1.2 Rang $\frac{1}{2}\varphi(n) - 1$.

QED.

2.3.2 Das Kreissystem und die Kreiszahlen

In diesem Abschnitt konstruieren wir eine Basis der Gruppe der Kreiszahlen $D^{(n)}$, indem wir diese Gruppe als isomorph zu $\mathcal{L}(n)_+$ herausarbeiten, wobei $\mathcal{L}(n)$ der n-te kombinierte Kreismodul ist.

Explizit ist $\mathcal{L}(n)$ gegeben als direkte Summe von freien Erzeugnissen der Mengen G_d mit $d|n$ modulo gewisser Relationen. Somit wird der Isomorphismus sinnvollerweise durch seine Wirkung auf die G_d angegeben.

Satz 2.3.3 *Zu $n \in \mathbf{N}_\infty$ sei $\mathcal{L}(n)$ der n-te kombinierte Kreismodul und $D^{(n)}$ die Gruppe der Kreiszahlen. Dann ist*

$$\mathcal{L}(n)_+ \cong D^{(n)}, \tag{116}$$

wobei $a \in G_d$ für $d|n$ auf $1 - \epsilon_d^a$ abgebildet wird.

Beweis
Wir zeigen die Exaktheit der Sequenz

$$0 \to T \to \mathcal{L}(n)/(1-\sigma)\mathcal{L}(n) \xrightarrow{\mu} D^{(n)} \to 1, \tag{117}$$

wobei T die Torsionsgruppe von $\mathcal{L}(n)/(1-\sigma)\mathcal{L}(n)$ und μ die im Satz definierte Abbildung ist, die $a \in G_d$ auf $1-\epsilon_d^a$ abbildet. Ist dies gezeigt, so folgt auch der behauptete Isomorphismus, denn nach Lemma 1.2.10, c, i ist $\mathcal{L}(n)_+$ gleich $\mathcal{L}(n)/(1-\sigma)\mathcal{L}(n)$ modulo Torsion.

$\mathcal{L}(n)$ ist definiert als Kombinat des $M\mathfrak{En}$-Systems $\Gamma(n) = (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d|n}$ mit $M_d = \langle G_d \rangle$. Konkret können wir $\mathcal{L}(n) = N/Q$ schreiben, wobei $N = \bigoplus_{d|n} M_d$ und $Q = \sum_{d|n} \langle r + \mathfrak{n}_d(r);\ r \in \mathcal{E}_d \rangle$ ist.

Es ist μ aus (117) definiert auf der disjunkten Vereinigung der Mengen G_d mit $d|n$, und daher auf das freie Erzeugnis N dieser Vereinigung homomorph fortsetzbar. Wir zeigen, daß μ als Abbildung von $\mathcal{L}(n)/(1-\sigma)\mathcal{L}(n)$ wohldefiniert ist. Da $\mathcal{L}(n)/(1-\sigma)\mathcal{L}(n) \cong N/((1-\sigma)N+Q)$ ist, ist zu zeigen, daß $(1-\sigma)N$ und Q unter μ auf Einheitswurzeln abgebildet werden.

- Für $(1-\sigma)N$ folgt dies sofort mit $(1-\epsilon_d^a)/(1-\epsilon_d^{-a}) = -\epsilon_d^a$.
- Es entspricht Q den Relationen, die durch Relativnormen entstehen.

  Bezeichnet nämlich $N_{d,p}$ für $p|d$ die Norm von $\mathbf{Q}(\epsilon_d)$ nach $\mathbf{Q}(\epsilon_{d/p})$, so gilt für $d \neq p$, daß

$$N_{d,p}(1-\epsilon_d^a) = \prod_{\substack{c \in G_d \\ c \equiv a \bmod d/p}} (1-\epsilon_d^c) = \begin{cases} (1-\epsilon_{d/p}^a)/(1-\epsilon_{d/p}^{a'}) & \text{falls } p^2 \nmid d, \\ 1-\epsilon_{d/p}^a & \text{falls } p^2 | d, \end{cases} \tag{118}$$

  mit $pa' \equiv a \bmod d/p$ im Fall $p^2 \nmid d$ ist. Das folgt aus der Polynomidentität $\prod_{\nu=0}^{p-1}(1-x\epsilon_p^\nu) = 1-x^p$, und zwar mit $x = \epsilon_{d/p}^{a'}$ im Fall $p^2 \nmid d$ und $x = \epsilon_d^a$ im Fall $p^2|d$.

  Eine ausführliche Untersuchung der Normrelationen wie in (118) findet sich beispielsweise in [2], Abschnitt 1.2.5.

  Es wird Q erzeugt von den Modulelementen $s(d,p,a) + \mathfrak{n}_d(s(d,p,a))$. Die Zeilensummen $s(d,p,a)$ werden nach Satz 2.1.3 unter μ auf das Produkt in der Mitte von (118) abgebildet, und $-\mathfrak{n}_d(s(d,p,a))$ wird unter μ auf die rechte Seite von (118) abgebildet. Insgesamt wird also Q unter μ trivial abgebildet.

Es sei zunächst $n \neq \infty$. Der Rang von $\mathcal{L}(n)_+$ wurde in Lemma 2.2.11 berechnet, der Rang von $D^{(n)}$ in Lemma 2.3.2. Wir erhalten $\operatorname{rg} \mathcal{L}(n)_+ = \operatorname{rg} D^{(n)}$. Es ist μ surjektiv und $D^{(n)}$ torsionsfrei. Somit ist $\ker \mu$ in der Tat die Torsionsgruppe von $\mathcal{L}(n)/(1-\sigma)\mathcal{L}(n)$ und daher (117) exakt.

Für $n = \infty$ zieht man sich auf den endlichen Fall zurück.

QED.

2.3.3 Der Kreismodul und relative Kreiszahlen

In $D^{(n)}$ gibt es zweierlei Sorten von Ausdrücken der Form $1-\epsilon_n^a$. Einerseits gibt es diejenigen mit $(a,n)=1$, die "echt" in $D^{(n)}$ liegen. Andererseits gibt es solche, die eigentlich von der Form $1-\epsilon_d^{a'}$ mit $d||n$ sind, und daher schon in $D^{(d)}$ liegen.

In diesem Abschnitt betrachten wir nur die "echten" Kreiszahlen $1-\epsilon_n^a$, indem wir die $D^{(d)}$ mit $d||n$ aus $D^{(n)}$ herausfaktorisieren. Anschließend zeigen wir, wie sich solche "Stücke" von $D^{(n)}$ wieder zusammensetzen lassen zu $D^{(n)}$.

Definition 2.3.4 *Zu $n\in\mathbf{N}$ sei $D^{(n)}$ die Gruppe der Kreiszahlen, und $K^{(n)}:=\prod_{d||n}D^{(d)}$. Dann nennen wir $\widehat{D^{(n)}}:=D^{(n)}/K^{(n)}$ die Gruppe der n-ten* relativen Kreiszahlen.

Die Gruppe der Kreiszahlen ist isomorph zu dem kombinierten Kreismodul $\mathcal{L}(n)_+$, der sich aus kleineren Stücken zusammensetzt, die partiell durch Teilbarkeit geordnet sind. Die relativen Kreiszahlen sind zu dem "obersten" dieser Stücke isomorph. Genau gilt:

Satz 2.3.5 *Zu $n\in\mathbf{N}$ sei $\widehat{D^{(n)}}$ die Gruppe der n-ten relativen Kreiszahlen und $Z(n)$ der n-te Kreismodul. Dann gilt*

$\widehat{D^{(n)}}\cong Z(n)_+$, *falls n keine Primzahl und $n\neq 4$ ist,*

$\widehat{D^{(p)}}\cong\langle G_p\rangle_+$, *falls $n=p$ Primzahl ist.*

Faßt man $Z(n)$ als Modul über G_n modulo Relationen auf, so ist der Isomorphismus dadurch gegeben, daß $a\in G_n$ auf $1-\epsilon_n^a$ abgebildet wird, wobei ϵ_n eine primitive n-te Einheitswurzel ist.

Beweis

Wir schreiben $\mathcal{L}(n)$ als Kombinat des $M\mathfrak{En}$-System $\Gamma(n):=(M_d,\mathcal{E}_d,\mathfrak{n}_d)_{d|n}$.

Es ist $Y_n:=M_n/\langle\mathcal{E}_n\rangle=Z(n)$, falls n keine Primzahl ist, und gleich $\langle G_p\rangle$, falls $n=p$ Primzahl ist. Insbesondere ist Y_n als Zeilenfaktormodul nach Lemma 1.4.5 frei.

Es ist $(Y_n)_+\cong\widehat{D^{(n)}}$ zu zeigen.

Definieren wir $N':=\bigoplus_{d||n}M_d$ und $Q':=\sum_{d||n}\langle r+\mathfrak{n}_d(r);\ r\in\mathcal{E}_d\rangle$, so erhalten wir das kommutative Diagramm

$$\begin{array}{ccccccccc} 0 & \to & (N'/Q')_+ & \to & \mathcal{L}(n)_+ & \to & (Y_n)_+ & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \prod\limits_{d||n} D^{(d)} & \to & D^{(n)} & \to & \widehat{D^{(n)}} & \to & 0. \end{array} \tag{119}$$

Die untere Sequenz ist nach Definition von $\widehat{D^{(n)}}$ exakt, die obere Sequenz ist nach Bemerkung 1.6.16 ebenfalls exakt, wobei wir die Gutartigkeit der

entsprechenden Sequenz ohne "+" ausnutzen. Alle senkrechten Pfeile sind offensichtlich surjektiv. Nach Satz 2.3.3 ist der mittlere senkrechte Pfeil ein Isomorphismus. Als Einschränkung dieses Isomorphismus ist der linke Pfeil ebenfalls ein Isomorphismus. Mit diesen Isomorphismen erhalten wir $\mathrm{rg}\,(Y_n)_+ = \mathrm{rg}\,\widehat{D^{(n)}}$.

Es ist Y_n torsionsfrei, und daher ist nach Lemma 1.2.10, a auch $(Y_n)_+$ torsionsfrei. Da $(Y_n)_+$ und $\widehat{D^{(n)}}$ den gleichen Rang haben und die Abbildung $(Y_n)_+ \to \widehat{D^{(n)}}$ surjektiv ist, folgt aus der Torsionsfreiheit von $(Y_n)_+$ der Isomorphismus $(Y_n)_+ \cong \widehat{D^{(n)}}$.

QED.

Die im Beweis zu Satz 2.3.5 bewiesene Torsionsfreiheit von $(Y_n)_+$ impliziert durch den Isomorphismus $(Y_n)_+ \cong \widehat{D^{(n)}}$, daß $\widehat{D^{(n)}}$ ebenfalls torsionsfrei ist. Wir halten dies als Korollar fest.

Korollar 2.3.6 *Es sei $n \neq 4$. Dann ist $\widehat{D^{(n)}}$ torsionsfrei.*

Bemerkung 2.3.7 *Der Fall $n = 4$ kommt in Satz 2.3.5 nicht vor und wird auch im folgenden nicht benötigt. Es sei angemerkt, daß man direkt nachrechnen kann, daß $\widehat{D^{(4)}}$ eine zweielementige Gruppe bildet (und daher nicht torsionsfrei ist).*

Insbesondere impliziert Satz 2.3.5 den folgenden Satz, der nur noch in der Sprache der Kreiszahlen formuliert ist.

Satz 2.3.8 *Es sei $n \in \mathbf{N}_\infty$. Zu $d \in \mathbf{N}$, $d \neq 4$, $d|n$ induziere $\widehat{B_d} \subseteq D^{(n)}$ eine Basis von $\widehat{D^{(d)}}$. Dann gilt*

a) Ist $n \not\equiv 0 \bmod 4$, so ist $\bigcup_{d|n} \widehat{B_d}$ eine Basis von $D^{(n)}$.

b) Ist $n \equiv 0 \bmod 4$, so ist $\{1 - \epsilon_4\} \cup \bigcup_{\substack{d|n \\ d\neq 2,4}} \widehat{B_d}$ eine Basis von $D^{(n)}$.

<u>*Beweis*</u>

Dieser Satz ist eine 1:1-Übertragung der entsprechenden Situation bei den Kreismoduln. Ist nämlich $\Gamma(n) = (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d|n}$ das Kreissystem mit Kombinat $\mathcal{L}(n)$, so haben wir nach Satz 2.3.3 den Isomorphismus $\mathcal{L}(n)_+ \cong D^{(n)}$.

Wir wenden Satz 2.2.14 an. In M_d definierte Basen von $(Y_d)_+ = (M_d/\langle \mathcal{E}_d \rangle)_+$, wobei Y_d nach (104) entweder als freies Erzeugnis von G_p oder als Kreismodul $Z(d)$ definiert ist, entsprechen nach Satz 2.3.5 den Basen $\widehat{B_d}$ von $\widehat{D^{(n)}}$, und es folgt damit Teil a.

In Teil b fließt noch zusätzlich ein, daß die Basis von $\mathcal{L}(4)_+$, wie sie im Anschluß an Satz 2.2.14 konstruiert wurde der Kreiszahl $1 - \epsilon_4 \in D^{(n)}$ entspricht.

QED.

2.4 P-Kreissysteme

P-Kreissysteme entstehen analog zu den Kreissystemen als ein $M\mathfrak{En}$-System $(M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d\in\Delta}$, das sich aus P-Kreismoduln zusammensetzt. Der wesentliche Unterschied zu Kreissystemen besteht in der Indexmenge Δ. Sie besteht nicht mehr aus allen Teilern einer Zahl n, sondern nur aus den sogenannten P-Teilern, das sind genau diejenigen Teiler von n mit $\gcd(d, n/d) = 1$. Da vieles beim P-Kreissystem analog zum Kreissystem läuft, sind die einzelnen Abschnitte so knapp wie möglich gehalten, und teilweise wird nur skizziert, wie die Argumentation im einzelnen aussieht.

Der Grund, warum P-Kreissysteme im Rahmen dieser Arbeit überhaupt behandelt werden, liegt darin, daß sie den bisher üblichen Weg ([2], [5], [8]) zur Behandlung von Kreiseinheiten widerspiegeln. Das P-Kreissystem ist allerdings in mancher Hinsicht schlechter als das Kreissystem. Beispielsweise sei hier schon erwähnt, daß es nicht möglich ist, ein P-Kreissystem für $n = \infty$ sinnvoll zu definieren. Beim Kreissystem konnte $n = \infty$ praktisch ohne zusätzlichen Aufwand mit den Fällen $n \neq \infty$ mitbehandelt werden. Im letzten Abschnitt dieses Kapitels werden dieser und andere Unterschiede ausführlich diskutiert.

Es sei noch daraufhingewiesen, daß im Fall, daß n quadratfrei ist, das P-Kreissystem mit dem Kreissystem übereinstimmt. Um die sonstigen Parallelen zwischen P-Kreissystem und Kreissystem zu dokumentieren, benutzen wir im wesentlichen beim P-Kreissystem die gleichen Bezeichnungen wie beim Kreissystem, setzen jedoch einen Akzent auf den entsprechenden Buchstaben, wenn das bezeichnete Objekt sich beim P-Kreissystem vom Kreissystem unterscheidet. Folglich bezeichnen wir das P-Kreissystem zu n in Analogie zum Kreissystem $\Gamma(n)$ mit $\acute{\Gamma}(n)$.

2.4.1 Der P-Kreismodul

Definition 2.4.1 *Zu $n \in \mathbf{N}$ definieren wir den P-Kreismodul $\acute{Z}(n)$ wie folgt:*

a) Ist $n = q$ die Potenz einer Primzahl, dann sei $\acute{Z}(q) = \langle G_q\rangle/\langle\sum_{a\in G_q}[a]\rangle$. Auf G_q (und damit auf $\acute{Z}(q)$) operiere σ durch $\sigma a := q - a$.

b) Ist $n = q_1 \cdots q_r$ das Produkt von paarweise teilerfremden Primzahlpotenzen, so definieren wir $\acute{Z}(n) := \acute{Z}(q_1) \otimes \cdots \otimes \acute{Z}(q_r)$. Auf $\acute{Z}(n)$ operiere σ diagonal.

Wie man schon an der Definition sieht, werden beim P-Kreismodul im Unterschied zu Kreismoduln Primzahlpotenzen als "kleinste" Einheiten bei der Zerlegung von n betrachtet, und nicht die Primzahlen.

Lemma 2.4.2 *Es sei $n = q_1 \cdots q_r \in \mathbf{N}$ in paarweise teilerfremde Primzahlpotenzen zerlegt. Der Rang von $\acute{Z}(n)$ ist dann gleich $\prod_{i=1}^{r}(\varphi(q_i) - 1)$.*

Beweis
Bei der Tensorproduktbildung multiplizieren sich die Ränge. Da der Rang von $\acute{Z}(q)$ gleich $\varphi(q)-1$ ist, wenn q eine Primzahlpotenz ist, folgt die Behauptung.

QED.

Im folgenden geben wir noch an, wie eine Normalbasis beziehungsweise Quasinormalbasis von $\acute{Z}(n)$ aussieht. Dabei ist zunächst anzumerken, daß $\acute{Z}(n)=0$ für $n \equiv 2 \bmod 4$ ist, was direkt aus $\acute{Z}(2)=0$ folgt. Der Fall $n \not\equiv 2 \bmod 4$ verläuft im wesentlichen analog zum ungeraden quadratfreien Fall bei der Konstruktion einer Basis von $Z(n)$ in Abschnitt 2.1.2.

Explizit erhalten wir auf dem folgenden Weg eine Normal- und Quasinormalbasis von $\acute{Z}(n)$:

- Ist $q \neq 2$ die Potenz einer Primzahl, so ist $[\acute{E}_q^0, \emptyset]$, wobei $\acute{E}_q^0$ definiert ist durch $\acute{E}_q^0 := \{a \in G_q;\ 1 \leq a < q/2\}$, eine Normalzerlegung von G_q.

- Aus der Normalzerlegung erhalten wir eine Normalbasis $[\acute{F}_q^0, \emptyset, \acute{F}_q^-]$ von $\acute{Z}(q)$ mit

$$\acute{F}_q^0 := \{a \in G_q;\ 1 < a < q/2\} \quad \text{und} \quad \acute{F}_q^- := \{\sum_{\substack{1 \leq a < q/2 \\ a \in G_q}} [a]\}.$$

  Eine Quasinormalbasis ist $[\acute{F}_q^0, \emptyset, \{1\}]$.

- Da $\acute{Z}(n)$ als Tensorprodukt von P-Kreismoduln $\acute{Z}(q)$ mit q Primzahlpotenz definiert ist, lassen sich Normalbasen und Quasinormalbasen von $\acute{Z}(n)$ wie bei Kreismoduln in Abschnitt 2.1.2 konstruieren. Beispielsweise sieht eine Quasinormalbasis $[\acute{G}^0, \acute{G}^+, \acute{G}^-]$ zu $\acute{Z}(n)$ mit $n = q_1 \cdots q_r$ folgendermaßen aus:

$$\begin{aligned}
\acute{G}^0 &:= \textstyle\bigcup_{i=1}^{r} \{(1, \ldots, 1, a_i, \ldots, a_r) \in G_{q_1} \times \cdots \times G_{q_r};\ 1 < a_i < q_i/2, \\
&\qquad \text{und } 1 \leq a_j < q_j - 1 \text{ für } j = i+1, \ldots, r\}, \\
\acute{G}^+ &:= \{(1, \ldots, 1)\}, \text{ falls } r \text{ gerade und } \acute{G}^+ := \emptyset, \text{ falls } r \text{ ungerade}, \\
\acute{G}^- &:= \{(1, \ldots, 1)\} \setminus \acute{G}^+.
\end{aligned}$$

Normalbasen und Quasinormalbasen für P-Kreismoduln werden also analog zu Normalbasen im Fall $n = u$ beziehungsweise $n = 4u$ bei Kreismoduln konstruiert, wobei u ungerade und quadratfrei ist.

Wie den Kreismodul können wir den P-Kreismodul interpretieren als $\langle G_n \rangle / \acute{R}_n$, wobei $\acute{R}_n$ eine geeignete Menge von Relationen ist. Es operiert σ auf G_n durch $\sigma a := n - a$ für $a \in G_n$, und $\acute{R}_n$ wird von Zeilensummen der Form

$$\acute{s}(n, q, a) = \sum_{\substack{x \in G_n \\ x \equiv a \bmod (n/q)}} [x] \tag{120}$$

erzeugt, wobei $a \in G_n$ und $q | n$ eine Primzahlpotenz mit $\gcd(q, n/q) = 1$ ist.

2.4.2 Das P-Kreissystem

Das P-Kreissystem ist das Analogon zum Kreissystem. Wir verwenden die gleichen Bezeichnungen wie für das Kreissystem in Abschnitt 2.2.1. Zusätzlich definieren wir zu $n \in \mathbf{N}$ die Mengen

- $T_n := \{d|n;\ \gcd(d, n/d) = 1\}$ die Menge der P-Teiler von n,
- $T'_n := T_n \setminus \{n\}$, die Menge der echten P-Teiler von n,
- $P_n \subseteq T_n$ als die Menge der P-Teiler von n, die Potenzen von Primzahlen sind.

Dabei seien T_n und T'_n jeweils durch Teilbarkeit partiell geordnet.

Definition 2.4.3 *Es sei $n \in \mathbf{N}$. Zu $d \in T_n$ sei $M_d := \langle G_d \rangle$, und $\acute{\mathcal{E}}_d$ sei die Menge aller Zeilensummen $\acute{s}(d, q, a)$ im P-Kreismodul $\acute{Z}(n)$, falls $d \notin P_n$ ist. Für $d \in P_n$ sei $\acute{\mathcal{E}}_d$ leer.*
Weiter seien auf den Zeilensummen aus $\acute{\mathcal{E}}_d$ Abbildungen $\acute{\mathfrak{n}}_d : \acute{\mathcal{E}}_d \to \bigoplus_{t \in T'_n} M_t$ dadurch gegeben, indem wir der Zeilensumme $\acute{s}(d, q, a) \in \acute{\mathcal{E}}_d$ mit $q \in P_d$ das Element $(p^{-1} - 1)[a \bmod d/q] \in M_{d/q}$ zuordnen, wobei p die Primzahl ist, die q teilt.
Unter diesen Voraussetzungen heißt das $M\mathfrak{En}$-System $\acute{\Gamma}(n) := (M_d, \acute{\mathcal{E}}_d, \acute{\mathfrak{n}}_d)_{d \in T_n}$ das n-te P-Kreissystem.

Genau wie im Fall des Kreissystems zeigt man, daß $\acute{\Gamma}(n)$ kombinierbar ist, und wir definieren für $n \in \mathbf{N}$ den n-ten kombinierten P-Kreismodul $\acute{\mathcal{L}}(n)$ als Kombinat des n-ten Kreissystems.

Im folgenden zeigen wir, daß der kombinierte Kreismodul $\mathcal{L}(n)$ und der kombinierte P-Kreismodul $\acute{\mathcal{L}}(n)$ isomorph sind. Da $\mathcal{L}(n)_+$ seinerseits isomorph zu der Gruppe der Kreiszahlen ist, erhalten wir damit auch einen Isomorphismus zwischen $\acute{\mathcal{L}}(n)_+$ und der Gruppe der Kreiszahlen.

Satz 2.4.4 *Es sei $n \in \mathbf{N}$. Dann ist der kombinierte P-Kreismodul $\acute{\mathcal{L}}(n)$ isomorph zum kombinierten Kreismodul $\mathcal{L}(n)$.*
Schreiben wir $\acute{\mathcal{L}}(n)$ und $\mathcal{L}(n)$ als Kombinate von $\acute{\Gamma}(n) = (M_d, \acute{\mathcal{E}}_d, \acute{\mathfrak{n}}_d)_{d \in T_n}$ beziehungsweise $\Gamma(n) = (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d|n}$, so ist der Isomorphismus dadurch gegeben, daß jeweils M_d als Teil von $\acute{\Gamma}(n)$ abgebildet wird auf M_d als Bestandteil von $\Gamma(n)$.

Beweis
Es sei $\acute{N} := \bigoplus_{d \in T_n} M_d$ und $\psi : \acute{N} \to \mathcal{L}(n)$, der Homomorphismus, der die M_d auf sich selbst abbildet.

Wir zeigen zunächst, daß ψ surjektiv ist und anschließend, daß der Modul $\acute{Q} := \sum_{d \in T_n} \langle r + \acute{\mathfrak{n}}_d(r);\ r \in \acute{\mathcal{E}}_d \rangle$ im Kern von ψ liegt. Es ist $\acute{\mathcal{L}}(n) = \acute{N}/\acute{Q}$, somit haben wir einen surjektiven Homomorphismus von $\acute{\mathcal{L}}(n)$ nach $\mathcal{L}(n)$.

Schließlich zeigen wir, daß die Ränge gleich sind. Da $\acute{\mathcal{L}}(n)$ als Kombinat torsionsfrei ist (denn nach Satz 1.6.14, a läßt sich sogar eine Basis von $\acute{\mathcal{L}}(n)$ konstruieren), folgt der behauptete Isomorphismus.

Im folgenden sei $Q := \sum_{d|n}\langle r + \mathfrak{n}_d(r);\ r \in \mathcal{E}_d\rangle$, so daß $\mathcal{L}(n) = N/Q$ mit $N := \bigoplus_{d|n} M_d$ ist.

ψ ist surjektiv: Es sei t ein Teiler von n, aber kein P-Teiler. Wir zeigen, daß $a \in G_t$ modulo Q als Bild von ψ vorkommt. Dazu reicht es zu zeigen, daß a modulo Q als Erzeugnis von G_{pt} dargestellt werden kann, wobei p eine Primzahl ist, die t teilt. Dann folgt nämlich induktiv, daß a modulo Q im Erzeugnis von $G_{p_1\cdots p_s t}$ liegt, wobei die p_i nicht notwendig verschiedene Primzahlen sind, die t teilen. Für geeignete $p_1, \ldots, p_s$ ist $p_1 \cdots p_s t \in T_n$.

Daß a modulo Q von G_{pt} erzeugt wird, folgt direkt, da $s(pt, p, a) - [a] \in Q$ ist, und $s(pt, p, a)$ eine Summe von Elementen aus G_{pt} ist.

$\acute{Q} \subseteq \ker\psi$: Es wird $\acute{Q}$ erzeugt von Elementen der Form

$$\acute{s}(d, q, a) + (p^{-1} - 1)[a \bmod d/q], \tag{121}$$

mit $d \in T_n$, $q = p^\alpha \in P_n$ und $a \in G_d$. Es ist zu zeigen, daß die Ausdrücke aus (121) modulo Q verschwinden.

Wir schreiben dazu $d = qt$, und es sei $a \in G_d$. Zunächst gilt

$$-(p^{-1} - 1)[a \bmod t] \equiv s(pt, p, a) \bmod Q, \tag{122}$$

und wir zeigen über vollständige Induktion nach α, daß

$$\acute{s}(p^\alpha t, p^\alpha, a) \equiv s(pt, p, a) \bmod Q \tag{123}$$

ist. Für $\alpha = 1$ ist $s = \acute{s}$ und daher nichts zu zeigen. Ist $\alpha \geq 2$ so erhalten wir aus der Definition der Zeilensummen s und $\acute{s}$ gemäß (86) und (120):

$$\begin{aligned}
\acute{s}(p^\alpha t, p^\alpha, a) &= \sum_{\substack{x \in G_{p^\alpha t} \\ x \equiv a \bmod t}} [x] = \sum_{\substack{x \in G_{p^{\alpha-1} t} \\ x \equiv a \bmod t}} \ \sum_{\substack{y \in G_{p^\alpha t} \\ y \equiv x \bmod p^{\alpha-1} t}} [y] \\
&= \sum_{\substack{x \in G_{p^{\alpha-1} t} \\ x \equiv a \bmod t}} s(p^\alpha t, p, x) \\
&\equiv \sum_{\substack{x \in G_{p^{\alpha-1} t} \\ x \equiv a \bmod t}} [x] \qquad \bmod Q \\
&= \acute{s}(p^{\alpha-1} t, p^{\alpha-1}, a) \equiv s(pt, p, a) \qquad \bmod Q.
\end{aligned} \tag{124}$$

Aus (122) und (123) folgt $\acute{s}(tq, q, a) + (p^{-1} - 1)[a \bmod t] \in Q$, was zu zeigen war.

$\operatorname{rg}\acute{\mathcal{L}}(n) = \operatorname{rg}\mathcal{L}(n)$: Zu $d = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ definieren wir $\acute{g}(d) := \prod_{i=1}^{s}(\varphi(p_i^{\alpha_i}) - 1)$. Für diese Funktion gilt, wie man durch Induktion nach der Anzahl der

Primteiler von n nachrechnet, $\sum_{d\in T_n} \acute{g}(d) = \varphi(n)$. Setzen wir $\acute{Y}_d := M_d/\langle\acute{\mathcal{E}}_d\rangle$, so ist nach Definition 2.4.3 in Analogie zu (104)

$$\acute{Y}_d = \begin{cases} 0 & \text{falls } d = 1, \\ \langle G_d\rangle & \text{falls } d \text{ Potenz einer Primzahl,} \\ \acute{Z}(d) & \text{sonst.} \end{cases} \tag{125}$$

Der Rang von $\langle G_d\rangle$ ist $\varphi(d)$, der Rang von $\acute{Z}(d)$ ist das Produkt der Ränge von $\acute{Z}(q)$ mit $q \in P_d$. Wir erhalten also

$$\operatorname{rg}\acute{Y}_d = \begin{cases} \acute{g}(d) - 1 & \text{falls } d = 1, \\ \acute{g}(d) + 1 & \text{falls } d \text{ Potenz einer Primzahl,} \\ \acute{g}(d) & \text{sonst.} \end{cases} \tag{126}$$

In Analogie zum Beweis von Lemma 2.2.9 ist der Rang von $\acute{\mathcal{L}}(n)$ die Summe über die Ränge von $\acute{Y}_d$, wobei d alle P-Teiler von n durchläuft. Somit erhalten wir gemäß der Summenformel für $\acute{g}(d)$

$$\operatorname{rg}\acute{\mathcal{L}}(n) = \varphi(n) + r - 1 = \operatorname{rg}\mathcal{L}(n), \tag{127}$$

wobei r die Anzahl der n teilenden verschiedenen Primzahlen ist.

QED.

Der Isomorphismus zwischen $\mathcal{L}(n)$ und $\acute{\mathcal{L}}(n)$ impliziert insbesondere die Gleichheit der Invarianten m^+ der beiden Moduln, das heißt, es gilt $m^+(\mathcal{L}(n)) = m^+(\acute{\mathcal{L}}(n))$. Ebenfalls bekannt sind die Invarianten m^+ der einzelnen $\acute{Y}_d$. Für $d = q \in P_n$ ist $m^+(\acute{Y}_q) = 0$ (falls $q \neq 2$). Sonst ist $\acute{Y}_d$ ein P-Kreismodul, für den in Abschnitt 2.4.1 bereits Normalbasen konstruiert sind, woraus sich die Invarianten ablesen lassen. Wie beim Kreissystem läßt sich dann direkt durch Aufsummieren die Gutartigkeit von $\acute{\Gamma}(n)$ nachweisen.

Mit der Gutartigkeit erhalten wir in Analogie zu Satz 2.2.14 den folgenden Satz über die Konstruktion von Basen von $\acute{\mathcal{L}}(n)$, $\acute{\mathcal{L}}(n)_+$ und $\acute{\mathcal{L}}(n)_-$. Dabei ist im Gegensatz zur Situation für $\mathcal{L}(n)$ die Unterscheidung zwischen $n \equiv 0 \bmod 4$ und $n \not\equiv 0 \bmod 4$ nicht notwendig.

Satz 2.4.5 *Zu $n \in \mathbf{N}$ sei $\acute{\mathcal{L}}(n)$ der kombinierte P-Kreismodul, der als Kombinat des n-ten P-Kreissystems $\acute{\Gamma}(n) = (M_d, \acute{\mathcal{E}}_d, \acute{\mathfrak{n}}_d)_{d\in T_n}$ entsteht, und zu $d \in T_n$ sei $\acute{Y}_d := M_d/\langle\acute{\mathcal{E}}_d\rangle$. Dann erhält man Basen von $\acute{\mathcal{L}}(n)$, $\acute{\mathcal{L}}(n)_+$ und $\acute{\mathcal{L}}(n)_-$ durch Vereinigung von in M_d lebenden Basen von $\acute{Y}_d$, $(\acute{Y}_d)_+$ beziehungsweise $(\acute{Y}_d)_-$, wobei d alle P-Teiler von n durchläuft.*

Durch den Isomorphismus zu $\mathcal{L}(n)_+$ ist $\acute{\mathcal{L}}(n)_+$ auch isomorph zu der Gruppe der Kreiszahlen $D^{(n)}$. Ohne das näher zu erläutern sei angemerkt, daß sich wie in Abschnitt 2.3.3 auch P-relative Kreiszahlen definieren lassen, indem man statt aller Teiler wieder nur P-Teiler verwendet. Von diesen läßt sich dann

zeigen, daß sie im wesentlichen isomorph zu den P-Kreismoduln sind. Wir führen das hier nicht näher aus, weil wir im folgenden Abschnitt herausarbeiten, daß das P-Kreissystem systematische Nachteile bei der Konstruktion von Basen von Kreiszahlen hat, und es daher sinnvoll ist, dazu auf das Kreissystem zurückzugreifen, und das P-Kreissystem nicht weiter zu verfolgen.

2.4.3 Der P-Kreismodul im direkten Vergleich

Wie haben nun festgestellt, daß sich die Kreiszahlen sowohl als kombinierter Kreismodul als auch als kombinierter P-Kreismodul interpretieren lassen.

Wir zeigen zunächst an einem Beispiel, wie der Unterschied zwischen $\acute{\mathcal{L}}(n)$ und $\mathcal{L}(n)$ zu verstehen ist, und diskutieren anschließend die Vor- und Nachteile von $\acute{\mathcal{L}}(n)$ gegenüber $\mathcal{L}(n)$.

Im folgenden bezeichnen wir die Elemente aus $a \in G_d$ wieder mit $[d, a]$.

Beispiel

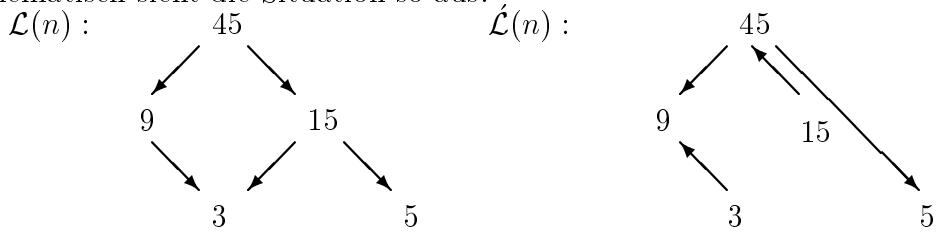
Es sei $n = 45$. Die Teiler von n sind $1, 3, 5, 9, 15$ und 45. Die P-Teiler sind $1, 9, 5$ und 45. Wir können dann die Gruppe der Kreiszahlen $D^{(45)}$ einerseits als Kreismodul $\mathcal{L}(45)$ interpretieren, andererseits als P-Kreismodul $\acute{\mathcal{L}}(n)$. Wie wird nun beispielsweise $1 - \epsilon_{15} \in D^{(45)}$ durch Basiselemente dargestellt?

Interpretieren wir $D^{(45)}$ als Kreismodul $\mathcal{L}(45)$, so entspricht die Kreiszahl $1-\epsilon_{15}$ dem Element $[15, 1] \in G_{15}$.

Im Falle von $\mathcal{L}(15)$ kann entweder $[15, 1]$ schon Teil einer Basis sein, oder aber man schreibt $[15, 1]$ modulo Zeilensummen als eine Summe von Basiselementen $[15, *]$. Dabei treten eventuell (bedingt durch die störenden Abbildungen $\mathfrak{n}_{15}$) Elemente $[5, *]$ und $[3, *]$ auf. Insbesondere fällt auf, daß es völlig ausreicht in $\mathcal{L}(15)$ statt in $\mathcal{L}(45)$ zu arbeiten.

Interpretieren wir die Gruppe der Kreiszahlen als P-Kreismodul $\acute{\mathcal{L}}(45)$, so ist $1 - \epsilon_{15}$ gar nicht direkt als Bild der Abbildung $\acute{\mathcal{L}}(45)_+ \to D^{(45)}$ verfügbar. Orientiert man sich am Beweis zu Satz 2.4.4, so erhält man eine Darstellung von $1 - \epsilon_{15}$ als Summe von Elementen der Form $[45, *] \in G_{45}$. Stellt man diese Summe wiederum durch Basiselemente dar, kommen eventuell solche der Form $[9, *]$ oder $[5, *]$ hinzu.

Schematisch sieht die Situation so aus:



Dabei gibt die Pfeilrichtung $d \to t$ an, daß bei der Darstellung eines Elementes $[d, *]$ durch Basiselemente in der Basisdarstellung Elemente $[t, *]$ vorkommen können. Hier sieht man anschaulich den Vorteil von $\mathcal{L}(n)$: Die Pfeile laufen alle in eine Richtung, das Diagramm für $n = 15$ ist als Subdiagramm enthalten,

und es ist beispielsweise zu einem Diagramm für $n = 135$ erweiterbar.

Trotzdem wurden bisher in [2], [5] und [8] für die Konstruktion von Basen von Kreiseinheiten Konstruktionen über P-Teiler verwendet. Dies ist im wesentlichen auf zwei Gründe zurückzuführen.

- Im Fall, daß $n = p^\alpha$ die Potenz einer Primzahl ist, ist $\acute{\mathcal{L}}(p^\alpha)$ nach Definition 2.4.3 einfach gleich $\langle G_{p^\alpha} \rangle$. Im Gegensatz dazu wird $\mathcal{L}(p^\alpha)$ in Definition 2.2.1 aus mehreren Moduln $Y_{p^\beta} = M_{p^\beta}/\langle \mathcal{E}_{p^\beta} \rangle$ mit $1 \leq \beta \leq \alpha$ zusammengesetzt, wobei $Y_p = \langle G_p \rangle$ und $Y_{p^\beta} = Z(p^\beta)$ für $\beta > 1$ ist.

- Konstruiert man aus der Menge aller Erzeuger $1 - \epsilon_d^a$ eine Basis durch sukzessives Entfernen von Elementen, so ist der Schritt, die Erzeuger, bei denen d kein P-Teiler ist, zu entfernen, elementar. (Er entspricht dem Beweis der Surjektivität von ψ im Beweis zu Satz 2.4.4.) Man kann dann anschließend mit einer kleineren Menge von Erzeugern rechnen.

Die folgenden Überlegungen sprechen jedoch gegen $\acute{\mathcal{L}}(n)$ und für die Verwendung von $\mathcal{L}(n)$.

- $\acute{\mathcal{L}}(n)$ verwischt die hierarchische Ordnung, die für $d|n$ die Struktur von $\mathcal{L}(d)$ als Teilstruktur von $\mathcal{L}(n)$ identifizierbar macht.

- Ein Analogon zu $\mathcal{L}(\infty)$, das heißt, zur Konstruktion einer Basis *aller* Kreiszahlen, wie sie in Satz 2.3.8 beschrieben ist, existiert nicht.

- Außerdem suggeriert die Interpretation von Kreiseinheiten als kombinierter P-Kreismodul $\acute{\mathcal{L}}(n)$ fälschlicherweise, daß die Normrelationen innerhalb der Kreiszahlen von zweierlei Natur sind, nämlich Relationen, die das Problem auf die Betrachtung von P-Teilern zurückführen, und solche, die in $\acute{\mathcal{L}}(n)$ bestehen. In Wirklichkeit sind aber alle Relationen von der Form Zeilensumme $+\mathfrak{n}_d$(Zeilensumme).

Aus diesen Gründen wird im Rest der Arbeit, das heißt, bei der Bestimmung der Basis von Kreiseinheiten etc. nicht mehr mit $\acute{\mathcal{L}}(n)$, sondern mit $\mathcal{L}(n)$ gearbeitet werden.

3 Kreiseinheiten

Es sei ϵ_n eine n-te Einheitswurzel. Die Gruppe der Kreiszahlen $D^{(n)}$ ist nach Kapitel 2.3 definiert als die von den Zahlen $1-\epsilon_n^a$ mit $a \in \mathbf{Z}$ und $a \not\equiv 0 \bmod n$ erzeugte Gruppe modulo Einheitswurzeln. Als die Gruppe der Kreiseinheiten $C^{(n)}$ wird die Untergruppe der Kreiszahlen bezeichnet, die aus Einheiten der Maximalordnung $\mathbf{Z}[\epsilon_n]$ von $\mathbf{Q}(\epsilon_n)$ besteht.

Während im Fall, daß n keine Primzahlpotenz ist, bereits $1-\epsilon_n$ eine Einheit in $\mathbf{Z}[\epsilon_n]$ ist, wird die Einheitengruppe im Fall, daß $n = q$ Primzahlpotenz ist, von Elementen der Form $(1-\epsilon_q^a)/(1-\epsilon_q)$ erzeugt (siehe Abschnitt 1.3 in [2]).

Ziel dieses Kapitels ist die explizite Konstruktion einer Basis von $C^{(n)}$ für $n \in \mathbf{N} \cup \{\infty\}$. Dazu untersuchen wir zur Vorbereitung im ersten Abschnitt den Zusammenhang zwischen Kreiseinheiten und Kreiszahlen. Im zweiten Abschnitt wird dann das Problem der Konstruktion einer Basis dadurch gelöst, indem wir einerseits zeigen, daß wir eine Basis der Gruppe der Kreiseinheiten durch Vereinigung von Basen von relativen Kreiseinheiten erhalten und andererseits von relativen Kreiszahlen auf relative Kreiseinheiten schließen.

Da wir nicht nur an einer prinzipiellen Vorgehensweise, sondern an einer *expliziten Konstruktion* einer Basis interessiert sind, beschreiben wir im anschließenden dritten Abschnitt ausführlich den Weg von Normalzerlegungen von Mengen über Quasinormalbasen von Kreismoduln bis hin zu einer Basis der Gruppe der Kreiseinheiten. Dieser Abschnitt wird abgerundet durch ein Beispiel für $n = 45$.

Schließlich gehen wir im letzten Abschnitt dieses Kapitels kurz auf die Relationen ein, die zwischen den Erzeugern der Kreiseinheiten bestehen.

3.1 Kreiszahlen und Kreiseinheiten

Wir führen im folgenden die Kreiseinheiten als Untergruppe der Kreiszahlen ein. Das soll jedoch nicht darüber hinwegtäuschen, daß die eigentlich wichtige Gruppe die der Kreiseinheiten ist, da sie als Untergruppe von endlichem Index der Einheitengruppe der Maximalordnung von $\mathbf{Q}(\epsilon_n)$ eigenständige Bedeutung in der algebraischen Zahlentheorie hat. Die Kreiszahlen sind "nur" ein Hilfsmittel im Rahmen dieser Arbeit, um Ergebnisse über Kreiseinheiten herzuleiten.

Definition 3.1.1 *Es sei $n \in \mathbf{N}$, und es bezeichne $U\mathbf{Z}[\epsilon_n]$ die Einheitengruppe von $\mathbf{Z}[\epsilon_n]$ modulo Torsion. Ist $D^{(n)}$ die Gruppe der n-ten Kreiszahlen, dann definieren wir $C^{(n)} := D^{(n)} \cap U\mathbf{Z}[\epsilon_n]$ als die* Gruppe der n-ten Kreiseinheiten.

Die Kreiseinheiten sind also genau die Kreiszahlen, die in $\mathbf{Z}[\epsilon_n]$ invertierbar sind. Das bedeutet, daß sich die Kreiseinheiten auch charakterisieren lassen als Kreiszahlen mit Absolutnorm ± 1, was in den folgenden Beweisen des öfteren benutzt wird.

In [11] konstruiert Ramachandra $\frac{1}{2}\varphi(n) - 1$ unabhängige Einheiten aus $C^{(n)}$, deren Erzeugnis endlichen Index in $C^{(n)}$ hat. In der Tat gilt:

Lemma 3.1.2 *Es sei $n > 2$. Dann ist $\operatorname{rg} C^{(n)} = \frac{1}{2}\varphi(n) - 1$.*

Beweis
In [15] wird gezeigt, daß $C^{(n)}$ endlichen Index in $U\mathbf{Z}[\epsilon_n]$ hat. Nach dem Dirichletschen Einheitensatz (siehe beispielsweise [17], Proposition 7-6-1) hat $U\mathbf{Z}[\epsilon_n]$ den Rang $\frac{1}{2}\varphi(n) - 1$.

QED.

Die Kreiszahlen $D^{(n)}$ sind verschieden von den Kreiseinheiten $C^{(n)}$. Beispielsweise ist $1-\epsilon_q \in D^{(q)}$, jedoch nicht in $C^{(q)}$, wenn q eine Potenz einer Primzahl ist. Ein Erzeugendensystem von $C^{(n)}$ gibt das folgende Lemma an.

Lemma 3.1.3 *Es sei $n \in \mathbf{N}$. Dann wird $C^{(n)}$ von den Elementen*

$$\frac{1-\epsilon_q^a}{1-\epsilon_q} \text{ mit } q|n \text{ und } q \text{ ist Primzahlpotenz, } a \in G_q, \text{ und}$$

$$1-\epsilon_d^a \text{ wobei } 1 < d|n \text{ und } d \in \mathbf{N} \text{ keine Primzahlpotenz ist, } a \in G_d$$

erzeugt.

Beweis
Einen Beweis dazu findet man beispielsweise in [2] auf Seite 25.

QED.

Die nächsten beiden Lemmata beschreiben genau den Zusammenhang zwischen Kreiseinheiten und Kreiszahlen. Im folgenden sei

$$n = q_1 \cdots q_r = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \tag{128}$$

mit $q_i = p_i^{\alpha_i}$ für $i = 1, \ldots, r$ die eindeutige Zerlegung von n in ein Produkt von Primzahlpotenzen. Dann ist $P_n = \{q_1, \ldots, q_r\}$.

Lemma 3.1.4 *Zu $n \in \mathbf{N}$ seien E ein beliebiges Erzeugendensystem der Gruppe der Kreiseinheiten $C^{(n)}$ und $r = |P_n|$ die Anzahl der Primteiler von n. Dann gilt:*

a) *Die Gruppe $D^{(n)}$ der Kreiszahlen wird erzeugt durch $E \cup \bigcup_{q \in P_n} \{1-\epsilon_q\}$.*

b) *Die Elemente $1-\epsilon_q$ mit $q \in P_n$ sind voneinander und von E linear unabhängig.*

c) $\operatorname{rg} D^{(n)} = \operatorname{rg} C^{(n)} + r$.

Beweis
Für Teil a reicht es, die Behauptung für ein festes Erzeugendensystem E_0 zu zeigen, da E_0 seinerseits im Erzeugnis von E liegt. Wir wählen E_0 als das Erzeugendensystem aus Lemma 3.1.3.

Es reicht nach Lemma 3.1.3 ferner zu zeigen, daß für alle $p = p_i$ und $\beta < \alpha := \alpha_i$ die Kreiszahl $1 - \epsilon_{p^\beta}$ von $1 - \epsilon_q$ für $q = p^\alpha$ und E_0 erzeugt wird, denn dann folgt aus

$$1 - \epsilon_{p^\beta}^a = \underbrace{\frac{1 - \epsilon_{p^\beta}^a}{1 - \epsilon_{p^\beta}}}_{\in C^{(n)}} (1 - \epsilon_{p^\beta}), \tag{129}$$

daß auch $1 - \epsilon_{p^\beta}^a$ für alle $a \in G_{p^\beta}$ erzeugt wird, und damit alle Erzeugenden von $D^{(n)}$ erzeugt werden.

Daß $1 - \epsilon_{p^\beta}$ erzeugt wird, folgt durch Induktion, indem man die Normrelation

$$\prod_{\substack{b \in G_q \\ b \equiv 1 \bmod q/p}} (1 - \epsilon_q^b) = 1 - \epsilon_{q/p} \tag{130}$$

für $p \neq q$ ausnutzt, die ein Spezialfall der Normrelation in (118) ist. Damit ist Teil a bewiesen.

Ist $u \in \langle E \rangle = C^{(n)}$, so erhalten wir aus einer Relation $1 = u \prod_{i=1}^r (1 - \epsilon_{q_i})^{b_i}$ mit $b_i \in \mathbf{Z}$ durch Normbildung von $\mathbf{Q}(\epsilon_n)$ nach $\mathbf{Q}$, daß $1 = \prod_{i=1}^r p_i^{b_i k_i}$ mit $k_i = \varphi(n)/\varphi(q_i) \neq 0$ ist. Also ist $b_i = 0$ für alle $i \in \{1, \ldots, r\}$, und es folgt Teil b.

Teil c ergibt sich durch Anwendung von a und b, indem wir den Fall betrachten, daß E sogar Basis ist.

QED.

Den Schlüssel zur Konstruktion einer Basis von $C^{(n)}$ aus einer Basis von $D^{(n)}$ liefert die Umkehrung von Teil a in Verbindung mit Teil b in Lemma 3.1.4, die wir im folgenden gleich für Basen formulieren.

Lemma 3.1.5 *Es seien $n \in \mathbf{N}$ und $B \subseteq C^{(n)}$. Ist $B \cup \bigcup_{q \in P_n} \{1 - \epsilon_q\}$ eine Basis von $D^{(n)}$, so ist bereits B eine Basis von $C^{(n)}$.*

Beweis
Natürlich ist B auch in $C^{(n)}$ linear unabhängig, es bleibt zu zeigen, daß B ein Erzeugendensystem von $C^{(n)}$ ist. Dies geschieht wie im Beweis von Teil b in Lemma 3.1.4: Da B Basis von $D^{(n)}$ ist, läßt sich $u \in C^{(n)}$ sicher schreiben als $u = v \prod_{i=1}^r (1 - \epsilon_{q_i})^{b_i}$ mit $v \in \langle B \rangle$ und $b_i \in \mathbf{Z}$. Normbildung zeigt $b_i = 0$ für alle $i = 1, \ldots, r$.

QED.

3.2 Relative Kreiseinheiten und relative Kreiszahlen

Wir konstruieren im folgenden Basen der Kreiseinheiten $C^{(n)}$. Dies geschieht dadurch, daß wir wie bei den Kreiszahlen analog zu Definition 2.3.4 relative

Kreiseinheiten $\widehat{C^{(n)}}$ einführen, und mit Hilfe des entsprechenden Ergebnisses über Kreiszahlen zeigen, daß die Vereinigung von in $C^{(n)}$ lebenden Basen von $\widehat{C^{(d)}}$ für $d|n$ eine Basis von $C^{(n)}$ ergibt.

Definition 3.2.1 *Zu $n \in \mathbf{N}$ sei $C^{(n)}$ die Gruppe der Kreiseinheiten, und $L^{(n)} := \prod_{d||n} C^{(d)}$. Dann bezeichnen wir mit $\widehat{C^{(n)}} := C^{(n)}/L^{(n)}$ die Gruppe der n-ten* relativen Kreiseinheiten.

Wir geben zunächst an, wie die relativen Kreiszahlen $\widehat{D^{(n)}}$ mit den relativen Kreiseinheiten zusammenhängen. Dazu schreiben wir $\widehat{D^{(n)}} := D^{(n)}/K^{(n)}$ mit $K^{(n)} = \prod_{d||n} D^{(d)}$ und definieren (in Analogie zu (35) in Abschnitt 1.5 über Differenzenmoduln, wobei die Negation dort der Division hier entspricht)

$$\Delta\widehat{D^{(n)}} := \langle \frac{1-\epsilon_n^a}{1-\epsilon_n} K^{(n)};\ a \in G_n \rangle. \tag{131}$$

Eine Basis von $\Delta\widehat{D^{(n)}}$ läßt sich mit Hilfe der in Abschnitt 1.5 entwickelten Methoden und der Isomorphismen aus Satz 2.3.5 konstruieren. Wir geben diese Konstruktion später explizit an. Zunächst gehen wir aber auf den Zusammenhang zwischen relativen Kreiseinheiten und relativen Kreiszahlen ein.

Satz 3.2.2 *Zu $n \in \mathbf{N}$ bezeichne $\widehat{C^{(n)}}$ die relativen Kreiseinheiten und $\widehat{D^{(n)}}$ die relativen Kreiszahlen.*

a) Ist n keine Primzahlpotenz, so gilt $\widehat{C^{(n)}} \cong \widehat{D^{(n)}}$.

b) Ist $n = q$ eine Primzahlpotenz, so ist $\widehat{C^{(q)}} \cong \Delta\widehat{D^{(q)}}$.

Ist $L^{(n)} = \prod_{d||n} C^{(d)}$ und $K^{(n)} = \prod_{d||n} D^{(d)}$, dann ist der Isomorphismus dadurch gegeben, daß $uL^{(n)}$ auf $uK^{(n)}$ für $u \in C^{(n)}$ abgebildet wird.

Beweis
Es ist $\widehat{C^{(n)}}$ rein formal keine Untergruppe von $\widehat{D^{(n)}}$. Mit einer ähnlichen Normbildung wie im Beweis von Lemma 3.1.4 zeigt man $C^{(n)} \cap K^{(n)} = L^{(n)}$ und erhält

$$\widehat{C^{(n)}} \cong C^{(n)}K^{(n)}/K^{(n)} \leq \widehat{D^{(n)}}. \tag{132}$$

Somit ergibt sich eine Einbettung $\psi : \widehat{C^{(n)}} \hookrightarrow \widehat{D^{(n)}}$.
Mit Lemma 3.1.3 erhält man aus dem Erzeugendensystem von $C^{(n)}$ ein Erzeugendensystem von $\widehat{C^{(n)}}$, und zwar

$$\begin{array}{ll} \{\frac{1-\epsilon_q^a}{1-\epsilon_q};\ a \in G_q\} & \text{falls } n = q \text{ die Potenz einer Primzahl ist,} \\ \{1-\epsilon_n^a;\ a \in G_n\} & \text{sonst.} \end{array} \tag{133}$$

Ein Erzeugendensystem von $\widehat{D^{(n)}}$ wird offensichtlich induziert durch

$$\{1-\epsilon_n^a;\ a\in G_n\}. \tag{134}$$

Gemäß (131) induziert

$$\{\frac{1-\epsilon_n^a}{1-\epsilon_n};\ a\in G_n\} \tag{135}$$

eine Erzeugendensystem von $\Delta\widehat{D^{(n)}}$. Durch Vergleich von (133) mit (134) in Teil a und (135) in Teil b folgt, daß ψ surjektiv ist, also Isomorphismus.

QED.

Basen für $\widehat{C^{(n)}}$ lassen sich also direkt aus Basen von $\widehat{D^{(n)}}$ beziehungsweise $\Delta\widehat{D^{(n)}}$ ableiten. Eine Basis von $C^{(n)}$ erhält man durch Vereinigung von Basen von $\widehat{C^{(d)}}$ mit $d|n$. Genauer gilt der folgende Satz:

Satz 3.2.3 *Es sei $n\in\mathbf{N}$. Zu $d|n$ induziere $\widehat{B_d}\subseteq C^{(n)}$ eine Basis von $\widehat{C^{(d)}}$. Dann ist $B_n:=\bigcup_{d|n}\widehat{B_d}$ eine Basis von $C^{(n)}$.*

Beweis

Es sei zunächst p eine Primzahl und $\alpha>0$. Ist $L^{(n)}:=\prod_{d||n}C^{(d)}$, so ist, da $C^{(p^{\alpha-1})}=L^{(p^\alpha)}$ ist, die Sequenz

$$1\to C^{(p^{\alpha-1})}\to C^{(p^\alpha)}\to\widehat{C^{(p^\alpha)}}\to 1 \tag{136}$$

exakt. Die Gruppe $\widehat{C^{(p^\alpha)}}$ ist torsionsfrei, da sie nach Satz 3.2.2 isomorph zu einer Untergruppe der Gruppe der relativen Kreiszahlen $\widehat{D^{(p^\alpha)}}$ ist, die für $p^\alpha\neq 4$ nach Korollar 2.3.6 torsionsfrei ist, und man rechnet direkt aus der Definition der Kreiseinheiten nach, daß $\widehat{C^{(4)}}=1$, also trivialerweise torsionsfrei ist.

Mit Lemma 1.6.2 (die additiv geschriebenen $\mathbf{Z}$-Moduln dort entsprechen multiplikativ geschriebenen abelschen Gruppen hier) folgt Satz 3.2.3 für $n=p^\alpha$. Für $q:=p^\alpha$ ist also $B_q:=\bigcup_{i=1}^{\alpha}\widehat{B_{p^i}}$ eine Basis von $C^{(q)}$. Aus Lemma 3.1.4 folgt damit, daß $G_q:=\{1-\epsilon_q\}\cup B_q$ eine Basis von $D^{(q)}$ ist.

Sei nun $n=q_1\cdots q_r=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ das Produkt paarweise teilerfremder Primzahlpotenzen, und es sei Θ_n die Menge aller Teiler von n, die keine Potenzen von Primzahlen sind.

Da nach Satz 3.2.2 $\widehat{C^{(d)}}\cong\widehat{D^{(d)}}$ für $d\in\Theta_n$ gilt, existieren nach Satz 2.3.8 $\widehat{F_d}\subseteq D^{(n)}$ mit den folgenden Eigenschaften:

a) $F_n:=\bigcup_{d|n}\widehat{F_d}$ ist eine Basis von $D^{(n)}$,

b) $F_{q_i}:=\bigcup_{d|q_i}\widehat{F_d}$ ist eine Basis von $D^{(q_i)}$ für $i=1,\ldots,r$,

c) $\widehat{F_d}=\widehat{B_d}$ für $d\in\Theta_n$.

Die Eigenschaft c zeigt, daß $\bigcup_{i=1}^{r} F_{q_i} \cup \bigcup_{d\in\Theta_n} \widehat{B_d}$ gleich F_n, und damit nach a Basis von $D^{(n)}$ ist. Wir haben bereits gezeigt, daß $G_{q_i} = \{1-\epsilon_{q_i}\} \cup \bigcup_{j=1}^{\alpha_i} \widehat{B_{p_i^j}}$ eine Basis von $D^{(q_i)}$ ist. Nach Eigenschaft b, können wir die F_{q_i} durch die G_{q_i} austauschen und erhalten, daß

$$\bigcup_{i=1}^{r} G_{q_i} \cup \bigcup_{d\in\Theta_n} \widehat{B_d} = \bigcup_{i=1}^{r} \{1-\epsilon_{q_i}\} \cup \bigcup_{d|n} \widehat{B_d} = \bigcup_{i=1}^{r} \{1-\epsilon_{q_i}\} \cup B_n \qquad (137)$$

eine Basis von $D^{(n)}$ ist. Mit Lemma 3.1.5 folgt, daß B_n Basis von $C^{(n)}$ ist, also die Behauptung.

QED.

Bemerkung 3.2.4 *Anders, als bei dem analogen Satz 2.3.8 für Kreiszahlen, ist hier eine Unterscheidung der Fälle $n \equiv 0 \bmod 4$ und $n \not\equiv 4 \bmod 0$ nicht notwendig, da $\widehat{C^{(4)}}$ und $\widehat{C^{(2)}}$ im Gegensatz zu $\widehat{D^{(4)}}$ und $\widehat{D^{(2)}}$ trivial sind, und daher in jedem Fall keinen Beitrag zu einer Basis von $C^{(n)}$ liefern.*

Bisher haben wir nur $n \in \mathbf{N}$ betrachtet. Wie bei den Kreiszahlen kann man auch $n = \infty$ zulassen.

Korollar 3.2.5 *Es sei $C^{(\infty)} := \bigcup_{d\in\mathbf{N}} C^{(d)}$ und $\widehat{B_d}$ eine in $C^{(\infty)}$ lebende Basis von $\widehat{C^{(d)}}$. Dann ist $B^{(\infty)} := \bigcup_{d\in\mathbf{N}} \widehat{B_d}$ eine Basis von $C^{(\infty)}$.*

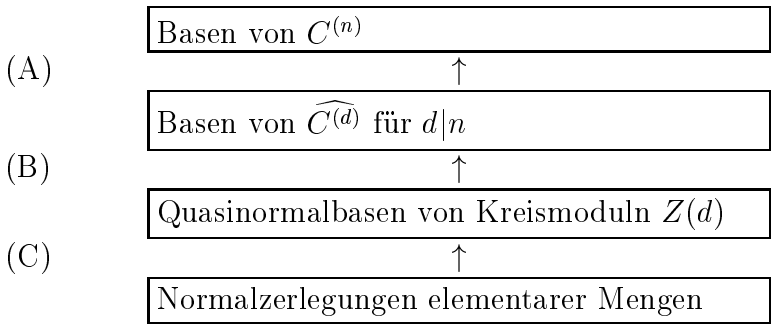
Beweis
Da jedes $u \in C^{(\infty)}$ in wenigstens einem der $C^{(n)}$ mit $n \in \mathbf{N}$ liegt, kann man sich zum Beweis der linearen Unabhängigkeit und zum Beweis, daß $B^{(\infty)}$ ein Erzeugendensystem ist, auf endliche Stücke zurückziehen.

QED.

3.3 Eine Basis der Kreiseinheiten

Im vorangegangenen Abschnitt wurde das Problem der Konstruktion einer Basis der Gruppe der Kreiseinheiten $C^{(n)}$ im Prinzip gelöst. Wir beschreiben im folgenden als Zusammenfassung der bisherigen Arbeit explizit, wie wir eine Basis von $C^{(n)}$ mit den bisher entwickelten Sätzen und Methoden erhalten.

Wir gliedern zunächst den Weg zu einer Basis von $C^{(n)}$ in drei Schritte (A), (B) und (C) auf, die wir anschließend im einzelnen erläutern.



zu(A): Die Methode eine Basis der Kreiseinheiten $C^{(n)}$ aus Basen der $\widehat{C^{(d)}}$ für $d|n$ zu konstruieren, ist nach Satz 3.2.3 denkbar einfach. In $C^{(n)}$ lebende Basen von $\widehat{C^{(d)}}$ sind zu vereinigen.

Weitaus komplexer ist der Aufwand zum Beweis von Satz 3.2.3. Dabei wird zunächst das entsprechende Ergebnis für die Gruppe der Kreiszahlen in Satz 2.3.8 formuliert. Um diesen Satz zu beweisen, werden die relativen Kreiszahlen mit Hilfe von Satz 2.3.5 mit den Kreismoduln $Z(d)$ für $d|n$ in Verbindung gebracht, die aufgefaßt als Moduln $M_d/\langle \mathcal{E}_d \rangle$, wobei M_d das freie Erzeugnis von G_d und $\mathcal{E}_d$ die Menge der Zeilensummen ist, zu dem Kreissystem $\Gamma(n)$ zusammengesetzt werden (Definition 2.2.1). Die Möglichkeit, Basen eines Moduls aus der Vereinigung von Basen geeigneter "Stücke" dieses Moduls zu erhalten, wird durch die Konzepte der Kombinierbarkeit und Gutartigkeit erfaßt. Die Kombinierbarkeit des Kreissystems liefert Lemma 2.2.3 und Satz 2.2.13 zeigt die Gutartigkeit, woraus mit Satz 1.6.14 die einfache Basenkonstruktion durch Vereinigung folgt.

zu (B): Um aufzuzeigen, wie wir aus Quasinormalbasen von Kreismoduln Basen der relativen Kreiszahlen $\widehat{C^{(d)}}$ erhalten, unterscheiden wir drei Fälle in Abhängigkeit von d.

$d = p$ Primzahl: Dazu sei zunächst angemerkt, daß in diesem Fall $\widehat{C^{(p)}} = C^{(p)}$ ist. Basen von $C^{(p)}$ sind wohlbekannt, und beispielsweise bereits in [2], Satz 5 konstruiert worden.

Mit den in dieser Arbeit entwickelten Methoden erhält man eine Basis von $\widehat{C^{(p)}}$ über die Isomorphismen

$$\widehat{C^{(p)}} \cong \Delta \widehat{D^{(p)}} \cong \Delta \langle G_p \rangle_+ . \tag{138}$$

Der linke Isomorphismus in (138) folgt aus Satz 3.2.2, der rechte Isomorphismus aus $\widehat{D^{(p)}} \cong \langle G_p \rangle_+$ nach Satz 2.3.5. Eine Normalbasis von $\langle G_p \rangle$ ist $[\{1, \ldots, \lfloor p/2 \rfloor\}, \emptyset, \emptyset]$, und daher induziert nach Lemma 1.2.10, a $\{1, \ldots, \lfloor p/2 \rfloor\}$ eine Basis von $\langle G_p \rangle$.

Eine Basis von $\Delta \langle G_p \rangle_+$ erhält man mit Lemma 1.5.7, a mit $M = \langle G_p \rangle$ und $R = \ker_M (\sigma + 1)$, so daß $M/R = \langle G_p \rangle_+$ gilt. Setzen wir in Lemma 1.5.7 $c^\sharp := 1 \in G_p$, so erhalten wir $\{[a] - [1];\ 1 < a < p/2\}$ als Basis von $\Delta \langle G_p \rangle_+$, und mit (138)

$$\{\frac{1 - \epsilon_p^a}{1 - \epsilon_p};\ 1 < a < \tfrac{1}{2}p\} \tag{139}$$

als Basis von $\Delta \widehat{D^{(p)}}$.

$d = q = p^\alpha$ Potenz einer Primzahl mit $\alpha > 1$: Es reicht hier, $q \neq 4$ zu betrachten, denn, wie man direkt nachrechnet, ist $\widehat{C^{(4)}} = 1$. Analog

zum Fall $n = p$ erhalten wir mit den Sätzen 3.2.2 und 2.3.5 einen Isomorphismus

$$\widehat{C^{(q)}} \cong \Delta\widehat{D^{(q)}} \cong \Delta Z(q)_+. \tag{140}$$

Eine Basis von $\Delta Z(q)_+$ erhält man mit Satz 1.5.16, b, für $\Lambda = G_{q/p}$ und $A = A_p := \{0, \ldots, p-1\}$. Setzen wir speziell

$$\Gamma = \{a \in G_{q/p};\ 1 \le a \le \tfrac{1}{2}q/p\}, \tag{141}$$

$\lambda^\sharp = 1$ und $a^\sharp = 0$, so induziert demnach

$$\{(\lambda, a) - (1, 0);\ (\lambda, a) \in \Gamma \times \{1, \ldots, p-1\}\} \tag{142}$$

eine Basis von $\Delta Z(q)_+$.

Der Isomorphismus $\widehat{D^{(q)}} \cong Z(q)_+$ wird im Beweis zu Satz 2.1.3 und Satz 2.3.3 explizit beschrieben (siehe dazu auch (146) im nächsten Abschnitt). Schreiben wir $Z(q) = \langle G_{q/p} \times A_p \rangle / R$ mit geeignetem R, so wird dort $(\lambda, a) \in G_{q/p} \times A_p$ auf $ap^{\alpha-1} + \lambda \in G_q$ abgebildet. Mit der Basis aus (142) erhalten wir

$$\{\frac{1 - \epsilon_q^{ap^{\alpha-1}+\lambda}}{1 - \epsilon_q};\ (\lambda, a) \in \Gamma \times \{1, \ldots, p-1\}\} \tag{143}$$

mit Γ aus (141) als in $C^{(q)}$ lebende Basis von $\widehat{C^{(q)}}$.

<u>d keine Potenz einer Primzahl:</u> In diesem Fall ist nach den Sätzen 3.2.2 und 2.3.5

$$\widehat{C^{(d)}} \cong \widehat{D^{(d)}} \cong Z(d)_+. \tag{144}$$

Eine Basis von $Z(d)_+$ erhalten wir nach Lemma 1.2.10 mit Hilfe einer Quasinormalbasis von $Z(d)$. Normalbasen und Quasinormalbasen von Kreismoduln wurden in Abschnitt 2.1.2 ausführlich entwickelt. Dabei traten verschiedene Fälle auf, nämlich $d \equiv 2 \bmod 4$, $d = u$ oder $d = 4u$, wobei u ungerade und quadratfrei ist, und alle sonstigen Fälle.

Allen Fällen ist gemeinsam, daß eine Quasinormalbasis von $Z(d)$ für $d = q_1 \cdots q_r = p_1^{\alpha_1} \cdots p_t^{\alpha_t} p_{t+1} \cdots p_r$ mit $\alpha_i > 1$ für $i = 1, \ldots, t$ wie etwa in (84) gegeben ist als Teilmenge von

$$S := \Lambda_{q_1} \times A_{p_1} \times \cdots \times \Lambda_{q_t} \times A_{p_t} \times G_{p_{t+1}} \times \cdots \times G_{p_r} \tag{145}$$

mit $\Lambda_{q_i} = G_{q_i/p_i}$ und $A_{p_i} = \{0, \ldots, p_i - 1\}$. Der Weg von dieser Teilmenge zu einer Basis der Kreiseinheiten wird durch Satz 2.1.3 beschrieben, der aufzeigt, wie der d-te Kreismodul als freies Erzeugnis über G_d modulo gewisser Relationen interpretiert werden kann. Der Isomorphismus wird explizit im Beweis von Satz 2.1.3 beschrieben. Wir erhalten die Bijektion $\zeta : S \to G_d$ mit Hilfe geeigneter

Bijektionen ξ und η gemäß

$$\begin{array}{ccccccc} \underbrace{\Lambda_{q_1} \times A_{p_1}} & \times \cdots \times & \underbrace{\Lambda_{q_t} \times A_{p_t}} & \times & G_{p_{t+1}} & \times \cdots \times & G_{p_r} \\ \downarrow \xi_1 & & \downarrow \xi_t & & \downarrow \mathrm{id} & & \downarrow \mathrm{id} \\ G_{q_1} & \times \cdots \times & G_{q_t} & \times & G_{q_{t+1}} & \times \cdots \times & G_{q_r} \\ & & & \downarrow \eta & & & \\ & & & G_d & & & \end{array} \tag{146}$$

Die Abbildungen ξ_i für $i = 1, \ldots, t$ sind dabei explizit gegeben durch $\xi_i(\lambda, a) = a p_i^{\alpha_i - 1} + \lambda$. Die Abbildung $\eta : G_{q_1} \times \cdots \times G_{q_r} \to G_d$ ist durch den Chinesischen Restsatz (Lösen simultaner Kongruenzen) gegeben. Eine explizite, algorithmische Beschreibung von η findet sich beispielsweise bei [7], Kapitel I, §4.9. Es sei angemerkt, daß die Umkehrabbildung η^{-1} einfach gegeben ist durch $a \mapsto (a \bmod q_1, \ldots, a \bmod q_r)$. Insgesamt gilt mit den Abbildungen ψ und κ aus (89), daß $\zeta = (\kappa \circ \psi)^{-1}$ ist.

Ist $[G^0, G^+, G^-]$ eine Quasinormalbasis von $Z(d)$, wie sie in Abschnitt 2.1.2 konstruiert wurde, so ist nach Lemma 1.2.10, a, i $G^0 \cup G^+$ eine Basis von $Z(d)_+$. Vermöge des Isomorphismus aus (144), der durch ζ beschrieben wird, induziert somit

$$\{1 - \epsilon_d^a;\ a \in \zeta(G^0 \cup G^+)\} \tag{147}$$

eine Basis von $\widehat{C^{(d)}}$.

zu (C): Wie man aus geeigneten Normalzerlegungen eine Quasinormalbasis des Kreismoduls erhält, wird ausführlich in Abschnitt 2.1.2 abgehandelt, und soll an dieser Stelle nicht wiederholt werden.

Entscheidend werden dabei die Konstruktionsmethoden aus den Abschnitten 1.3.2 und 1.3.3 benutzt, in denen eine Quasinormalbasis eines Tensorproduktes $L \otimes M$ aus Quasinormalbasen von L und M gebildet wird.

Beispiel

Es sei $n = 45$. Wir erhalten eine Basis von $C^{(45)}$ durch die Vereinigung von in $C^{(45)}$ lebenden Basen der $\widehat{C^{(d)}}$ für $d = 3, 5, 9, 15, 45$. Wir geben diese Basen nun explizit an:

$d = 3, 5$: Wir lesen die Basis direkt aus (139) ab und erhalten $\emptyset$ als Basis von $\widehat{C^{(3)}}$ (das heißt, es ist $\widehat{C^{(3)}} = 1$) und

$$\{(1 - \epsilon_5^2)/(1 - \epsilon_5)\} \tag{148}$$

als Basis von $\widehat{C^{(5)}}$.

$\underline{d = 9:}$ Hier erhalten wir eine Basis direkt aus (143). Es ist $\Gamma = \{1\}$ und somit

$$\{(1-\epsilon_9^4)/(1-\epsilon_9), (1-\epsilon_9^7)/(1-\epsilon_9)\} \tag{149}$$

eine Basis von $\widehat{C^{(9)}}$.

$\underline{d = 15:}$ Eine Basis liefert (147). Die Mengen G^0 und G^+ entnehmen wir dem Fall "quadratfrei und ungerade" aus Abschnitt 2.1.2. Wir erhalten $G^0 = \{(1,2)\}$ und $G^+ = \{(1,1)\}$, und damit $\zeta(G^0 \cup G^+) = \{7,1\}$. Also ist

$$\{1-\epsilon_{15}^7, 1-\epsilon_{15}\} \tag{150}$$

eine Basis von $\widehat{C^{(15)}}$.

$\underline{d = 45:}$ Wie für $d = 15$ folgt die Basis aus (147). Hier entnehmen wir aber G^0 und G^+ dem Fall "sonstige" in Abschnitt 2.1.2, und erhalten $G^+ = \emptyset$ und $G^0 = H_9 \times A_3^\flat \times G_5^\flat$, mit $H_9 = \{1\}$, $A_3^\flat = \{1,2\}$ und $G_5^\flat = \{2,3,4\}$ gemäß (84). Explizit ist

$$G^0 = \{(1,1,2),(1,1,3),(1,1,4),(1,2,2),(1,2,3),(1,2,4)\}, \tag{151}$$

und es folgt $\zeta(G^0) = \{22,13,4,7,43,34\}$. Eine Basis von $\widehat{C^{(45)}}$ ist daher gegeben durch

$$\{1-\epsilon_{45}^{22}, 1-\epsilon_{45}^{13}, 1-\epsilon_{45}^4, 1-\epsilon_{45}^7, 1-\epsilon_{45}^{43}, 1-\epsilon_{45}^{34}\}. \tag{152}$$

Insgesamt ist also die Vereinigung von (148), (149), (150) und (152) eine Basis von $C^{(45)}$.

3.4 Relationen der Kreiseinheiten - Ennolarelationen

Obwohl das Hauptanliegen dieser Arbeit die Konstruktion von Basen ist, sei an dieser Stelle noch kurz auf die Relationen in der Gruppe der Kreiseinheiten eingegangen. Im Zusammenhang mit den Kreiseinheiten gibt es zwei offensichtliche Relationstypen, nämlich die *Normrelationen*, die durch Relativerweiterungen entstehen, beispielsweise

$$N_{\mathbf{Q}(\epsilon_{18})\to\mathbf{Q}(\epsilon_6)}(1-\epsilon_{18}) = 1-\epsilon_6, \tag{153}$$

und solche, die durch *komplexe Konjugation* entstehen, wie

$$1-\epsilon_6 = -\epsilon_6\overline{(1-\epsilon_6)} = -\epsilon_6(1-\epsilon_6^{-1}). \tag{154}$$

Erstere spiegelt sich bei den Kreismoduln als Zeilensumme wider, letztere wird als Operation von σ interpretiert. Milnor vermutete noch, daß alle Relationen von diesen offensichtlichen Relationen erzeugt werden. Erst Ennola entdeckte

(siehe [4]), daß eine weitere Relation existiert, die jedoch erst dann auftritt, wenn n von mehr als zwei verschiedenen Primfaktoren geteilt wird.

Die Untersuchung der Kreiseinheiten im Zusammenhang mit $\mathbf{Z}[\sigma]$-Moduln zeigt, daß die von Ennola entdeckte Relation in keiner Weise außergewöhnlich ist, sondern zwangsläufig durch das Zusammenspiel der σ-Operation mit anderen Relationen, nämlich den Normrelationen, entsteht.

Die Gruppe der n-ten relativen Kreiseinheiten $\widehat{C^{(n)}}$ ist nach den Sätzen 3.2.2 und 2.3.5 im Fall, daß n keine Primzahlpotenz ist, isomorph zu $Z(n)_+$, wobei $Z(n)$ der n-te Kreismodul ist. Weiterhin haben wir nach Lemma 1.2.10, daß $Z(n)_+$ isomorph ist zum torsionsfreien Anteil von $Z(n)/(1-\sigma)Z(n)$. Wie beispielsweise im Beweis von Satz 2.3.3 benutzt wurde, entsprechen die Normrelationen den Zeilensummen von $Z(n)$. Die Relationen, die durch komplexe Konjugation entstehen, entsprechen dem Herausfaktorisieren von $(1-\sigma)Z(n)$. Somit erhalten wir die exakte Sequenz

$$0 \to \hat{T} \to Z(n)/(1-\sigma)Z(n) \to \widehat{C^{(n)}} \to 1. \tag{155}$$

Da $\widehat{C^{(n)}} \cong Z(n)_+$ ist, ist $\hat{T}$ die Torsionsgruppe von $Z(n)/(1-\sigma)Z(n)$, und jedes Element von $\hat{T}$ führt zu einer Relation, die nicht direkt von Normrelationen oder komplexer Konjugation erzeugt wird.

Lemma 1.2.10, c, i zeigt auch, wie sich $\hat{T}$ explizit aus dem F^--Teil einer Normalbasis $[F^0, F^+, F^-]$ von $Z(n)$ ergibt. Wir erhalten damit den folgenden Satz.

Satz 3.4.1 *Es sei $n = q_1 \cdots q_r$ und $L^{(n)} = \prod_{d\|n} C^{(d)}$. Die Relationen innerhalb der n-ten relativen Kreiseinheiten $\widehat{C^{(n)}} = C^{(n)}/L^{(n)}$ entstehen durch Relationen vom Typ (153) und (154), das heißt durch Normrelationen und komplexe Konjugation. In den folgenden zwei Fällen kommt genau eine weitere Relation hinzu:*

i) *n ungerade und quadratfrei, $r > 1$ und $2 \nmid r$.*

ii) *$n = 4u$ mit u ungerade und quadratfrei, $r > 1$ und $2 \nmid r$.*

Diese weitere Relation ist explizit gegeben durch

$$\prod_{a \in V_n} (1 - \epsilon_n^a) \in L^{(n)}. \tag{156}$$

Dabei ist $V_n \subseteq G_n$ definiert als gemäß dem Chinesischen Restsatz isomorph zur Menge $V_{q_1} \times \cdots \times V_{q_r}$ mit $V_{q_i} = \{1 \le a < q_i/2;\ (a, q_i) = 1\}$ für $i = 1, \ldots, r$.

Beweis
Interessant sind nur die Fälle, in denen n keine Primzahlpotenz ist. In den Fällen, in denen n Primzahlpotenz ist, rechnet man direkt nach (beispielsweise mit (45)), daß sich alle Erzeuger von einer gegebenen Basis durch Normrelationen und komplexe Konjugationsrelationen darstellen lassen.

Ist n nicht die Potenz einer Primzahl, so ist $\widehat{C^{(n)}}$ isomorph zu $Z(n)_+$, wobei $Z(n)$ der n-te Kreismodul ist. Ist $[F^0, F^+, F^-]$ eine Normalbasis von $Z(n)_+$, so tritt nach der Vorbemerkung zu diesem Satz eine weitere Relation genau dann auf, wenn $F^- \neq \emptyset$ ist.

In Abschnitt 2.1.2 wurden ausführlich Normalbasen von $Z(n)$ konstruiert. Insbesondere ist im Fall, daß n nicht von der Form $n = u$ oder $n = 4u$ mit u ungerade und quadratfrei ist, $m^-(Z(n)) = 0$, das heißt, F^- ist leer.

In den anderen Fällen ist F^- einelementig und explizit in (82) beziehungsweise (83) angegeben. Übersetzt man dies mit der in (146) verwendeten Abbildung auf Kreiszahlen, so entspricht dies genau der Relation (156). Beispielsweise im Fall, daß n ungerade und quadratfrei ist, ist $p_i = q_i$ und $V_{q_i} = \{1, \ldots, \lfloor p_i/2 \rfloor\}$ für alle $i = 1, \ldots, r$, und der Zusammenhang zwischen (82) und (156) ist nach (146) direkt gegeben durch die Abbildung $\eta : G_{p_1} \times \cdots \times G_{p_r} \to G_n$.

QED.

Zum Schluß geben wir an, wie die Situation aussieht, wenn man statt der relativen Kreiseinheiten die Gruppe der Kreiseinheiten $C^{(n)}$ betrachtet. Jede Relation in $C^{(n)}$ ist natürlich auch eine Relation in der Gruppe der Kreiszahlen $D^{(n)}$. Umgekehrt können wir eine Relation u innerhalb von $D^{(n)}$ wie im Beweis von Lemma 3.1.4 schreiben als $u = v \prod_{i=1}^{r} (1 - \epsilon_{q_i})^{b_i}$ mit $v \in C^{(n)}$ und $b_i \in \mathbf{Z}$. Normbildung zeigt $b_i = 0$ für alle $i = 1, \ldots, r$, woraus folgt, daß u auch eine Relation in $C^{(n)}$ ist.

Daher betrachten wir im folgenden die Relationen innerhalb der Gruppe der Kreiszahlen $D^{(n)}$. Hier haben wir im Beweis von Satz 2.3.3 die exakte Sequenz

$$0 \to T \to \mathcal{L}(n)/(1-\sigma)\mathcal{L}(n) \to D^{(n)} \to 1. \tag{157}$$

Da die Torsionsgruppe T von $\mathcal{L}(n)/(1-\sigma)\mathcal{L}(n)$ nach Lemma 1.2.10, c nur 2-Torsion besitzt, bestätigt dies beispielsweise direkt Satz 8.9 in [16], nämlich daß das Quadrat jeder Relation in $D^{(n)}$ von Norm- und Konjugationsrelationen erzeugt wird.

Wie T explizit aussieht, erhält man durch eine Normalbasis $[E^0, E^+, E^-]$ von $\mathcal{L}(n)$, die man durch Anwendung von Algorithmus 1.6.15 auf das Kreissystem $\Gamma(n)$ erhält gemäß dem folgenden Algorithmus und dem daran anschließenden Satz.

Algorithmus 3.4.2 *Der folgende Algorithmus konstruiert Relationen innerhalb der Gruppe der Kreiszahlen, die nicht von den offensichtlichen Relationen gemäß (153) und (154) erzeugt werden.*

1. (Normalbasen der Y_d) *Man berechne zu jedem $1 < d|n$ jeweils eine Normalbasis B_d zu Y_d. Die Y_d sind dabei wie in (104) definiert, nämlich als $\langle G_d \rangle$ falls d Primzahl ist und als Kreismoduln $Z(d)$ sonst.*

   Normalbasen für Kreismoduln werden ausführlich in Abschnitt 2.1.2 behandelt. Normalbasen für $\langle G_d \rangle$ konstruiert man gemäß Abschnitt 1.4.2.

2. (Normalbasis des kombinierten Kreismoduls) *Man konstruiere aus den Normalbasen der Y_d eine Normalbasis $[E^0, E^+, E^-]$ des kombinierten Kreismoduls $\mathcal{L}(n)$ mittels Algorithmus 1.6.15. Insbesondere ist man dabei an E^- interessiert.*

3. (Kreismodul $\rightarrow$ Kreiszahlen) *Der Zusammenhang zwischen $\mathcal{L}(n)$ und $D^{(n)}$ ist gemäß Satz 2.3.3 mit der Abbildung $\mu : [a, d] \mapsto 1 - \epsilon_d^a$ gegeben, durch die die Elemente $[a, d] \in G_d$ für $d|n$ von $\mathcal{L}(n)$ auf Kreiszahlen abgebildet werden.*

   Nach Lemma 1.2.10, c, i erzeugt E^- die Torsionsgruppe T des Moduls $\mathcal{L}(n)/(1-\sigma)\mathcal{L}(n)$. Man bilde also E^- mit μ auf $D^{(n)}$ ab.

Satz 3.4.3 *Zu $n > 2$ sei r die Anzahl der Primteiler von n und*

$$c = \begin{cases} 2^{r-1} - r & \text{falls } n \not\equiv 2 \bmod 4, \\ 2^{r-2} - (r-1) & \text{falls } n \equiv 2 \bmod 4. \end{cases} \tag{158}$$

Dann existieren in $D^{(n)}$ genau 2^c verschiedene Ennolarelationen, die von c verschiedenen Relationen erzeugt werden. Mit anderen Worten, es existiert eine Menge von Ennolarelationen $\{d_1, \ldots, d_c\} \subseteq D^{(n)}$ im freien Erzeugnis der Menge $\{1-\epsilon_d^a;\ d|n,\ a \in G_d\}$, so daß jede Ennolarelation von der Form $\prod_{i=1}^{c} d_i^{\delta_i}$ mit $\delta \in \{0, 1\}$ ist. Die d_i für $i = 1, \ldots, c$ erhält man explizit aus Algorithmus 3.4.2.

Beweis

Der Wert c ergibt sich aus (110) in Lemma 2.2.10, das den Wert $m^-(\mathcal{L}(n))$ und damit die Mächtigkeit von dem in Algorithmus 3.4.2, Schritt 2, konstruierten E^- liefert.

Ennolarelationen sind gegeben als Torsionsanteil von $\mathcal{L}(n)/(1-\sigma)\mathcal{L}(n)$. In Lemma 1.2.10, c, i wird angegeben, wie die Torsionsgruppe explizit aus einer Normalbasis berechnet wird. Beim Übergang vom kombinierten Kreismodul auf die Gruppe der Kreiszahlen übersetzt sich die additive Schreibweise in Lemma 1.2.10 in die multiplikative Darstellung $\prod_{i=1}^{c} d_i^{\delta_i}$.

QED.

Es ist $n = 60$ die kleinste Zahl für die in (158) $c > 0$ ist, also Ennolarelationen bei Kreiszahlen auftreten. Im Anhang geben wir unter anderem auch explizite Beispiele für Ennolarelationen. Weiter sei auf die explizite Berechnung einer Ennolarelation im allgemeinen Stickelbergerideal mit dem zum Algorithmus 3.4.2 analogen Algorithmus 4.4.1 an Hand des Beispiels für $n = 15$ hingewiesen.

4 Stickelbergerelemente

Bei allen im folgenden durchgeführten Betrachtungen sei $n > 2$ eine feste natürliche Zahl, und $G_n := \{1 \leq a < n;\ \gcd(a,n) = 1\}$. Da n fest ist, schreiben wir statt G_n auch G.

Die Stickelbergerelemente $\theta(a)$ sind Elemente im Gruppenring $\mathbf{Q}G$, die Relationen genügen, die den Relationen von Kreiseinheiten ähnlich sind. Auch in der Literatur werden Stickelbergerelemente und Kreiseinheiten oft gemeinsam behandelt, wie beispielsweise in [8], [12] oder [15]. Grob gesagt gilt folgendes. Bezeichnet $\mathcal{L}(n)$ den kombinierten n-ten Kreismodul, dann ist der von den Stickelbergerelementen aufgespannte Modul im wesentlichen isomorph zu $\mathcal{L}(n)_-$, wohingegen die Gruppe der Kreiszahlen isomorph zu $\mathcal{L}(n)_+$ ist. Daher ist die Hauptarbeit, nämlich die Bestimmung der Invarianten m^+, m^-, die Berechnung des Ranges von $\mathcal{L}(n)$ und der Nachweis der Gutartigkeit, bereits im zweiten Kapitel getan.

Nach der Definition der Stickelbergerelemente und dem Nachweis der grundlegenden Relationen zwischen diesen Elementen im ersten Abschnitt rechnen wir im zweiten Abschnitt den Isomorphismus zu $\mathcal{L}(n)_-$ nach. Anschließend zeigen wir im dritten Abschnitt ausführlich, wie wir eine Basis des Stickelbergerideals mit den in dieser Arbeit entwickelten Methoden erhalten. Der vierte Abschnitt beschäftigt sich dann schließlich mit den Ennolarelationen, die hier ähnlich wie bei den Kreiseinheiten auftreten. Abgerundet wird dieser Abschnitt durch die ausführliche Herleitung einer Ennolarelation für das Stickelbergerideal für $n = 15$ und ein Beispiel einer Ennolarelation für $n = 5005$.

4.1 Definition und Eigenschaften

Zu $x \in \mathbf{Q}$ sei im folgenden $y = \langle x \rangle$ definiert als diejenige Zahl im Intervall $[0,1)$ mit $y \equiv x \bmod \mathbf{Z}$.

Sinnot definiert in [15] das Stickelbergerelement wie folgt.

Definition 4.1.1 *Für $\tau \in G$ bezeichne τ^{-1} das Inverse von τ modulo n in G. Dann heißt zu $a \in \mathbf{Z}$ das Element*

$$\theta(a) = \sum_{\tau \in G} \left\langle -\frac{a\tau}{n} \right\rangle \tau^{-1} \tag{159}$$

im Gruppenring $\mathbf{Q}G$ Stickelbergerelement.

Man sieht direkt, daß $\theta(a) = \theta(a')$ ist, wenn $a \equiv a' \bmod n$ ist. Außerdem ist $\theta(0) = 0$. Betrachten wir daher das $\mathbf{Z}$-Erzeugnis der $\theta(a)$, so wird dieses von den $n-1$ Elementen $\theta(1), \ldots, \theta(n-1)$ erzeugt.

Ausgangspunkt der Überlegungen sind die beiden folgenden Relationen, denen das Stickelbergerelement genügt.

Lemma 4.1.2 *Es sei $a \in \{1, \ldots, n-1\}$ und d ein Teiler von n. Dann gelten*

$$\theta(a) + \theta(n-a) = \sum_{\tau \in G} \tau \tag{160}$$

und

$$\sum_{\nu=0}^{d-1} \theta(a + \nu\frac{n}{d}) - \theta(da) = \tfrac{1}{2}(d-1) \sum_{\tau \in G} \tau. \tag{161}$$

Beweis
Es gilt $\langle a/n \rangle = \langle a'/n \rangle$ falls $a \equiv a' \bmod n$ ist. Damit folgt direkt die Relation (160) aus

$$\left\langle -\frac{a\tau}{n} \right\rangle + \left\langle -\frac{n\tau - a\tau}{n} \right\rangle = 1 \tag{162}$$

für $\tau \in G$.
Die Relation (161) erhält man ebenfalls mit elementarer Arithmetik: Es ist zu zeigen, daß für jedes $\tau \in G$ die Gleichung

$$\sum_{\nu=0}^{d-1} \left\langle -(\frac{\tau a}{n} + \frac{\nu\tau}{d}) \right\rangle - \left\langle -\frac{d\tau a}{n} \right\rangle = \tfrac{1}{2}(d-1) \tag{163}$$

gilt. Durchläuft ν die Zahlen $0, \ldots, d-1$, so auch $-\nu\tau \bmod d$. Setzen wir außerdem $b := -\tau a \bmod n$, so ist (163) äquivalent zu

$$\sum_{\mu=0}^{d-1} \left\langle \frac{b}{n} + \frac{\mu}{d} \right\rangle - \left\langle \frac{db}{n} \right\rangle = \tfrac{1}{2}(d-1). \tag{164}$$

Wir können sogar $0 \leq b < n/d$ annehmen, denn sowohl die Summe als auch $\langle db/n \rangle$ bleibt gleich, wenn wir b durch b' ersetzen mit $b \equiv b' \bmod n/d$.
Ist aber (164) mit $0 \leq b < n/d$ zu zeigen, so liegen alle Ausdrücke in den spitzen Klammern sowieso in $[0, 1)$. Die Klammern können daher weggelassen werden, und die Gleichheit in (164) folgt direkt durch Ausrechnen.

QED.

Es sei schon an dieser Stelle bemerkt, wie die Analogie zwischen (160) und (161) zu den Relationen der Kreiseinheiten aussieht. Es entspricht (160) der komplexen Konjugation und (161) den durch Relativnormen implizierten Relationen.

4.2 Stickelbergerelemente und das Kreissystem

Die Stickelbergerelemente liegen in $\mathbf{Q}G$. Im folgenden sind wir an den Relationen interessiert, die zwischen den Stickelbergerelementen existieren. Das heißt, wir suchen eine Basis des $\mathbf{Z}$-Erzeugnisses der $\theta(a)$ in $\mathbf{Q}G$. Dieses Erzeugnis ist ein gebrochenes Ideal in $\mathbf{Q}G$, jedoch nicht identisch mit "dem" Stickelbergerideal. Für den Begriff "Stickelbergerideal" existieren in der Literatur

verschiedene Definitionen (siehe dazu [15]), die in der Regel gewisse Teilmoduln vom Erzeugnis der Stickelbergerelemente bedeuten.

Um Verwechslungen von vorneherein auszuschließen, sprechen wir im folgenden vom allgemeinen Stickelbergerideal:

Definition 4.2.1 *Das* $\mathbf{Z}$*-Erzeugnis* $I := \langle \theta(1), \ldots, \theta(n-1) \rangle$ *der Stickelbergerelemente heiße* allgemeines Stickelbergerideal.

Im weiteren beweisen wir den Zusammenhang zwischen dem n-ten kombinierten Kreismodul und dem allgemeinen Stickelbergerideal. Dazu führen wir noch die folgenden beiden Bezeichnungen ein. Es sei $s(G) := \sum_{\tau \in G} \tau$ und

$$\omega := \begin{cases} s(G) & \text{falls } n \text{ ungerade,} \\ \frac{1}{2}s(G) & \text{falls } n \text{ gerade.} \end{cases} \tag{165}$$

Nach (160) und (161) liegt ω im allgemeinen Stickelbergerideal.

Wir zeigen einen Isomorphismus zwischen $\mathcal{L}(n)_-$ und $I/\langle\omega\rangle$, wobei $\mathcal{L}(n)$ der n-te kombinierte Kreismodul und I das allgemeine Stickelbergerideal ist. Dazu untersuchen wir zunächst $I/\langle\omega\rangle$.

Lemma 4.2.2 *Es sei* I *das allgemeine Stickelbergerideal. Dann gilt*

a) $I/\langle\omega\rangle$ *ist torsionsfrei,*

b) $rg(I/\langle\omega\rangle) = \frac{1}{2}\varphi(n)$.

Beweis

Zu a: Auf G operiere (wie üblich) σ durch Negation modulo n. Man sieht dann direkt aus (160), daß $(1+\sigma)\theta(a) = s(G)$ für $a \in \{1, \ldots, n-1\}$ ist.

Sei nun

$$\sum_{a=1}^{n-1} \alpha_a \theta(a) = \lambda s(G) \tag{166}$$

mit $\lambda \in \mathbf{Q}$ und $\alpha_a \in \mathbf{Z}$. Multiplizieren wir (166) mit $(1+\sigma)$, so folgt $2\lambda \in \mathbf{Z}$, das heißt, in λ taucht höchstens 2 im Nenner auf. Ist nun n gerade, so ist $\omega = \frac{1}{2}s(G)$, und Teil a ist gezeigt. Im Fall, daß n ungerade ist, gilt $\omega = s(G)$. Da auf der linken Seite von (166) nur ungerade Nenner stehen, λ aber höchstens 2 als Nenner hat, muß λ sogar in $\mathbf{Z}$ sein. In beiden Fällen erhalten wir somit $\lambda s(G) = k\omega$ mit $k \in \mathbf{Z}$, und es folgt Teil a.

Zu b: Nach Bemerkung 1.2.11 ist $\operatorname{rg} I = \operatorname{rg}(1-\sigma)I + \operatorname{rg}(1+\sigma)I$. Zur Bestimmung des Rangs von I bestimmen wir jeweils den Rang von $(1+\sigma)I$ und $(1-\sigma)I$.

$\operatorname{rg}(1-\sigma)I$: Sinnot zeigt in [15], daß der Rang von $(1-\sigma)I$ gleich dem Rang von $(1-\sigma)\mathbf{Z}G$ ist. Da $[H, \emptyset, \emptyset]$ mit $H = \{\tau \in G;\ 1 \le \tau < n/2\}$ eine Normalbasis von $\mathbf{Z}G$ und $\operatorname{rg}\mathbf{Z}G = \varphi(n)$ ist, ist $(1-\sigma)H$ eine Basis von $(1-\sigma)\mathbf{Z}G$ und daher $\operatorname{rg}(1-\sigma)\mathbf{Z}G = \frac{1}{2}\varphi(n)$.

rg $(1+\sigma)I$: Wie in Teil a schon festgestellt, ist $(1+\sigma)I \subseteq \langle\omega\rangle$ und nichttrivial, hat also Rang Eins.

Insgesamt erhalten wir $\operatorname{rg} I = \frac{1}{2}\varphi(n)+1$, also $\operatorname{rg}(I/\langle\omega\rangle) = \frac{1}{2}\varphi(n)$.

QED.

Der kombinierte Kreismodul $\mathcal{L}(n)$ ist definiert als die direkte Summe der freien Moduln $\langle G_d\rangle$ mit $d|n$ modulo gewisser Relationen. Wir geben daher den folgende Isomorphismus durch seine Wirkung auf die $a \in G_d$ an, die wir wie üblich mit $[d,a] \in G_d$ bezeichnen.

Satz 4.2.3 *Es sei I das allgemeine Stickelbergerideal und $\mathcal{L}(n)$ der n-te kombinierte Kreismodul. Dann ist*

$$\mathcal{L}(n)_- \cong I/\langle\omega\rangle. \tag{167}$$

Dabei wird $[d,a] \in G_d$ für $d|n$ abgebildet auf $\theta(a\frac{n}{d})$.

Beweis
Der Beweis wird direkt analog zum Beweis von Satz 2.3.3 geführt, in dem der Isomorphismus zwischen $\mathcal{L}(n)_+$ und den n-ten Kreiszahlen gezeigt wurde. Das heißt, wir zeigen analog zu (117) die Exaktheit der Sequenz

$$0 \to T \to \mathcal{L}(n)/(1+\sigma)\mathcal{L}(n) \xrightarrow{\mu} I/\langle\omega\rangle \to 0, \tag{168}$$

wobei T die Torsionsgruppe von $\mathcal{L}(n)/(1+\sigma)\mathcal{L}(n)$ ist und μ die in Satz 4.2.3 angegebene Abbildung, die $[d,a]$ auf $\theta(a\frac{n}{d})$ abbildet. Ist die Exaktheit von (168) gezeigt, dann folgt auch die Behauptung des Satzes, denn $\mathcal{L}(n)_-$ ist nach Lemma 1.2.10, c, ii gleich $\mathcal{L}(n)/(1+\sigma)\mathcal{L}(n)$ modulo Torsion.
Es ist $\mathcal{L}(n)$ definiert als Kombinat des $M\mathfrak{En}$-Systems $\Gamma(n) = (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d|n}$ mit $M_d = \langle G_d\rangle$. Dabei ist $\mathcal{L}(n)$ explizit gegeben gemäß $\mathcal{L}(n) = N/Q$ mit $N = \bigoplus_{d|n} M_d$ und $Q = \sum_{d|n}\langle r + \mathfrak{n}_d(r);\ r \in \mathcal{E}_d\rangle$.
Wir zeigen zunächst die Wohldefiniertheit der Abbildung μ. Dabei benutzen wir $\mathcal{L}(n)/(1+\sigma)\mathcal{L}(n) \cong N/((1+\sigma)N+Q)$, wobei N das freie Erzeugnis der disjunkten Vereinigung der Mengen G_d ist. Da μ auf diesen G_d erklärt wurde, ist μ auf N eindeutig homomorph fortsetzbar, und es ist zu zeigen, daß die Bilder von $(1+\sigma)N$ und Q unter μ in $\langle\omega\rangle$ liegen.

- Für $(1+\sigma)N$ folgt dies durch

$$\theta(a\frac{n}{d}) + \theta((d-a)\frac{n}{d}) = \theta(a\frac{n}{d}) + \theta(n - a\frac{n}{d}) \in \langle\omega\rangle \tag{169}$$

nach (160).

- Den Erzeugern von Q entsprechen die Relationen aus (161). Um dies zu zeigen definieren wir zu $d \in \mathbf{N}$, $p|d$ prim und $b \in G_{d/p}$ wie in (98) die Menge $Y := \{x \in G_d;\ x \equiv b \bmod d/p\}$. Nach Lemma 2.2.7 ist

$$X := \{b + \nu\frac{d}{p};\ \nu = 0, \ldots, p-1\} = \begin{cases} Y & \text{falls } p^2|d \\ Y \cup \{pb'\} & \text{falls } p^2 \not| d \end{cases} \tag{170}$$

  mit $b' \in G_{d/p}$ so, daß $pb' \equiv b \bmod d/p$ gilt.

  Es wird Q von Elementen der Form $s(d,p,b) + \mathtt{n}_d(s(d,p,b))$ erzeugt, wobei $s(d,p,b)$ eine Zeilensumme gemäß (86) ist. Die $\mathtt{n}_d$ sind in (92), Definition 2.2.1, definiert. Explizit erhalten wir:

$$s(d,p,b) \overset{\mu}{\mapsto} \sum_{x \in Y} \theta(x\frac{n}{d}) \tag{171}$$

  und

$$\mathtt{n}_d(s(d,p,b)) \overset{\mu}{\mapsto} \begin{cases} -\theta(b\frac{pn}{d}) & \text{falls } p^2|d, \\ \theta(b'\frac{pn}{d}) - \theta(b\frac{pn}{d}) & \text{falls } p^2 \not| d. \end{cases} \tag{172}$$

  Mit (170) folgt, indem wir Relation (161) ausnutzen, nach Lemma 2.2.7

$$\begin{aligned} s(d,p,b) + \mathtt{n}_d(s(d,p,b)) &\overset{\mu}{\mapsto} \sum_{\nu=0}^{p-1} \theta(\frac{n}{d}\left(b + \nu\frac{d}{p}\right)) - \theta(b\frac{pn}{d}) \\ &= \sum_{\nu=0}^{p-1} \theta(\frac{n}{d}b + \nu\frac{n}{p}) - \theta(p\frac{n}{d}b) \qquad \in \langle\omega\rangle. \end{aligned} \tag{173}$$

Wir haben bisher gezeigt, daß μ in der Sequenz (168) wohldefiniert ist. Weiter ist μ als Abbildung von N nach $I/\langle\omega\rangle$ auch surjektiv, da ein Urbild von $\theta(a)$ gegeben ist durch $[n/t, a/t] \in G_{n/t}$ mit $t = \gcd(a,n)$.

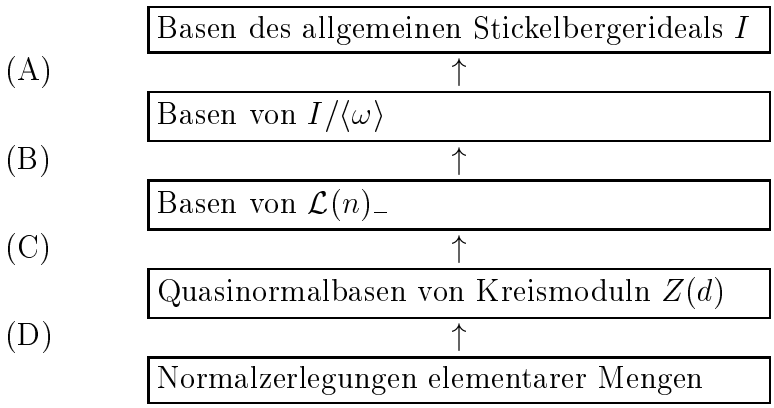
Nach Lemma 2.2.11 ist der Rang von $\mathcal{L}(n)_-$ gleich $\frac{1}{2}\varphi(n)$, und somit gemäß Lemma 4.2.2, b gleich dem Rang von $I/\langle\omega\rangle$.

Daraus folgt, daß der Kern von μ als auf $\mathcal{L}(n)/(1+\sigma)\mathcal{L}(n)$ definierte Abbildung von der Torsionsgruppe T von $\mathcal{L}(n)/(1+\sigma)\mathcal{L}(n)$ gebildet wird. Dies beweist die Exaktheit von (168) und damit den Satz.

QED.

4.3 Eine Basis des allgemeinen Stickelbergerideals

Durch den Isomorphismus $\mathcal{L}(n)_- \cong I/\langle\omega\rangle$ ergibt sich also insbesondere auch eine Basis von $I/\langle\omega\rangle$ durch eine Basis von $\mathcal{L}(n)_-$. Wir zeigen nun im einzelnen, wie dieser Konstruktionsweg abläuft. Wir fassen zunächst schematisch die verschiedenen Schritte zusammen, und erläutern diese anschließend im einzelnen.



zu (A): Dieser Schritt ist sehr einfach und hier nur der Vollständigkeit wegen aufgeführt. Eine (in I lebende) Basis von $I/\langle\omega\rangle$ ergibt durch Hinzufügen von ω nach Bemerkung 1.1.2 eine Basis von I.

zu (B): Nach Definition 2.2.1 und 2.2.4 ist $\mathcal{L}(n)$ definiert als direkte Summe von Moduln $M_d := \langle G_d\rangle$ mit $d|n$. Es sei $V := \{[d,a];\ d|n,\ a \in G_d\}$ die disjunkte Vereinigung aller G_d. Wie wir in (C) sehen werden, ist eine Basis von $\mathcal{L}(n)_-$ als Teilmenge von $W \subseteq V$ gegeben. Nach Satz 4.2.3 ist dann

$$\{\theta(a\frac{n}{d});\ [d,a] \in W\} \tag{174}$$

eine Basis von $I/\langle\omega\rangle$.

zu (C): Nach Satz 2.2.14 ergibt sich eine Basis von $\mathcal{L}(n)_-$ im Fall $4 \not| n$ durch einfache Vereinigung von in $M_d = \langle G_d\rangle$ lebenden Basen gewisser Moduln $(Y_d)_-$ mit $d|n$. Im Fall $4|n$ durchläuft d alle Teiler von n, außer 2 und 4. Zusätzlich muß im Fall $4|n$ gemäß der Diskussion im Anschluß an Satz 2.2.14 noch $[4,1]$ zur Basis hinzugenommen werden.

Die Y_d sind gemäß Definition 2.2.1 definiert durch

$$Y_d = \begin{cases} 0 & \text{falls } d = 1, \\ \langle G_d\rangle & \text{falls } d \text{ Primzahl}, \\ Z(d) & \text{sonst}, \end{cases} \tag{175}$$

wobei $Z(d)$ der d-te Kreismodul ist.

Im Fall $d = 1$ ist nichts zu sagen, da Y_1 der Nullmodul und somit die Basis leer ist. Wir unterscheiden nun die beiden anderen Fälle.

$d = p$ Primzahl: Dieser Fall läßt sich direkt nachrechnen: Ist $p = 2$ so ist $Y_2 = \langle G_2\rangle$ und daher $(Y_2)_- = 0$. Die Basis von $(Y_2)_-$ ist somit leer. Ansonsten ist beispielsweise $[W_p, \emptyset, \emptyset]$ mit

$$W_p := \{[p,a];\ 1 \le a < \tfrac{1}{2}p\} \tag{176}$$

eine Normalbasis von Y_p, und somit ist nach Lemma 1.2.10 W_p eine Basis von $(Y_p)_-$.

$d > 1$ und keine Primzahl: In diesem Fall ist $Y_d = Z(d)$. Hier sei auf den Fall "d keine Potenz einer Primzahl" von Schritt (B) in der Konstruktion einer Basis der Kreiseinheiten in Abschnitt 3.3 verwiesen. Wir rekapitulieren an dieser Stelle nur, daß eine Quasinormalbasis von $Z(d)$ als Teilmenge von

$$S := \Lambda_{q_1} \times A_{p_1} \times \cdots \times \Lambda_{q_t} \times A_{p_t} \times G_{p_{t+1}} \times \cdots \times G_{p_r} \tag{177}$$

mit $\Lambda_{q_i} := G_{q_i/p_i}$ und $A_{p_i} = \{0, \ldots, p_i - 1\}$ gegeben ist, und sich die Abbildung $\zeta : S \to G_d$ gemäß

$$\begin{array}{ccccccccc} \underbrace{\Lambda_{q_1} \times A_{p_1}} & \times \cdots \times & \underbrace{\Lambda_{q_t} \times A_{p_t}} & \times & G_{p_{t+1}} & \times \cdots \times & G_{p_r} & & \\ \downarrow \xi_1 & & \downarrow \xi_t & & \downarrow \mathrm{id} & & \downarrow \mathrm{id} & & \\ G_{q_1} & \times \cdots \times & G_{q_t} & \times & G_{q_{t+1}} & \times \cdots \times & G_{q_r} & & \\ & & & \downarrow \eta & & & & & \\ & & & G_d & & & & & \end{array} \tag{178}$$

ergibt, wobei die Abbildungen ξ_i für $i = 1, \ldots, t$ explizit gegeben sind durch $\xi_i(\lambda, a) = a p_i^{\alpha_i - 1} + \lambda$, und η durch den Chinesischen Restsatz wohldefiniert ist.

Ist nun $[G^0, G^+, G^-]$ eine Quasinormalbasis von $Z(d)$ gemäß Abschnitt 2.1.2, dann ist nach Lemma 1.2.10, a $G^0 \cup G^-$ eine Basis von $Z(d)_-$. Für $d \neq 4$ definieren wir daher in Analogie zu (147)

$$W_d := \{[d, a];\ a \in \zeta(G^0 \cup G^-)\}. \tag{179}$$

Definieren wir noch $W_4 := \{[4, 1]\}$ so erhalten wir in Schritt (C) nach Satz 2.2.14 eine Basis W von $\mathcal{L}(n)_-$ durch

$$W := \bigcup_{d|n} W_d \tag{180}$$

mit W_d wie in (176) und (179) und $W_1 = \emptyset$.

zu (D): Dies ist der gleiche Schritt wie Schritt (C) in Abschnitt 3.3, und wie dort sei hier ebenfalls auf Abschnitt 2.1.2 verwiesen.

Wir erläutern diese Konstruktion an einem Beispiel.

Beispiel

Es sei $n = 45$. Wir erhalten eine Basis von I über eine Basis von $\mathcal{L}(45)_-$, die wir durch Vereinigung von Basen $W_d \subseteq G_d$ der $(Y_d)_-$ mit $d|45$ erhalten. Wir bestimmen zunächst die W_d:

$d = 3$: Wir lesen die Basis direkt aus (176) ab und erhalten

$$W_3 = \{[3, 1]\} \tag{181}$$

als Basis von $\langle G_3 \rangle_-$.

$\underline{d = 5:}$ Hier ist nach (176)

$$W_5 = \{[5,1],[5,2]\} \tag{182}$$

eine Basis von $\langle G_5 \rangle_-$.

$\underline{d = 9:}$ Eine Quasinormalbasis von $(Y_9)_-$ erhalten wir aus dem Fall "sonstige" in Abschnitt 2.1.2. Nach (84) ist $[G^0, \emptyset, \emptyset]$ mit $G^0 = H_9 \times A_3^\flat$ eine Quasinormalbasis von $Z(9) = Y_9$. Dabei ist $H_9 = \{1\}$ und $A_3^\flat = \{1,2\}$, was unter Verwendung der Abbildungen aus (178) explizit (in Analogie zu (149))

$$W_9 = \{[9,4],[9,7]\} \tag{183}$$

als Basis von $Z(9)_-$ ergibt.

$\underline{d = 15:}$ Eine Quasinormalbasis $[G^0, G^+, G^-]$ von $Z(15)$ entnehmen wir dem Fall "quadratfrei und ungerade" aus Abschnitt 2.1.2. Wir erhalten insbesondere $G^0 = \{(1,2)\}$, $G^- = \emptyset$ und das hier nicht interessierende $G^+ = \{(1,1)\}$. Mit (178) ist daher nach Lemma 1.2.10

$$W_{15} = \{[15,7]\} \tag{184}$$

eine Basis von $Z(15)_-$.

$\underline{d = 45:}$ Wie für $d = 9$ entnehmen wir G^0 und G^- dem Fall "sonstige" in Abschnitt 2.1.2, und erhalten $G^- = \emptyset$ und $G^0 = H_9 \times A_3^\flat \times G_5^\flat$, mit $H_9 = \{1\}$, $A_3^\flat = \{1,2\}$ und $G_5^\flat = \{2,3,4\}$. Es ist also

$$G^0 = \{(1,1,2),(1,1,3),(1,1,4),(1,2,2),(1,2,3),(1,2,4)\}, \tag{185}$$

und unter Verwendung von (178) ist

$$W_{45} = \{[45,22],[45,13],[45,4],[45,7],[45,43],[45,34]\} \tag{186}$$

eine Basis von $Z(45)_-$.

Die Vereinigung von (181), (182), (183), (184) und (186) ergibt

$$\begin{aligned} W \;=\; & \{[45,22],[45,13],[45,4],[45,7],[45,43],[45,34],[15,7], \\ & [9,4],[9,7],[5,1],[5,2],[3,1]\} \end{aligned} \tag{187}$$

als Basis von $\mathcal{L}(n)_-$. Die Basis von I erhalten wir schließlich durch die Abbildung $[d,a] \mapsto \theta(an/d)$ und Hinzunahme von ω aus (165). Also ist

$$\{\omega, \theta(22), \theta(13), \theta(4), \theta(7), \theta(43), \theta(34), \theta(21), \theta(20), \theta(35), \theta(9), \theta(18), \theta(15)\} \tag{188}$$

eine Basis des allgemeinen Stickelbergerideals I für $n = 45$.

4.4 Ennolarelationen für Stickelbergerelemente

Die Frage, ob alle Relationen, die zwischen den Stickelbergerelementen bestehen, vom Typ (160) und (161) sind, läßt sich nun analog zu der entsprechenden Frage für Kreiseinheiten in Abschnitt 3.4 beantworten.

Es sei $\mathcal{L}(n)$ der n-te kombinierte Zeilenfaktormodul. In Satz 4.2.3 erhielten wir einen Isomorphismus zwischen $\mathcal{L}(n)_-$ und $I/\langle\omega\rangle$. Genauer wurde die Exaktheit der Sequenz

$$0 \to T \to \mathcal{L}(n)/(1+\sigma)\mathcal{L}(n) \to I/\langle\omega\rangle \to 0 \tag{189}$$

bewiesen, wobei T die Torsionsgruppe von $\mathcal{L}(n)/(1+\sigma)\mathcal{L}(n)$ ist. Wie im Beweis zu Satz 4.2.3 ausgeführt, werden die Relationen (160) und (161) erfaßt als die "Normrelationen" und "komplexe Konjugationsrelationen" des Moduls $\mathcal{L}(n)/(1+\sigma)\mathcal{L}(n)$.

Relationen innerhalb von $I/\langle\omega\rangle$, die nicht durch (160) und (161) entstehen, werden durch die Torsionsgruppe T gegeben. Wir nennen diese Relationen in Analogie zur Situation bei den Kreiseinheiten *Ennolarelationen*.

Mit einer Normalbasis von $\mathcal{L}(n)$ lassen sich wie in Algorithmus 3.4.2 und Satz 3.4.3 für Kreiszahlen die Torsionsgruppe T und damit die Ennolarelationen gemäß Lemma 1.2.10 bestimmen. Wir beschreiben diese Konstruktion zunächst als Algorithmus und interpretieren das Ergebnis im darauffolgenden Satz.

Algorithmus 4.4.1 *Der folgende Algorithmus konstruiert Relationen innerhalb des allgemeinen Stickelbergerideals I, die nicht von Relationen gemäß (160) und (161) erzeugt werden.*

1. (Normalbasen der Y_d) *Man berechne zu jedem $1 < d|n$ jeweils eine Normalbasis B_d zu Y_d. Die Y_d sind dabei wie in (175) definiert, nämlich als $\langle G_d\rangle$ falls d Primzahl ist und als Kreismoduln $Z(d)$ sonst.*

   Normalbasen für Kreismoduln wurden ausführlich in Abschnitt 2.1.2 behandelt. Normalbasen für $\langle G_d\rangle$ konstruiert man gemäß Abschnitt 1.4.2.

2. (Normalbasis des kombinierten Kreismoduls) *Man konstruiere aus den Normalbasen der Y_d eine Normalbasis $[E^0, E^+, E^-]$ des kombinierten Kreismoduls $\mathcal{L}(n)$ mittels Algorithmus 1.6.15.*

3. (Kreismodul $\to$ Stickelbergerideal) *Der Zusammenhang zwischen $\mathcal{L}(n)$ und I ist gemäß Satz 4.2.3 durch die Abbildung $\mu : [a,d] \mapsto \theta(an/d)$ gegeben, die die Elemente $[a,d] \in G_d$ für $d|n$ von $\mathcal{L}(n)$ auf die Stickelbergerelemente abbildet.*

   Nach Lemma 1.2.10, c, ii erzeugt E^+ die Torsionsgruppe T des Moduls $\mathcal{L}(n)/(1+\sigma)\mathcal{L}(n)$ (siehe dazu auch den folgenden Satz 4.4.2). Man bilde also mit μ die Elemente aus E^+ auf I ab.

4. (Berechnung des ω-Anteils) *Das Bild von E^+ unter μ aus Schritt 3 ist eine Linearkombination der $\theta(i)$ für $i = 1, \ldots, n-1$, die nach (168) in $I/\langle\omega\rangle$ verschwindet, also zu einer Relation*

$$\sum_{i=1}^{n-1} \alpha_i \theta(i) \in \langle\omega\rangle \tag{190}$$

mit $\alpha_i \in \mathbf{Z}$ führt. Die $\theta(i)$ sind explizit in (159) definiert. Man rechne die linke Seite aus und bestimme damit $\lambda \in \mathbf{Z}$ so, daß

$$\sum_{i=1}^{n} \alpha_i \theta(i) + \lambda\omega = 0 \tag{191}$$

gilt.

Satz 4.4.2 *Zu $n > 2$ sei r die Anzahl der Primteiler von n und*

$$c := \begin{cases} 2^{r-1} - 1 & \text{falls } n \not\equiv 2 \bmod 4, \\ 2^{r-2} & \text{falls } n \equiv 2 \bmod 4. \end{cases} \tag{192}$$

Dann existieren in I genau 2^c verschiedene Ennolarelationen, die von c verschiedenen Relationen erzeugt werden. Mit anderen Worten, es existiert eine Menge von Ennolarelationen $\{d_1, \ldots, d_c\}$ im freien $\mathbf{Z}$-Erzeugnis der Menge $\{\theta(i);\ 1 \le i < n\} \cup \{\omega\}$, so daß jede Ennolarelation von der Form

$$\sum_{i=1}^{c} \delta_i d_i \tag{193}$$

mit $\delta \in \{0, 1\}$ ist. Die d_i für $i = 1, \ldots, c$ erhält man explizit aus Algorithmus 4.4.1.

<u>*Beweis*</u>
Der Wert c ergibt sich aus Lemma 2.2.10, das den Wert $m^+(\mathcal{L}(n))$ und damit die Mächtigkeit von dem in Algorithmus 4.4.1, Schritt 2, konstruierten E^+ liefert.

Ennolarelationen sind gegeben als Torsionsanteil von $\mathcal{L}(n)/(1+\sigma)\mathcal{L}(n)$. In Lemma 1.2.10, c, ii wird angegeben, wie die Torsionsgruppe explizit aus einer Normalbasis berechnet wird, woraus insbesondere (193) folgt.

QED.

Im folgenden erläutern wir Algorithmus 4.4.1 durch ein Beispiel, in dem wir eine Ennolarelation für $n = 15$ berechnen. Anschließend geben wir eine Ennolarelation für $n = 5005$ an.

<u>*Beispiele*</u>
Es sei $n = 15$. Da nach Lemma 2.2.10 $m^+(\mathcal{L}(15)) = 1$ ist, existiert genau eine Ennolarelation, die wir im folgenden konstruieren werden. Dazu benötigen wir zunächst Normalbasen der Y_d für $d = 3, 5, 15$:

d = 3,5 Es ist $Y_d = \langle G_d \rangle$. Normalbasen $B_d = [E_d^0, \emptyset, \emptyset]$ von Y_d sind (wie in (181) und (182)) gegeben durch

$$E_3^0 := \{[3,1]\} \qquad \text{und} \qquad E_5^0 := \{[5,1],[5,2]\}. \tag{194}$$

d = 15 Es ist $Z(15) = Z(3) \otimes Z(5)$, und wir erhalten nach Satz 1.3.4. eine Normalbasis von $Z(15)$ aus Normalbasen von $Z(3)$ und $Z(5)$. Die beiden letzteren konstruieren wir gemäß Lemma 1.4.6. Insgesamt ist mit

$$\begin{array}{lll} F_3^0 = \emptyset, & F_3^+ = \emptyset, & F_3^- = \{[3,1]\}, \\ F_5^0 = \{[5,2]\}, & F_5^+ = \emptyset, & F_5^- = \{[5,1]+[5,2]\}, \\ F_{15}^0 = \{([3,1],[5,2])\}, & F_{15}^+ = \{([3,1],[5,1])+([3,1],[5,2])\} & \end{array} \tag{195}$$

und $F_{15}^- = \emptyset$ jeweils eine Normalbasis $[F_d^0, F_d^+, F_d^-]$ von $Z(d)$ für $d = 3, 5, 15$ definiert.

Fassen wir $Z(15)$ gemäß Satz 2.1.3 als Erzeugnis von G_{15} auf, das heißt, wenden wir ζ aus (178), homomorph fortgesetzt auf $\langle G_3 \times G_5 \rangle$, auf F_{15}^+ an, so ist $\zeta(F_{15}^+) = \{[15,1]+[15,7]\}$.

Algorithmus 1.6.15 liefert nun eine Normalbasis von $\mathcal{L}(15)$. Dies geschieht dadurch, daß wir das $M\mathfrak{En}$-System $\Gamma(15) := (M_d, \mathcal{E}_d, \mathfrak{n}_d)_{d|15}$ gemäß Definition 2.2.1 betrachten. Konkret ist nach dieser Definition in $\Gamma(15)$ jeweils $M_d = \langle G_d \rangle$ für $d|15$. Desweiteren ist $\mathcal{E}_1 = \mathcal{E}_3 = \mathcal{E}_5 = \emptyset$, und $\mathcal{E}_{15}$ und die Wirkung von $\mathfrak{n}_{15}$ auf $\mathcal{E}_{15}$ ist gemäß der folgenden Tabelle gegeben:

$\mathcal{E}_{15}$		$\mathfrak{n}_{15}(s(\cdots))$
$s(15,5,1) =$	$[15,1]+[15,4]+[15,7]+[15,13]$	$[3,2]-[3,1]$
$s(15,5,2) =$	$[15,2]+[15,8]+[15,11]+[15,14]$	$[3,1]-[3,2]$
$s(15,3,1) =$	$[15,1]+[15,11]$	$[5,2]-[5,1]$
$s(15,3,2) =$	$[15,2]+[15,7]$	$[5,4]-[5,2]$
$s(15,3,3) =$	$[15,13]+[15,8]$	$[5,1]-[5,3]$
$s(15,3,4) =$	$[15,4]+[15,14]$	$[5,3]-[5,4]$

(196)

Mit den Normalbasen der $Y_d = M_d/\langle \mathcal{E}_d \rangle$ aus (195) als Eingabe konstruieren wir, indem wir Algorithmus 1.6.15 auf $\Gamma(15)$ anwenden, eine Normalbasis $[G^0, G^+, G^-]$ von $\mathcal{L}(15)$, und erhalten dabei insbesondere (G^0 und G^- interessieren hier nicht weiter)

$$G^+ := \{[15,1]+[15,7]-[5,1]-[3,1]\}. \tag{197}$$

Die Abbildung $[d,a] \mapsto \theta(an/d)$ liefert

$$\theta(1)+\theta(7)-\theta(3)-\theta(5) = \lambda\omega \tag{198}$$

für ein $\lambda \in \mathbf{Z}$. Durch direktes Einsetzen der Definition von $\theta(\cdot)$ gemäß (159) in die linke Seite von (198) rechnen wir $\lambda = 0$ aus und erhalten

$$\theta(1)+\theta(7)-\theta(3)-\theta(5) = 0 \tag{199}$$

als Ennolarelation.

Diese Konstruktion läßt sich mit SIMATH [14] implementieren, und wir erhalten für $n = 5005 = 5 \cdot 7 \cdot 11 \cdot 13$ die Relation

$$\theta(1)+\theta(2)+\theta(16)+\theta(57)+\theta(71)+\theta(92)+\theta(122)+\theta(136)+\theta(157)+\theta(211)+\theta(212)+\theta(276)+\theta(302)+\theta(331)+\theta(366)+\theta(367)+\theta(421)+\theta(422)+\theta(456)+\theta(486)+\theta(521)+\theta(562)+\theta(576)+\theta(577)+\theta(617)+\theta(652)+\theta(716)+\theta(717)+\theta(731)+\theta(771)+\theta(772)+\theta(786)+\theta(807)+\theta(862)+\theta(926)+\theta(927)+\theta(981)+\theta(1002)+\theta(1016)+\theta(1017)+\theta(1046)+\theta(1072)+\theta(1081)+\theta(1136)+\theta(1137)+\theta(1171)+\theta(1212)+\theta(1226)+\theta(1277)+\theta(1291)+\theta(1332)+\theta(1366)+\theta(1367)+\theta(1422)+\theta(1431)+\theta(1457)+\theta(1486)+\theta(1487)+\theta(1501)+\theta(1522)+\theta(1576)+\theta(1577)+\theta(1641)+\theta(1696)+\theta(1717)+\theta(1731)+\theta(1732)+\theta(1772)+\theta(1786)+\theta(1787)+\theta(1851)+\theta(1886)+\theta(1926)+\theta(1927)+\theta(1941)+\theta(1982)+\theta(2017)+\theta(2047)+\theta(2081)+\theta(2082)+\theta(2136)+\theta(2137)+\theta(2172)+\theta(2201)+\theta(2227)+\theta(2291)+\theta(2292)+\theta(2346)+\theta(2367)+\theta(2381)+\theta(2411)+\theta(2432)+\theta(2446)+\theta(2487)+\theta(2501)+\theta(2502)+\theta(2577)+\theta(2641)+\theta(2642)+\theta(2656)+\theta(2696)+\theta(2697)+\theta(2731)+\theta(2732)+\theta(2787)+\theta(2796)+\theta(2851)+\theta(2852)+\theta(2887)+\theta(2927)+\theta(2941)+\theta(2942)+\theta(3006)+\theta(3061)+\theta(3082)+\theta(3096)+\theta(3137)+\theta(3151)+\theta(3202)+\theta(3216)+\theta(3291)+\theta(3292)+\theta(3347)+\theta(3356)+\theta(3382)+\theta(3411)+\theta(3412)+\theta(3446)+\theta(3447)+\theta(3501)+\theta(3502)+\theta(3566)+\theta(3642)+\theta(3656)+\theta(3657)+\theta(3697)+\theta(3711)+\theta(3732)+\theta(3776)+\theta(3797)+\theta(3811)+\theta(3851)+\theta(3852)+\theta(3866)+\theta(3942)+\theta(4006)+\theta(4007)+\theta(4061)+\theta(4062)+\theta(4096)+\theta(4097)+\theta(4126)+\theta(4152)+\theta(4161)+\theta(4216)+\theta(4217)+\theta(4292)+\theta(4306)+\theta(4357)+\theta(4371)+\theta(4412)+\theta(4426)+\theta(4447)+\theta(4502)+\theta(4566)+\theta(4567)+\theta(4581)+\theta(4621)+\theta(4656)+\theta(4657)+\theta(4712)+\theta(4721)+\theta(4776)+\theta(4777)+\theta(4811)+\theta(4812)+\theta(4852)+\theta(4866)+\theta(4867)+\theta(4931)-\theta(5)+\theta(45)+\theta(120)+\theta(185)-\theta(355)+\theta(365)+\theta(430)+\theta(500)+\theta(575)+\theta(640)+\theta(885)+\theta(890)+\theta(925)+\theta(955)+\theta(1135)+\theta(1200)+\theta(1275)+\theta(1340)+\theta(1345)+\theta(1410)-\theta(1510)+\theta(1550)+\theta(1615)+\theta(1695)-\theta(1720)+\theta(1730)+\theta(1795)+\theta(1940)+\theta(2005)-\theta(2280)+\theta(2290)+\theta(2320)+\theta(2355)+\theta(2385)+\theta(2565)+\theta(2705)+\theta(2710)+\theta(2770)+\theta(2775)+\theta(2850)-\theta(2875)+\theta(2980)+\theta(3060)-\theta(3085)+\theta(3095)+\theta(3125)+\theta(3160)+\theta(3305)+\theta(3370)+\theta(3620)-\theta(3645)+\theta(3720)+\theta(3750)+\theta(3760)+\theta(4005)+\theta(4075)+\theta(4135)+\theta(4140)+\theta(4215)-\theta(4240)+\theta(4280)+\theta(4460)+\theta(4490)+\theta(4525)+\theta(4530)+\theta(4735)+\theta(4775)+\theta(4915)+\theta(4985)-\theta(14)-\theta(112)-\theta(189)-\theta(259)-\theta(294)-\theta(322)-\theta(392)-\theta(399)-\theta(469)-\theta(497)-\theta(504)-\theta(574)-\theta(644)-\theta(714)-\theta(854)-\theta(882)-\theta(952)-\theta(959)-\theta(1029)-\theta(1064)-\theta(1099)-\theta(1169)-\theta(1407)-\theta(1414)-\theta(1477)-\theta(1484)-\theta(1554)-\theta(1624)-\theta(1652)-\theta(1659)-\theta(1862)-\theta(1869)-\theta(1939)-\theta(2009)-\theta(2037)-\theta(2107)-\theta(2114)-\theta(2219)-\theta(2247)-\theta(2317)-\theta(2324)-\theta(2394)-\theta(2429)-\theta(2499)-\theta(2562)-\theta(2569)-\theta(2779)-\theta(2807)-\theta(2884)-\theta(2954)-\theta(2989)-\theta(3017)-\theta(3024)-\theta(3192)-\theta(3339)-\theta(3374)-\theta(3402)-\theta(3409)-\theta(3472)-\theta(3479)-\theta(3577)-\theta(3584)-\theta(3654)-\theta(3794)-\theta(3864)-\theta(3934)-\theta(3962)-\theta(4032)-\theta(4039)-\theta(4109)-\theta(4144)-\theta(4172)-\theta(4249)-\theta(4319)-\theta(4354)-\theta(4487)-\theta(4494)-\theta(4557)-\theta(4564)-\theta(4704)-\theta(4739)-\theta(4809)-\theta(4942)-\theta(4949)-\theta(22)-\theta(176)-\theta(187)-\theta(341)-\theta(627)-\theta(781)-\theta(792)-\theta(946)-\theta(1177)-\theta(1331)-\theta(1342)-\theta(1496)-\theta(1782)-\theta(1947)-\theta(2101)-\theta(2332)-\theta(2486)-\theta(2497)-\theta(2871)-$$

$$\theta(3102)-\theta(3476)-\theta(3487)-\theta(3641)-\theta(3872)-\theta(4026)-\theta(4191)-\theta(4477)-\theta(4631)-\theta(4642)-\theta(4796)-\theta(26)-\theta(208)-\theta(221)-\theta(468)-\theta(481)-\theta(676)-\theta(741)-\theta(923)-\theta(936)-\theta(1196)-\theta(1391)-\theta(1586)-\theta(1651)-\theta(1768)-\theta(2041)-\theta(2106)-\theta(2301)-\theta(2483)-\theta(2496)-\theta(2756)-\theta(2951)-\theta(3016)-\theta(3198)-\theta(3211)-\theta(3471)-\theta(3666)-\theta(3926)-\theta(4043)-\theta(4316)-\theta(4381)-\theta(4498)-\theta(4758)-\theta(4771)-\theta(105)+\theta(490)+\theta(840)+\theta(945)+\theta(1225)+\theta(1260)+2\theta(1610)+\theta(1645)+\theta(1715)-\theta(1960)+\theta(2065)+\theta(2100)-\theta(2450)+\theta(2765)-\theta(2835)+2\theta(3535)+\theta(3570)+\theta(3920)+\theta(3990)+\theta(4025)-\theta(4270)+\theta(4340)+\theta(4410)-\theta(4655)+\theta(4690)-\theta(4725)+\theta(4795)-\theta(110)-\theta(495)-\theta(825)-\theta(1265)-\theta(2420)-\theta(3190)-\theta(3630)+\theta(3905)-\theta(4345)-\theta(4400)-\theta(4785)-\theta(130)-\theta(1495)-\theta(1560)+\theta(2340)-\theta(2925)-\theta(3705)+\theta(4615)+2\theta(462)+\theta(1309)+\theta(2387)+\theta(2464)+\theta(3157)+2\theta(4312)+\theta(4389)+\theta(182)+\theta(637)+\theta(1092)+\theta(1456)+\theta(1547)+\theta(2457)+\theta(3276)+\theta(3367)+\theta(3822)+\theta(4277)+\theta(286)+\theta(2288)+\theta(2431)+\theta(3146)+\theta(385)+\theta(770)+2\theta(1155)-3\theta(1540)+\theta(2310)+\theta(455)-\theta(1365)-\theta(2275)+\theta(1430)+56\omega=0$$

als Ennolarelation.

Das zur Berechnung dieser Relation benutzte Programm ist im wesentlichen eine modifizierte Form des im Anhang beschriebenen Programms für Kreiseinheiten. Wir skizzieren im folgenden, wie sich zumindest für ungerades quadratfreies n verifizieren läßt, daß diese Relation in der Tat nicht aus Relationen aus (160) und (161) gebildet wird. Es sei darauf hingewiesen, daß sich dieser Test mit etwas mehr Aufwand auch auf allgemeines n anwenden läßt.

- Es sei $\mathcal{J}$ das freie Erzeugnis von ω und der Elemente $\theta(i)$ für $i=1,\dots,n$. Weiter sei

$$E := \{a \in \{1,\dots,n-1\};\ [a \bmod p] \in \{1, p-1\} \text{ für alle } p|n \text{ prim}\}. \tag{200}$$

  Auf $\mathcal{J}$ definieren wir den gewichteten Augmentationshomomorphismus modulo 2 gemäß

$$\begin{array}{rccl} \widetilde{\mathrm{aug}}: & \mathcal{J} & \to & \mathbf{Z}/2\mathbf{Z} \\ & \sum_{i=1}^{n-1}\alpha_i\theta(i)+\lambda\omega & \mapsto & \left(\sum_{j\in E}\alpha_j\right) \bmod 2. \end{array} \tag{201}$$

- Faßt man die Relationen aus (160) und (161) als Elemente von $\mathcal{J}$ auf (indem man "=" durch "−" ersetzt), so zeigt man, daß $\widetilde{\mathrm{aug}}$ auf diesen Elementen jeweils gleich Null ist. Für (160) erhält man dies direkt aus $[n-a \bmod p] = p-a$. Für (161) benutze man, daß im Fall $a \notin E$ die Menge $X := \{a+\nu\frac{n}{d};\ \nu=0,\dots,d-1\}$ mit E leeren Schnitt hat, und im anderen Fall in X genau in gerader Anzahl die x aus E vorkommen, die $x \equiv a \bmod n/d$ erfüllen. Dies läßt sich mit elementarer Kongruenzrechnung nachrechnen.

- Da $\widetilde{\mathrm{aug}}$ Homomorphismus ist, hat jedes Element aus $\mathcal{J}$, das sich als Kombination von Relationen gemäß (160) und (161) darstellen läßt, ebenfalls gewichtete Augmentation Null modulo 2.

  Die oben berechnete Relation hat aber gewichtete Augmentation Eins, da $\theta(1)$ das einzige $\theta(i)$ mit $i \in E$ ist, das in obiger Relation vorkommt.

A Anhang: Algorithmische Umsetzung

Bei der Diskussion der einzelnen Konstruktionen von Basen im Rahmen dieser Arbeit wurde immer wieder auch auf die explizite Berechenbarkeit der Basen hingewiesen.

In Bezug auf Basen stellt sich zusätzlich die Frage, wie man die Basisdarstellung von einer gegebenen Kreiseinheit erhält. In diesem Anhang geben wir dazu einen Algorithmus an, der eine solche Darstellung berechnet, wobei auf die bisher entwickelten Methoden zurückgegriffen wird. Das ursprüngliche Problem, die Bestimmung einer Basis der Kreiseinheiten, ist mit dem folgenden Algorithmus ebenfalls abgedeckt, indem man alle Kreiseinheiten $1-\epsilon_n^a$ beziehungsweise $\dfrac{1-\epsilon_n^a}{1-\epsilon_n}$ für $1 \leq a < n$ durchläuft und diejenigen ausgibt, die als Basisdarstellung sich selbst haben.

Der Algorithmus wurde in der objektorientierten Programmiersprache C++ mit Hilfe von SIMATH [14] implementiert, und das dabei entstandene Programm ist unter http://emmy.math.uni-sb.de/∼marc frei erhältlich. Die folgende Beschreibung der Algorithmen in diesem Anhang ist möglichst implementierungsnah gewählt. Um dabei aber nicht den Bezug zu den in der vorliegenden Arbeit entwickelten Methoden zu verlieren, wird zu jedem Algorithmus erläutert, wie die einzelnen Schritte mit diesen Methoden zusammenhängen.

Zunächst behandeln wir den einfacheren Fall der Kreiszahlen. Anschließend geben wir einen Algorithmus für die Kreiseinheiten an, der auf dem für die Kreiszahlen aufbaut. Schließlich werden im letzten Abschnitt einige Beispielrechnungen vorgeführt.

A.1 Der Algorithmus für Kreiszahlen

Wir arbeiten im Algorithmus mit den folgenden Objekten:

- Erzeugende Kreiszahlen $1-\epsilon_n^a$, mit $n \in \mathbf{N}$ und $a \in G_n$, im folgenden mit $u_{n,a}$ oder u_ν, wobei ν das Tupel (n,a) darstellt, bezeichnet.
- Produkte $P = \prod u_\nu^{a_\nu} := \prod (1-\epsilon_n^a)^{a_\nu}$ von den Kreiszahlen, wobei das Produkt alle Tupel $\nu = (n,a)$ mit $n \in \mathbf{N}$ und $a \in G_n$ durchläuft, aber fast alle $a_\nu = 0$ sind.

Eine grobe Version eines Algorithmus, der die Basisdarstellung einer Kreiszahl berechnet, sieht wie folgt aus.

Algorithmus A.1.1 *Gegeben sei ein Produkt $\prod u_\nu^{a_\nu}$. Der folgenden Algorithmus berechnet eine Basisdarstellung dieses Produkts.*

0. *Setze $P := \prod u_\nu^{a_\nu}$.*

1. *Sind alle u_ν mit $a_\nu > 0$ Basiselemente, dann befindet sich P bereits in Basisdarstellung. Gib P aus und beende den Algorithmus.*
2. *Wähle k mit $a_k \neq 0$, so daß u_k kein Basiselement ist.*
3. *Schreibe "in geeigneter Weise" $u_k = \prod u_\nu^{b_\nu}$.*
4. *Setze $P := u_k^{-a_k} \prod u_\nu^{a_\nu + a_k b_\nu}$.*
5. *Gehe zu Schritt 1.*

Der Erfolg des Algorithmus steht und fällt mit der Realisierung von Schritt 3, der Darstellung von u_k in "geeigneter Weise". Offensichtlich ist $u_k = u_k$ in Schritt 3 nicht geeignet, und das andere Extrem, die Vorschrift "Schreibe u_k als Produkt von Basiselementen", gewissermaßen eine Paraphrasierung von Algorithmus A.1.1, also auch nicht brauchbar.

Im folgenden benennen wir den umständlichen Ausdruck "schreibe u_k als" kurz mit "u_k entwickeln". Algorithmus A.1.1 liest sich dann in Kurzfassung:

> Entwickle die Faktoren u_k von $\prod u_\nu^{a_\nu}$ so lange, bis es nichts mehr zu entwickeln gibt.

Dabei sind wir an einer möglichst einfach realisierbaren Entwicklung interessiert, die aber dennoch in Algorithmus A.1.1 weiterführt.

Wir werden die folgenden elementaren Möglichkeiten benutzen, um u_k zu entwickeln, die wir hier zunächst benennen und später explizit algorithmisch beschreiben werden.

B) Entwickle gar nicht, u_k liegt bereits in der Basis B.

S) Entwickle durch komplexe Konjugation.

Z-p) Entwickle mit Hilfe der Zeilensumme bezüglich einem Primteiler p von n.

E) Entwickle nach Ennola.

H) Entwicklung von $u_{2,1}$.

Wir geben nun mit einer anschließenden Erläuterung einen Algorithmus an, der entscheidet, welches u_k wie entwickelt werden soll. Danach geben wir in zwei weiteren Algorithmen die Entwicklungen explizit an, und zeigen schließlich, daß mit dieser Wahl Algorithmus A.1.1 das Gewünschte liefert. Mit der Schreibweise $c := a \bmod q$ meinen wir im folgenden dasjenige $c \in G_q$ mit $c \equiv a \bmod q$.

Algorithmus A.1.2 *Es sei eine erzeugende Kreiszahl u_ν gegeben. Der folgende Algorithmus entscheidet, wie $u_\nu = u_{n,a}$ für $n \in \mathbf{N}$ und $a \in G_n$ entwickelt werden soll. Er liefert also eine der Methoden B, S, Z-p, E oder H zurück.*

0. (Initialisierung) *Es sei* $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ *die eindeutige Zerlegung in Primfaktoren, und* $q_i := p_i^{\alpha_i}$.

1. (Entscheidung) *Behandle den ersten der folgenden Fälle, der auf* n *zutrifft:*

   I) $n = 2$*? Gib H aus.*

   II) $n = 4$*? Ist* $a = 1$*, so gib B aus, sonst S.*

   III) $n = p_1$ *Primzahl? Ist* $a < p_1/2$*, so gib B aus, sonst S.*

   IV) $n \equiv 2 \bmod 4$*? Gib Z-2 aus.*

   V) n *quadratfrei oder* $n = 4u$ *mit* u *quadratfrei? Für* $i = 1, \ldots, r$ *sei* $a_i := a \bmod q_i$.

   V,i) Sind alle $a_i = 1$ *für* $i = 1, \ldots, r$*, so gib E aus, falls* r *ungerade und gib B aus, falls* r *gerade.*

   V,ii) Es sei l *minimal mit* $a_l \neq 1$*. Ist* $a_l < q_l/2$*, so gib S aus.*

   V,iii) Sind alle a_i *für* $i = l, \ldots, r$ *ungleich* $q_i - 1$*, so gib B aus.*

   V,iv) Es sei k *minimal mit* $a_k = q_k - 1$*. Gib Z-*p_k *aus.*

   VI) alle sonstigen n*: Für* $i = 1, \ldots, r$ *sei* $a_i := a \bmod p_i$ *falls* $\alpha_i = 1$*. Ansonsten sei* $\lambda_i := a \bmod q_i/p_i$ *und* $a_i := ((a \bmod q_i) - \lambda_i)/p_i^{\alpha_i - 1}$.

   VI,i) Es sei l *minimal mit* $q_l \neq 4$ *und* $\alpha_l > 1$*. Ist* $\lambda_l > p_l^{\alpha-1}/2$*, so gib S aus.*

   VI,ii) Ist $a_i \neq p_i - 1$ *für alle* $i = 1, \ldots, r$*, dann gib B aus.*

   VI,iii) Es sei l *minimal mit* $a_l = p_l - 1$*. Gib Z-*p_l *aus.*

Wir geben kurz an, wie dieser Algorithmus mit den bisher entwickelten Basiskonstruktionen zusammenhängt. Die Fälle I und II sind lediglich Spezialfälle, die aus der Nichtgutartigkeit des Kreissystems zu $n = 4$ resultieren (man vergleiche Fall b, ii von Satz 2.2.14).

Fall III behandelt den Fall, daß $n = p$ Primzahl ist. In diesem Fall ist $\widehat{D^{(p)}} \cong \langle G_p \rangle_+$. Die im Algorithmus zugrundegelegte Basis von $\langle G_p \rangle_+$ ist $\{1, \ldots, \lfloor p/2 \rfloor\}$.

Fall IV ist der triviale Fall $n \equiv 2 \bmod 4$. In diesem Fall ist $Z(n) = 0$, und zwar deswegen, weil $a \in G_n$ gleichzeitig gleich $s(n, 2, a)$, das heißt, gleich der Zeilensumme über die Komponente G_2 ist. In diesem Fall entwickeln wir a gemäß $[a] = s(n, 2, a) = -\mathtt{n}_n(s(n, 2, a))$.

In Fall V und VI wird die Quasinormalbasis aus Abschnitt 2.1.2 zugrunde gelegt.

Um den Algorithmus vollständig zu erklären, muß noch angegeben werden, wie die Entwicklungen konkret aussehen. Zunächst geben wir die Entwicklungen an, die durch Normrelationen und komplexe Konjugation entstehen.

Algorithmus A.1.3 *Die Entwicklungen S, Z-p und H für eine erzeugende Kreiszahl* $u_k = u_{n,a}$ *aus Algorithmus A.1.2 werden explizit wie folgt berechnet.*

S: *Mit S bezeichnen wir die Entwicklung mit Hilfe der Relation, die durch komplexe Konjugation entsteht. Wir nutzen also* $u_{n,a} = u_{n,n-a}$ *aus, und geben daher* $u_{n,n-a}$ *zurück.*

Z-p: *Hier nutzen wir die Normrelation, die durch Bildung der Relativnorm von* $\mathbf{Q}(\epsilon_n) \to \mathbf{Q}(\epsilon_{n/p})$ *entstehen, aus (vergleiche (118)). Explizit heißt das, daß wir das Produkt* $u_k s_p^{-1} \mathtt{n}(s_p)^{-1}$ *zurückgeben. Mit* $d := n/p$ *und* $b := a \bmod d$ *berechnen sich* $\mathtt{n}(s_p)$ *und die Zeilensumme* s_p *wie folgt:*

s_p: *Für* $i = 0, \ldots, p-1$ *sei* $c_i := b + id$. *Setze*

$$s_p := \prod_{\substack{i=0,\ldots,p-1 \\ (c_i,n)=1}} u_{n,c_i}. \tag{202}$$

$\mathtt{n}(s_p)$: *Gilt* $p|d$, *so setze* $\mathtt{n}(s_p) := u_{d,b}^{-1}$. *Ansonsten setze* $\mathtt{n}(s_p) := u_{d,b}^{-1} u_{d,bc}$ *mit* $c := p^{-1} \bmod d$.

H: *Für* $u_{2,1}$ *ist eine Sonderbehandlung erforderlich (vergleiche etwa die Diskussion um die Nichtgutartigkeit des Kreissystems im Fall* $n \equiv 0 \bmod 4$*). Begründet durch die Normrelation* $u_{2,1} = u_{4,1} u_{4,3}$ *geben wir* $u_{4,1} u_{4,3}$ *zurück.*

Im folgenden geben wir an, wie die in Satz 3.4.1 entwickelte Ennolarelation algorithmisch umgesetzt wird. Dabei benutzen wir die Tatsache, daß das Quadrat der Ennolarelation wiederum eine Relation ist, die aus Relationen Z-p, S und H zusammengesetzt ist. Es reicht daher aus, eine geeignete Relation $u_k^2 = \prod u_\nu^{a_\nu}$ anzugeben, die so aufgebaut ist, daß bei der Berechnung der Basisdarstellung $\prod u_\nu^{b_\nu}$ von $\prod u_\nu^{a_\nu}$ nicht mehr u_k entwickelt werden muß. Als Basisdarstellung von u_k erhalten ist dann $\prod u_\nu^{b_\nu/2}$. An dieser Stelle wird der der Algorithmus also rekursiv.

Algorithmus A.1.4 *Es sei eine erzeugende Kreiszahl* u_k *gegeben. Der folgende Algorithmus berechnet die Entwicklung E nach Ennola.*

0. (Initialisierung) *Es sei* $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ *die eindeutige Zerlegung von n in Primzahlpotenzen. Es sei weiter* $q_i := p_i^{\alpha_i}$.

1. (Der S^q-Operator) *Zunächst führen wir den Operator* S^q *auf einer erzeugenden Kreiszahl* $u_{n,b}$ *für* $q = q_i$ *ein. Dieser Operator ordnet* $u_{n,b}$ *die erzeugende Kreiszahl* $u_{n,c}$ *zu mit* $c \equiv -b \bmod q$ *und* $c \equiv b \bmod n/q$.

2. (Die S^q-Spur) *Setze* $v^{(1)} := u_k$ *und berechne für* $i = 1, \ldots, r$ *jeweils* $v^{(i+1)} := S^{q_i} v^{(i)}$.

3. (Berechnung der Zeilensummen) *Zu jedem* p_i *und* $v^{(i)}$ *mit* $i = 1, \ldots, r$ *berechne das Produkt* $Q_i := s_{p_i} \mathtt{n}(s_{p_i})$ *mit* s_{p_i} *und* $\mathtt{n}(s_{p_i})$ *wie in Teil Z-p in Algorithmus A.1.3.*

4. (Berechnung der Wechselsumme) *Setze* $P := v^{(1)}v^{(r+1)}\prod_{i=1}^{r} Q_i^{(-1)^i}$.

5. (Entwicklung und Ausgabe) *Berechne mit Algorithmus A.1.1 die Basisdarstellung* $\prod u_\nu^{a_\nu}$ *von* P. *Gib* $\prod u_\nu^{a_\nu/2}$ *als Basisdarstellung von* u_k *aus.*

Es ruft Algorithmus A.1.4 demnach rekursiv den ursprünglichen Algorithmus A.1.1 auf. Dies stellt kein prinzipielles Problem dar, da bei der Entwicklung von P in Schritt 5 diese Ennolaentwicklung nicht mehr genutzt wird. In den Beispielen zeigen wir, wie sich die Rekursion vermeiden läßt, was den Algorithmus insgesamt beschleunigt.

Wir skizzieren im folgenden, wie sich die Korrektheit von Algorithmus A.1.1 beweisen läßt.

Satz A.1.5 *Es liefert Algorithmus A.1.1 in Verbindung mit den Algorithmen A.1.2, A.1.3 und A.1.4 in der Tat eine Basisdarstellung eines Produktes* $\prod u_\nu^{a_\nu}$.

Beweisskizze

Man überprüft zunächst, daß in Algorithmus A.1.2 genau dann B ausgegeben wird, falls u_k ein Basiselement ist. Außerdem spiegeln die einzelnen Entwicklungsschritte E, Z-p, S und H die Relationen, die durch Zeilensummen und durch komplexe Konjugation entstanden sind, wider. Das heißt, in jedem Schritt von Algorithmus A.1.1 stellt P in der Tat immer die gleiche Kreiszahl dar.

Aus dieser Beobachtung heraus erhalten wir:

Terminiert Algorithmus A.1.1, so liefert er eine Basisdarstellung.

Mit anderen Worten, bisher ist gezeigt, daß der Algorithmus entweder unendlich lange läuft, oder aber eine Basisdarstellung liefert. Es bleibt zu zeigen, daß der Algorithmus terminiert.

Die Idee dazu besteht darin, daß wir eine vollständige Ordnung "$<$" der u_k angeben, die die folgenden Eigenschaften hat:

A) Es existieren nur endliche viele u_l mit $u_l < u_k$.

B) Ist u_k kein Basiselement, und entwickelt man u_k einmal mit Hilfe der Algorithmen A.1.2, A.1.3 und A.1.4 zu $u_k = \prod u_\nu^{a_\nu}$, dann gilt $u_\nu < u_k$ für alle ν mit $a_\nu \neq 0$.

Daß der Algorithmus terminiert ist mit dieser Ordnung direkt einzusehen, denn die u_k, die keine Basiselemente sind, verkleinern sich im Sinne dieser Ordnung bei jedem Durchlauf von Schritt 4 in Algorithmus A.1.1. Die Bedingung A verhindert aber einen unendlichen Abstieg.

Im Rest dieses Beweises definieren wir die Ordnung auf den erzeugenden Elementen u_k, die die Eigenschaften A und B erfüllt.

Im folgenden geben wir an, wie wir jeder erzeugenden Kreiszahl u_k ein 4-Tupel $\tau(u_k) = (c_1, c_2, c_3, c_4) \in \mathbf{N}_0^4$ zuordnen. Diese Tupel seien ihrerseits lexikographisch geordnet, das heißt, $(c_1, c_2, c_3, c_4) < (d_1, d_2, d_3, d_4)$ gelte genau dann, wenn $l \in \{1, 2, 3, 4\}$ existiert mit $c_l < d_l$ und $c_i = d_i$ für $1 \leq i < l$.

Bei der nachfolgenden Festlegung von τ zeigt sich, daß jedes 4-Tupel nur endlich viele Urbilder u_k unter τ hat. Die u_k mit jeweils gleichem τ-Wert seien irgendwie geordnet. Ansonsten sei $u_k < u_l$, falls $\tau(u_k) < \tau(u_l)$ ist.

Wir verwenden zur Definition von τ die Bezeichnungen und Fallunterscheidungen aus Algorithmus A.1.2: Zu $u_k = u_{n,a}$ schreiben wir $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ und $q_i := p_i^{\alpha_i}$. Wir legen τ wie folgt fest (es gilt der erste zutreffende Fall):

I) $n = 2$? Es sei $\tau(u_{2,1}) = (4, 4, 0, 0)$.

II) $n = 4$? Es seien $\tau(u_{4,3}) = (4, 3, 0, 0)$ und $\tau(u_{4,1}) = (4, 0, 0, 0)$.

III) $n = p_1$ Primzahl? Es sei $\tau(u_{n,a}) = (n, 0, 0, 0)$ für $a < p_1/2$, sonst $(n, 1, 0, 0)$.

IV) $n \equiv 2 \bmod 4$? Es sei $\tau(u_{n,a}) = (n, 0, 0, 0)$.

V) n quadratfrei oder $n = 4u$ mit u quadratfrei? Für $i = 1, \ldots, r$ sei $a_i := a \bmod q_i$. Es sei $\xi \in \{1, \ldots, r+1\}$ maximal, so daß $a_i \in \{1, p_\xi - 1\}$ für $0 < i < \xi$ ist. Weiter sei $\eta = 1$, falls $a_\xi < q_\xi/2$ und $\eta = 0$ sonst. Schließlich sei ζ die Anzahl der a_i mit $a_i = q_i - 1$, für $i = 1, \ldots, r$. Mit diesen Werten definieren wir $\tau(u_{n,a}) = (n, \xi, \eta, \zeta)$.

VI) alle sonstigen n: Für $i = 1, \ldots, r$ sei $a_i := a \bmod p_i$, falls $\alpha_i = 1$. Sonst sei $\lambda_i := a \bmod q_i/p_i$ und $a_i := ((a \bmod q_i) - \lambda_i)/p_i^{\alpha_i - 1}$.

Es sei l minimal mit $p_l^{\alpha_l} \neq 4$ und $\alpha_l > 1$. Es sei $\eta = 1$, falls $\lambda_l > p_l^{\alpha_l - 1}/2$, und sonst $\eta = 0$. Schließlich sei ζ die Anzahl der a_i mit $a_i = p_i - 1$. Wir definieren $\tau(u_{n,a}) = (n, 0, \eta, \zeta)$.

A.2 Der Algorithmus für Kreiseinheiten

Ähnlich wie bei den Kreiszahlen arbeiten wir mit den folgenden beiden Objekten:

- Erzeugende Kreiseinheiten $v_{n,a}$, mit $n \in \mathbf{N}$ und $a \in G_n$, die auch mit v_ν bezeichnet werden, wobei $\nu = (n, a)$ ist. Es ist $v_{n,a} = 1 - \epsilon_n^a$, falls n keine Potenz einer Primzahl ist, und $v_{q,a} = (1 - \epsilon_q^a)/(1 - \epsilon_q)$, falls $n = q = p^\alpha$ die Potenz einer Primzahl ist.

- Produkte $Q = \prod_\nu v_\nu^{a_\nu}$, wobei das Produkt alle Tupel $\nu = (n, a)$ durchläuft, und fast alle $a_\nu = 0$ sind.

Zur Berechnung der Basisdarstellung von $\prod v_\nu^{a_\nu}$ benutzen wir die gleiche Strategie wie bei den Kreiszahlen, die in Kurzfassung so aussieht:

Entwickle die Faktoren v_k von $\prod v_\nu^{a_\nu}$ so lange, bis es nichts mehr zu entwickeln gibt.

Um die Entwicklungsstrategien für Kreiseinheiten soweit wie möglich auf diejenigen für Kreiszahlen zurückzuführen, stellen wir zunächst einen Algorithmus vor, der ein Kreiszahlenprodukt $\prod u_\nu^{a_\nu}$ in ein Kreiseinheitenprodukt $\prod v_\nu^{b_\nu}$ umrechnet. Die umgekehrte Umrechnung ist trivial, es ist jeweils $v_{q,a} = u_{q,a}/u_{q,1}$, beziehungsweise $v_{n,a} = u_{n,a}$ zu setzen, je nachdem, ob $n = q$ Primzahlpotenz ist oder nicht.

Algorithmus A.2.1 *Es sei ein Produkt $P = \prod u_\nu^{a_\nu}$ von erzeugenden Kreiszahlen gegeben. Der folgende Algorithmus rechnet P in ein Produkt $Q = \prod v_\nu^{b_\nu}$ von erzeugenden Kreiseinheiten um, falls dieses möglich ist.*

0. (Initialisierung) *Es sei m das kleinste gemeinsame Vielfache aller n mit $a_\nu = a_{n,a} \neq 0$ und $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ die eindeutige Zerlegung von m in Potenzen von Primzahlen. Es sei weiter $q_i = p_i^{\alpha_i}$*

1. (Reduktion auf Primzahlpotenzen) *Definiere Q als das Produkt der Faktoren $v_\nu^{a_\nu}$, wobei $\nu = (n, a)$ derart ist, daß n keine Primzahlpotenz ist. Streiche aus P die entsprechenden Faktoren $u_\nu^{a_\nu}$. Jetzt besteht P nur noch aus Faktoren der Form $u_{p_i^\beta, a}$.*

2. (Umrechnung) *Führe für $j = 1, \ldots, r$, $p := p_j$, $\alpha := \alpha_j$ und $q := p^\alpha$ die folgenden Schritte aus:*

   I) Führe für $\beta = 1, \ldots, \alpha - 1$, alle $a \in G_{p^\beta}$ und $\nu = (p^\beta, a)$ die folgenden Operationen aus:

   $$Q := Q v_\nu^{a_\nu},$$
   $$P := P/((u_\nu/s_p)^{a_\nu}) \text{ mit } s_p = \prod_{i=0}^{p-1} u_{p^{\beta+1}, 1+ip^\beta}.$$

   II) Es sei $q = p^\alpha$. Für alle $a \in G_q$ und $\nu = (q, a)$ führe die folgenden Operationen aus:

   $$Q := Q v_\nu^{a_\nu},$$
   $$P := P/((u_\nu/u_{q,1})^{a_\nu}).$$

3. (Entscheidung und Ausgabe) *Ist $P = 1$, so ist Q das gesuchte Produkt. Sonst existiert keine Darstellung, das heißt, das ursprüngliche Produkt P liegt nicht in der Gruppe der Kreiseinheiten.*

Ist P_0 das ursprüngliche Produkt P beim Start des Algorithmus, so macht man die Beobachtung, daß nach jedem Schritt $P_0 = PQ$ gilt. Insbesondere wird in Unterschritt I von Schritt 2 die in (130) beschriebene Normrelation ausgenutzt, auf Grund der $u_{p^\beta,1} = s_p$ ist.

Da P in Schritt 3 höchstens aus Faktoren $u_\nu^{a_\nu}$ mit $\nu = (p^\alpha, 1)$ besteht, die keine Einheiten und voneinander linear unabhängig sind (Lemma 3.1.4), ist P genau dann gleich Eins, wenn P_0 bereits eine Kreiseinheit ist.

Algorithmus A.2.1 ermöglicht es, das Problem der Kreiseinheiten im zusammengesetzten Fall zurückzuführen auf das Entwickeln im Kreiszahlfall. Die eigentliche Arbeit muß nur noch getan werden, wenn $v_\nu = v_{q,a}$ mit einer Primzahlpotenz q ist. In diesem Fall gibt es die folgenden Möglichkeiten der Entwicklung einer erzeugenden Kreiseinheit v_ν, die wir zunächst auflisten und später explizit angeben:

B) Entwickle gar nicht, v_ν ist Teil der Basis.

S) Entwickle gemäß komplexer Konjugation.

Z) Entwickle über Zeilensummen gemäß (45).

T) Entwickle trivial zu 1 (beispielsweise $v_{q,1}$).

Der Entscheidungsalgorithmus sieht wie folgt aus.

Algorithmus A.2.2 *Es sei eine erzeugende Kreiseinheit $v_{n,a}$ gegeben. Der folgende Algorithmus entscheidet, wie $v_{n,a}$ entwickelt werden soll, liefert also eine der Methoden B, E, Z-p, S, Z oder T zurück.*

Behandle den ersten der folgenden Fälle, der auf n zutrifft:

I) n keine Potenz einer Primzahl? Gib B, S, Z-p oder E aus, je nachdem was Algorithmus A.1.2 für $u_{n,a}$ liefert.

II) $n = 2$ oder $n = 4$? Gib T aus.

III) n Primzahl? Ist $a = 1$, gib T aus. Ist sonst $a < p/2$, so gib B aus, sonst S.

IV) sonstige n (Es ist nun $n = p^\alpha$ die Potenz einer Primzahl mit $\alpha > 1$).

IV,i) Setze $\lambda := a \bmod p^{\alpha-1}$ und $b := (a - \lambda)/p^{\alpha-1}$.

V,ii) Ist $\lambda > p^{\alpha-1}/2$? Gib S aus.

V,iii) Ist $b \neq 0$? Gib B aus.

V,iv) Ist $\lambda = 1$? Gib T aus.

V,v) Gib Z aus.

Die zugehörigen Entwicklungsalgorithmen sehen folgendermaßen aus. Die Entwicklungsstrategien E und Z-p benutzen die Kreiszahlenalgorithmen. Strategie Z ist eine Übertragung von Gleichung (45).

Algorithmus A.2.3 *Die Entwicklungen E, Z-p, S, T und Z einer erzeugenden Kreiseinheit $v_{n,a}$ aus Algorithmus A.2.2 werden wie folgt berechnet:*

E,Z-p: *Entwickle $v_{n,a}$ als $u_{n,a}$ mit Hilfe der Algorithmen A.1.1, A.1.2 und A.1.3 zu $P = \prod_\nu u_\nu^{a_\nu}$. Rechne anschließend mit Algorithmus A.2.1 P zu $Q = \prod_\nu v_\nu^{b_\nu}$ um, und gib Q zurück.*

S: *Gib $v_{n,n-a}$ zurück.*

T: *Gib 1 zurück.*

Z: *Schreibe $n = p^\alpha$. Gib $v_{n,a}(s_a/s_1)^{-1}\mathtt{n}(s_a/s_1)^{-1}$ zurück. Es ist dabei mit $d := q/p$ und $b := a \bmod d$:*

$$s_a := \prod_{i=1}^{p-1} v_{n,b+id} \text{ (auch für } a = 1\text{) und } \mathtt{n}(s_a s_1^{-1}) := v_{d,b}^{-1}.$$

Zum Schluß sei noch angemerkt, daß der Korrektheitsbeweis des Algorithmus zur Berechnung der Basisdarstellung bei Kreiseinheiten direkt analog zu dem entsprechenden Beweis für Kreiszahlen (Satz A.1.5) geführt werden kann. Dabei kann man zur Definition der Ordnung auf den erzeugenden Kreiseinheiten v_k sogar $\tau(v_k) := \tau(u_k)$, mit τ wie in der Beweisskizze zu Satz A.1.5 angegeben, wählen.

A.3 Beispiele

Wir geben in diesem Abschnitt Beispiele für Basen und Entwicklungen an. Einmal für $n = 60$, da dies die kleinste Zahl ist, bei der eine Ennolarelation auftritt (Das Beispiel von Ennola in [4] ist übrigens für $n = 105$), und für $n = 16$, als extremes Beispiel einer Primzahlpotenz. Schließlich zeigen wir eine Ennolarelation für $n = 3 \cdot 4 \cdot 5 \cdot 7 \cdot 11 = 4620$.

$\underline{n = 60}$

Eine Basis erhält man am einfachsten, indem man alle erzeugenden Einheiten mit Algorithmus A.2.2 überprüft und diejenigen mit Ergebnis B ausgibt. Man findet damit

$$1 - \epsilon_{60}^{37},\ 1 - \epsilon_{20}^{17},\ 1 - \epsilon_{20},\ 1 - \epsilon_{15}^{7},\ 1 - \epsilon_{15},\ 1 - \epsilon_{12},\ \frac{1 - \epsilon_5^2}{1 - \epsilon_5}$$

als Basis von $C^{(60)}$.

Wir geben nun exemplarisch an, wie $u = 1 - \epsilon_{60}^{41}$ als Produkt von Basiselementen dargestellt wird. Es sei noch einmal darauf hingewiesen, daß alle Gleichheiten modulo Einheitswurzeln zu verstehen sind. Ob und nach welcher Methode eine erzeugende Einheit jeweils entwickelt wird, entscheidet sich nach Algorithmus A.2.2. Liefert dieser nicht B, also liegt die erzeugende Einheit nicht in der Basis, so erhalten wir die Entwicklung explizit aus Algorithmus A.2.3.

Es wird $u = 1 - \epsilon_{60}^{41}$ nach Z-3 entwickelt. Wir erhalten:

$$u = (1 - \epsilon_{60})^{-1} (1 - \epsilon_{20}) \left(1 - \epsilon_{20}^{7}\right)^{-1}. \tag{203}$$

Jetzt wird irgendeine erzeugende Einheit aus der rechten Seite von (203), die nicht selbst schon Basiselement ist, entwickelt. Im Prinzip ist es gleichgültig, welche von diesen erzeugenden Einheiten wir auswählen. Wir wählen hier wie auch in den folgenden Schritten die gemäß der in der Beweisskizze von Satz A.1.5 definierten Ordnung größte, womit wir es vermeiden, eventuell zweimal die gleiche erzeugende Einheit zu entwickeln. Dementsprechend entwickeln wir nun $1-\epsilon_{60}$.

Als Entwicklungsmethode erhalten wir E, das heißt, wir entwickeln nach Algorithmus A.1.4. Wir führen dabei jedoch nur die Schritte 0-4 aus. Den rekursiven Schritt 5 lassen wir weg. In Schritt 4 gilt $(1-\epsilon_{60})^2 = P$, oder explizit

$$\begin{aligned}(1-\epsilon_{60})^2 &= \left(1-\epsilon_{60}^{23}\right)^{-1}\left(1-\epsilon_{60}^{47}\right)^{-1}(1-\epsilon_{30})\left(1-\epsilon_{20}^{11}\right)^{-1}\left(1-\epsilon_{20}^{17}\right)\\ &\quad \left(1-\epsilon_{12}^{7}\right)^{-1}\left(1-\epsilon_{12}^{11}\right).\end{aligned} \tag{204}$$

Dieses in das Quadrat von (203) eingesetzt ergibt

$$\begin{aligned}u^2 &= \left(1-\epsilon_{60}^{23}\right)\left(1-\epsilon_{60}^{47}\right)(1-\epsilon_{30})^{-1}(1-\epsilon_{20})^2\left(1-\epsilon_{20}^{7}\right)^{-2}\\ &\quad (1-\epsilon_{20}^{11})(1-\epsilon_{20}^{17})^{-1}\left(1-\epsilon_{12}^{7}\right)\left(1-\epsilon_{12}^{11}\right)^{-1}.\end{aligned} \tag{205}$$

Wir erhalten als weitere Entwicklungen

$$\begin{aligned}1-\epsilon_{60}^{23} &= \left(1-\epsilon_{60}^{53}\right)^{-1}\left(1-\epsilon_{30}^{23}\right) && \text{nach Z-2}\\ 1-\epsilon_{60}^{53} &= \left(1-\epsilon_{60}^{13}\right)^{-1}\left(1-\epsilon_{20}^{11}\right)^{-1}\left(1-\epsilon_{20}^{13}\right) && \text{nach Z-3}\\ 1-\epsilon_{60}^{13} &= 1-\epsilon_{60}^{47} && \text{nach S}\\ 1-\epsilon_{60}^{47} &= \left(1-\epsilon_{60}^{17}\right)^{-1}\left(1-\epsilon_{30}^{17}\right) && \text{nach Z-2}\\ 1-\epsilon_{60}^{17} &= \left(1-\epsilon_{60}^{37}\right)^{-1}\left(1-\epsilon_{20}^{17}\right)\left(1-\epsilon_{20}^{19}\right)^{-1} && \text{nach Z-3 .}\end{aligned} \tag{206}$$

Dies eingesetzt in (205) ergibt

$$\begin{aligned}u^2 &= \left(1-\epsilon_{60}^{37}\right)^2(1-\epsilon_{30})^{-1}\left(1-\epsilon_{30}^{17}\right)^2\left(1-\epsilon_{30}^{23}\right)(1-\epsilon_{20})^2\left(1-\epsilon_{20}^{7}\right)^{-2}\\ &\quad \left(1-\epsilon_{20}^{11}\right)^2\left(1-\epsilon_{20}^{13}\right)^{-1}\left(1-\epsilon_{20}^{17}\right)^{-3}\left(1-\epsilon_{20}^{19}\right)^2\left(1-\epsilon_{12}^{7}\right)\left(1-\epsilon_{12}^{11}\right)^{-1}.\end{aligned} \tag{207}$$

Es ist $1-\epsilon_{60}^{37}$ Basiselement. Die Faktoren $1-\epsilon_{30}^{*}$ werden alle nach Z-2 entwickelt, und mit

$$\begin{aligned}1-\epsilon_{30} &= (1-\epsilon_{15})\left(1-\epsilon_{15}^{8}\right)^{-1} && \text{nach Z-2}\\ 1-\epsilon_{30}^{17} &= (1-\epsilon_{15})^{-1}\left(1-\epsilon_{15}^{2}\right) && \text{nach Z-2}\\ 1-\epsilon_{30}^{23} &= \left(1-\epsilon_{15}^{4}\right)^{-1}\left(1-\epsilon_{15}^{8}\right) && \text{nach Z-2}\end{aligned} \tag{208}$$

erhalten wir

$$\begin{aligned}u^2 &= \left(1-\epsilon_{60}^{37}\right)^2(1-\epsilon_{20})^2\left(1-\epsilon_{20}^{7}\right)^{-2}\left(1-\epsilon_{20}^{11}\right)^2\\ &\quad \left(1-\epsilon_{20}^{13}\right)^{-1}\left(1-\epsilon_{20}^{17}\right)^{-3}\left(1-\epsilon_{20}^{19}\right)^2(1-\epsilon_{15})^{-3}\\ &\quad \left(1-\epsilon_{15}^{2}\right)^2\left(1-\epsilon_{15}^{4}\right)^{-1}\left(1-\epsilon_{15}^{8}\right)^2\left(1-\epsilon_{12}^{7}\right)\\ &\quad \left(1-\epsilon_{12}^{11}\right)^{-1}.\end{aligned} \tag{209}$$

Mit

$$\begin{array}{rcll} 1-\epsilon_{20}^{19} &=& \left(1-\epsilon_{20}^{9}\right)^{-1}\left(1-\epsilon_{10}^{9}\right) & \text{nach Z-2} \\ 1-\epsilon_{20}^{9} &=& \left(1-\epsilon_{20}\right)^{-1}\left(1-\epsilon_{20}^{13}\right)^{-1}\left(1-\epsilon_{20}^{17}\right)^{-1} & \text{nach Z-5} \\ 1-\epsilon_{20}^{11} &=& \left(1-\epsilon_{20}\right)^{-1}\left(1-\epsilon_{10}\right) & \text{nach Z-2} \\ 1-\epsilon_{20}^{13} &=& 1-\epsilon_{20}^{7} & \text{nach S} \\ 1-\epsilon_{20}^{7} &=& \left(1-\epsilon_{20}^{17}\right)^{-1}\left(1-\epsilon_{10}^{7}\right) & \text{nach Z-2} \end{array} \tag{210}$$

und

$$\begin{array}{rcll} 1-\epsilon_{15}^{4} &=& \left(1-\epsilon_{15}\right)^{-1}\left(1-\epsilon_{15}^{7}\right)^{-1}\left(1-\epsilon_{15}^{13}\right)^{-1}\dfrac{1-\epsilon_3}{1-\epsilon_3} & \\ & & \left(\dfrac{1-\epsilon_3^2}{1-\epsilon_3}\right)^{-1} & \text{nach Z-5} \\ 1-\epsilon_{15}^{8} &=& \left(1-\epsilon_{15}^{13}\right)^{-1}\left(\dfrac{1-\epsilon_5}{1-\epsilon_5}\right)^{-1}\dfrac{1-\epsilon_5^3}{1-\epsilon_5} & \text{nach Z-3} \\ 1-\epsilon_{15}^{13} &=& 1-\epsilon_{15}^{2} & \text{nach S} \\ 1-\epsilon_{15}^{2} &=& \left(1-\epsilon_{15}^{7}\right)^{-1}\dfrac{1-\epsilon_5^2}{1-\epsilon_5}\left(\dfrac{1-\epsilon_5^4}{1-\epsilon_5}\right)^{-1} & \text{nach Z-3} \end{array} \tag{211}$$

erhalten wir

$$\begin{array}{rcl} u^2 &=& \left(1-\epsilon_{60}^{37}\right)^2\left(1-\epsilon_{20}\right)^2\left(1-\epsilon_{15}\right)^{-2}\left(1-\epsilon_{12}^{7}\right) \\ & & \left(1-\epsilon_{12}^{11}\right)^{-1}\left(1-\epsilon_{10}\right)^2\left(1-\epsilon_{10}^{7}\right)^{-1}\left(1-\epsilon_{10}^{9}\right)^2 \\ & & \left(\dfrac{1-\epsilon_5}{1-\epsilon_5}\right)^{-2}\dfrac{1-\epsilon_5^2}{1-\epsilon_5}\left(\dfrac{1-\epsilon_5^3}{1-\epsilon_5}\right)^2\left(\dfrac{1-\epsilon_5^4}{1-\epsilon_5}\right)^{-1} \\ & & \left(\dfrac{1-\epsilon_3}{1-\epsilon_3}\right)^{-1}\dfrac{1-\epsilon_3^2}{1-\epsilon_3}. \end{array} \tag{212}$$

Die Entwicklungen

$$\begin{array}{rcll} 1-\epsilon_{12}^{11} &=& \left(1-\epsilon_{12}^{5}\right)^{-1}\left(1-\epsilon_{6}^{5}\right) & \text{nach Z-2} \\ 1-\epsilon_{12}^{5} &=& \left(1-\epsilon_{12}\right)^{-1}\dfrac{1-\epsilon_4}{1-\epsilon_4}\left(\dfrac{1-\epsilon_4^3}{1-\epsilon_4}\right)^{-1} & \text{nach Z-3} \\ 1-\epsilon_{12}^{7} &=& \left(1-\epsilon_{12}\right)^{-1}\left(1-\epsilon_{6}\right) & \text{nach Z-2} \\ 1-\epsilon_{10} &=& \dfrac{1-\epsilon_5}{1-\epsilon_5}\left(\dfrac{1-\epsilon_5^3}{1-\epsilon_5}\right)^{-1} & \text{nach Z-2} \\ 1-\epsilon_{10}^{7} &=& \left(\dfrac{1-\epsilon_5}{1-\epsilon_5}\right)^{-1}\dfrac{1-\epsilon_5^2}{1-\epsilon_5} & \text{nach Z-2} \\ 1-\epsilon_{10}^{9} &=& \left(\dfrac{1-\epsilon_5^2}{1-\epsilon_5}\right)^{-1}\dfrac{1-\epsilon_5^4}{1-\epsilon_5} & \text{nach Z-2} \end{array} \tag{213}$$

eingesetzt in (212) ergeben

$$\begin{aligned} u^2 &= \left(1-\epsilon_{60}^{37}\right)^2 (1-\epsilon_{20})^2 (1-\epsilon_{15})^{-2} (1-\epsilon_{12})^{-2} \\ &\quad (1-\epsilon_6)\left(1-\epsilon_6^5\right)^{-1} \frac{1-\epsilon_5}{1-\epsilon_5}\left(\frac{1-\epsilon_5^2}{1-\epsilon_5}\right)^{-2} \\ &\quad \frac{1-\epsilon_5^4}{1-\epsilon_5}\frac{1-\epsilon_4}{1-\epsilon_4}\left(\frac{1-\epsilon_4^3}{1-\epsilon_4}\right)^{-1}\left(\frac{1-\epsilon_3}{1-\epsilon_3}\right)^{-1} \\ &\quad \frac{1-\epsilon_3^2}{1-\epsilon_3}. \end{aligned} \tag{214}$$

Die erzeugenden Einheiten $1-\epsilon_6$, $1-\epsilon_6^5$, $\frac{1-\epsilon_5}{1-\epsilon_5}$, $\frac{1-\epsilon_5^4}{1-\epsilon_5}$, $\frac{1-\epsilon_4}{1-\epsilon_4}$, $\frac{1-\epsilon_4^3}{1-\epsilon_4}$, $\frac{1-\epsilon_3}{1-\epsilon_3}$ und $\frac{1-\epsilon_3^2}{1-\epsilon_3}$ entwickeln sich alle (eventuell über einen Umweg über Z-2 und S) zu 1. Ziehen wir die Quadratwurzel aus dem verbleibenden Produkt, erhalten wir schließlich als Basisdarstellung von $u = 1-\epsilon_{60}^{41}$ das Produkt

$$u = \left(1-\epsilon_{60}^{37}\right)(1-\epsilon_{20})(1-\epsilon_{15})^{-1}(1-\epsilon_{12})^{-1}\left(\frac{1-\epsilon_5^2}{1-\epsilon_5}\right)^{-1}. \tag{215}$$

Diese Gleichheit gilt modulo Einheitswurzeln. Um Gleichheit als komplexe Zahlen zu erhalten, kann man bei den S-Entwicklungen jeweils die Einheitswurzeln berücksichtigen und beim Wurzelziehen das Vorzeichen durch Einsetzen konkreter Werte berechnen. Alternativ kann man auch direkt durch Einsetzen ausprobieren, welcher der Werte ϵ_{60}^a mit $0 \le a < 59$ passt, was beispielsweise direkt mit dem zum SIMATH-Paket [14] gehörigen Kalkulator simcalc ausgerechnet werden kann. Man erhält damit $a = 56$, also gilt (diesmal nicht modulo Torsion, sondern direkt als Gleichheit algebraischer Zahlen)

$$1-\epsilon_{60}^{41} = \epsilon_{15}^{14}\left(1-\epsilon_{60}^{37}\right)(1-\epsilon_{20})(1-\epsilon_{15})^{-1}(1-\epsilon_{12})^{-1}\left(\frac{1-\epsilon_5^2}{1-\epsilon_5}\right)^{-1}. \tag{216}$$

$\underline{n = 16}$

Eine Basis von $C^{(16)}$ erhält man wie im Fall $n = 60$. Hier ist sie gegeben durch

$$\frac{1-\epsilon_{16}^{11}}{1-\epsilon_{16}}, \frac{1-\epsilon_{16}^{9}}{1-\epsilon_{16}}, \frac{1-\epsilon_8^5}{1-\epsilon_8}.$$

Gemäß Algorithmus A.2.2 sind alle Entwicklungen von erzeugenden Einheiten, die nicht in der Basis liegen, außer einer S- oder T-Entwicklungen. Wir geben die einzige Z-Entwicklung an:

$$\frac{1-\epsilon_{16}^3}{1-\epsilon_{16}} = \frac{1-\epsilon_{16}}{1-\epsilon_{16}}\frac{1-\epsilon_{16}^9}{1-\epsilon_{16}}\left(\frac{1-\epsilon_{16}^{11}}{1-\epsilon_{16}}\right)^{-1}\left(\frac{1-\epsilon_8}{1-\epsilon_8}\right)^{-1}\frac{1-\epsilon_8^3}{1-\epsilon_8}. \tag{217}$$

Bereinigt man diese um Faktoren, die sich trivial entwickeln, entwickelt man $\frac{1-\epsilon_8^3}{1-\epsilon_8}$ zu $\frac{1-\epsilon_8^5}{1-\epsilon_8}$ und berechnet man den Torsionsanteil, so erhält man

$$\frac{1-\epsilon_{16}^{3}}{1-\epsilon_{16}} = \epsilon_8^7 \frac{1-\epsilon_{16}^{9}}{1-\epsilon_{16}} \left(\frac{1-\epsilon_{16}^{11}}{1-\epsilon_{16}}\right)^{-1} \frac{1-\epsilon_8^5}{1-\epsilon_8} \tag{218}$$

als Basisdarstellung.

$\underline{n = 4620}$

Es ist 4620 nach Satz 3.4.1 die kleinste Zahl mit 5 Primfaktoren, bei der Ennolarelationen auftreten. Eine Basis der Gruppe der Kreiseinheiten besteht aus 479 Elementen. Gemäß Algorithmus A.1.2 wird $1-\epsilon_{4620}$ nach Ennola entwickelt. Die Basisdarstellung von $1-\epsilon_{4620}$ hat 244 Faktoren, das heißt, es ist

$$\begin{aligned}
1-\epsilon_{4620} = \epsilon_{231}^{73} &\left(1-\epsilon_{4620}^{37}\right)^{-1} \left(1-\epsilon_{4620}^{157}\right)^{-1} \left(1-\epsilon_{4620}^{421}\right)^{-1} \left(1-\epsilon_{4620}^{541}\right)^{-1} \\
&\left(1-\epsilon_{4620}^{577}\right)^{-1} \left(1-\epsilon_{4620}^{661}\right)^{-1} \left(1-\epsilon_{4620}^{841}\right)^{-1} \left(1-\epsilon_{4620}^{961}\right)^{-1} \left(1-\epsilon_{4620}^{1081}\right)^{-1} \\
&\left(1-\epsilon_{4620}^{1501}\right)^{-1} \left(1-\epsilon_{4620}^{1597}\right)^{-1} \left(1-\epsilon_{4620}^{1717}\right)^{-1} \left(1-\epsilon_{4620}^{2017}\right)^{-1} \left(1-\epsilon_{4620}^{2137}\right)^{-1} \\
&\left(1-\epsilon_{4620}^{2257}\right)^{-1} \left(1-\epsilon_{4620}^{2521}\right)^{-1} \left(1-\epsilon_{4620}^{2557}\right)^{-1} \left(1-\epsilon_{4620}^{2641}\right)^{-1} \left(1-\epsilon_{4620}^{2677}\right)^{-1} \\
&\left(1-\epsilon_{4620}^{2941}\right)^{-1} \left(1-\epsilon_{4620}^{3061}\right)^{-1} \left(1-\epsilon_{4620}^{3181}\right)^{-1} \left(1-\epsilon_{4620}^{3481}\right)^{-1} \left(1-\epsilon_{4620}^{3601}\right)^{-1} \\
&\left(1-\epsilon_{4620}^{3697}\right)^{-1} \left(1-\epsilon_{4620}^{4117}\right)^{-1} \left(1-\epsilon_{4620}^{4237}\right)^{-1} \left(1-\epsilon_{4620}^{4357}\right)^{-1} \left(1-\epsilon_{4620}^{4537}\right)^{-1} \\
&\left(1-\epsilon_{1540}^{37}\right) \left(1-\epsilon_{1540}^{57}\right) \left(1-\epsilon_{1540}^{101}\right) \left(1-\epsilon_{1540}^{157}\right) \left(1-\epsilon_{1540}^{177}\right) \left(1-\epsilon_{1540}^{257}\right) \\
&\left(1-\epsilon_{1540}^{261}\right) \left(1-\epsilon_{1540}^{317}\right) \left(1-\epsilon_{1540}^{397}\right) \left(1-\epsilon_{1540}^{401}\right) \left(1-\epsilon_{1540}^{421}\right) \left(1-\epsilon_{1540}^{437}\right) \\
&\left(1-\epsilon_{1540}^{477}\right) \left(1-\epsilon_{1540}^{537}\right) \left(1-\epsilon_{1540}^{541}\right) \left(1-\epsilon_{1540}^{577}\right) \left(1-\epsilon_{1540}^{597}\right) \left(1-\epsilon_{1540}^{617}\right) \\
&\left(1-\epsilon_{1540}^{717}\right) \left(1-\epsilon_{1540}^{757}\right) \left(1-\epsilon_{1540}^{877}\right) \left(1-\epsilon_{1540}^{961}\right) \left(1-\epsilon_{1540}^{981}\right) \left(1-\epsilon_{1540}^{1017}\right) \\
&\left(1-\epsilon_{1540}^{1037}\right) \left(1-\epsilon_{1540}^{1081}\right) \left(1-\epsilon_{1540}^{1097}\right) \left(1-\epsilon_{1540}^{1101}\right) \left(1-\epsilon_{1540}^{1137}\right) \left(1-\epsilon_{1540}^{1157}\right) \\
&\left(1-\epsilon_{1540}^{1237}\right) \left(1-\epsilon_{1540}^{1241}\right) \left(1-\epsilon_{1540}^{1277}\right) \left(1-\epsilon_{1540}^{1317}\right) \left(1-\epsilon_{1540}^{1417}\right) \left(1-\epsilon_{1540}^{1457}\right) \\
&\left(1-\epsilon_{1540}^{1521}\right) \left(1-\epsilon_{1155}\right) \left(1-\epsilon_{1155}^{52}\right)^{-1} \left(1-\epsilon_{1155}^{67}\right)^{-1} \left(1-\epsilon_{1155}^{127}\right)^{-1} \\
&\left(1-\epsilon_{1155}^{172}\right)^{-1} \left(1-\epsilon_{1155}^{211}\right) \left(1-\epsilon_{1155}^{226}\right)^{-1} \left(1-\epsilon_{1155}^{277}\right)^{-1} \left(1-\epsilon_{1155}^{292}\right)^{-1} \\
&\left(1-\epsilon_{1155}^{337}\right)^{-1} \left(1-\epsilon_{1155}^{382}\right)^{-1} \left(1-\epsilon_{1155}^{397}\right)^{-1} \left(1-\epsilon_{1155}^{436}\right)^{-1} \left(1-\epsilon_{1155}^{457}\right)^{-1} \\
&\left(1-\epsilon_{1155}^{502}\right)^{-1} \left(1-\epsilon_{1155}^{547}\right)^{-1} \left(1-\epsilon_{1155}^{556}\right)^{-1} \left(1-\epsilon_{1155}^{607}\right)^{-1} \left(1-\epsilon_{1155}^{646}\right)^{-1} \\
&\left(1-\epsilon_{1155}^{667}\right)^{-1} \left(1-\epsilon_{1155}^{712}\right)^{-1} \left(1-\epsilon_{1155}^{766}\right)^{-1} \left(1-\epsilon_{1155}^{787}\right)^{-1} \left(1-\epsilon_{1155}^{877}\right)^{-1} \\
&\left(1-\epsilon_{1155}^{976}\right)^{-1} \left(1-\epsilon_{1155}^{997}\right)^{-1} \left(1-\epsilon_{1155}^{1117}\right)^{-1} \left(1-\epsilon_{924}^{37}\right) \left(1-\epsilon_{924}^{73}\right) \left(1-\epsilon_{924}^{157}\right) \\
&\left(1-\epsilon_{924}^{169}\right) \left(1-\epsilon_{924}^{205}\right) \left(1-\epsilon_{924}^{289}\right) \left(1-\epsilon_{924}^{409}\right) \left(1-\epsilon_{924}^{493}\right) \left(1-\epsilon_{924}^{541}\right) \\
&\left(1-\epsilon_{924}^{577}\right) \left(1-\epsilon_{924}^{625}\right) \left(1-\epsilon_{924}^{661}\right) \left(1-\epsilon_{924}^{673}\right) \left(1-\epsilon_{924}^{709}\right) \left(1-\epsilon_{924}^{793}\right) \\
&\left(1-\epsilon_{924}^{829}\right) \left(1-\epsilon_{660}^{37}\right) \left(1-\epsilon_{660}^{97}\right) \left(1-\epsilon_{660}^{157}\right) \left(1-\epsilon_{660}^{181}\right) \left(1-\epsilon_{660}^{277}\right) \\
&\left(1-\epsilon_{660}^{397}\right) \left(1-\epsilon_{660}^{457}\right) \left(1-\epsilon_{660}^{541}\right) \left(1-\epsilon_{660}^{577}\right) \left(1-\epsilon_{420}\right) \left(1-\epsilon_{420}^{157}\right) \\
&\left(1-\epsilon_{420}^{241}\right) \left(1-\epsilon_{420}^{337}\right) \left(1-\epsilon_{385}^{12}\right)^{-1} \left(1-\epsilon_{385}^{16}\right) \left(1-\epsilon_{385}^{17}\right) \left(1-\epsilon_{385}^{31}\right) \\
&\left(1-\epsilon_{385}^{36}\right)^{-1} \left(1-\epsilon_{385}^{51}\right)^{2} \left(1-\epsilon_{385}^{52}\right) \left(1-\epsilon_{385}^{72}\right) \left(1-\epsilon_{385}^{82}\right)^{-1} \left(1-\epsilon_{385}^{86}\right)
\end{aligned}$$

$$\left(1-\epsilon_{385}^{107}\right)\left(1-\epsilon_{385}^{127}\right)\left(1-\epsilon_{385}^{152}\right)^{-1}\left(1-\epsilon_{385}^{162}\right)\left(1-\epsilon_{385}^{171}\right)\left(1-\epsilon_{385}^{206}\right)$$
$$\left(1-\epsilon_{385}^{211}\right)^{-1}\left(1-\epsilon_{385}^{222}\right)\left(1-\epsilon_{385}^{226}\right)\left(1-\epsilon_{385}^{227}\right)\left(1-\epsilon_{385}^{261}\right)\left(1-\epsilon_{385}^{276}\right)$$
$$\left(1-\epsilon_{385}^{277}\right)\left(1-\epsilon_{385}^{282}\right)\left(1-\epsilon_{385}^{292}\right)\left(1-\epsilon_{385}^{327}\right)\left(1-\epsilon_{385}^{331}\right)\left(1-\epsilon_{385}^{337}\right)$$
$$\left(1-\epsilon_{385}^{346}\right)\left(1-\epsilon_{385}^{347}\right)\left(1-\epsilon_{385}^{366}\right)\left(1-\epsilon_{385}^{381}\right)\left(1-\epsilon_{385}^{382}\right)\left(1-\epsilon_{308}^{9}\right)^{-1}$$
$$\left(1-\epsilon_{308}^{37}\right)^{-1}\left(1-\epsilon_{308}^{45}\right)^{-1}\left(1-\epsilon_{308}^{57}\right)^{-1}\left(1-\epsilon_{308}^{93}\right)^{-1}\left(1-\epsilon_{308}^{101}\right)^{-1}$$
$$\left(1-\epsilon_{308}^{113}\right)^{-1}\left(1-\epsilon_{308}^{149}\right)\left(1-\epsilon_{308}^{157}\right)^{-2}\left(1-\epsilon_{308}^{169}\right)^{-1}\left(1-\epsilon_{308}^{177}\right)^{-1}$$
$$\left(1-\epsilon_{308}^{185}\right)^{-1}\left(1-\epsilon_{308}^{213}\right)^{-1}\left(1-\epsilon_{308}^{225}\right)^{-1}\left(1-\epsilon_{308}^{233}\right)^{-1}\left(1-\epsilon_{308}^{269}\right)^{-1}$$
$$\left(1-\epsilon_{308}^{289}\right)^{-1}\left(1-\epsilon_{231}^{31}\right)^{-1}\left(1-\epsilon_{231}^{73}\right)^{-1}\left(1-\epsilon_{231}^{148}\right)\left(1-\epsilon_{231}^{163}\right)^{-1}\left(1-\epsilon_{231}^{169}\right)$$
$$\left(1-\epsilon_{231}^{190}\right)\left(1-\epsilon_{231}^{205}\right)^{-1}\left(1-\epsilon_{220}^{37}\right)^{-1}\left(1-\epsilon_{220}^{57}\right)^{-1}\left(1-\epsilon_{220}^{97}\right)^{-1}$$
$$\left(1-\epsilon_{220}^{101}\right)^{-1}\left(1-\epsilon_{220}^{137}\right)^{-1}\left(1-\epsilon_{220}^{157}\right)^{-1}\left(1-\epsilon_{220}^{177}\right)^{-1}\left(1-\epsilon_{220}^{181}\right)^{-1}$$
$$\left(1-\epsilon_{220}^{217}\right)^{-1}\left(1-\epsilon_{165}^{16}\right)\left(1-\epsilon_{165}^{91}\right)\left(1-\epsilon_{165}^{97}\right)^{-1}\left(1-\epsilon_{165}^{127}\right)^{-1}\left(1-\epsilon_{165}^{136}\right)$$
$$\left(1-\epsilon_{140}^{17}\right)^{-1}\left(1-\epsilon_{140}^{101}\right)^{-1}\left(1-\epsilon_{140}^{137}\right)\left(1-\epsilon_{132}^{25}\right)\left(1-\epsilon_{105}^{22}\right)\left(1-\epsilon_{105}^{37}\right)$$
$$\left(1-\epsilon_{105}^{52}\right)\left(1-\epsilon_{105}^{67}\right)\left(1-\epsilon_{105}^{82}\right)\left(1-\epsilon_{84}^{37}\right)^{-1}\left(1-\epsilon_{84}^{73}\right)^{-1}\left(1-\epsilon_{77}^{9}\right)^{-1}$$
$$\left(1-\epsilon_{77}^{16}\right)^{-1}\left(1-\epsilon_{77}^{23}\right)^{-1}\left(1-\epsilon_{77}^{30}\right)^{-1}\left(1-\epsilon_{77}^{36}\right)\left(1-\epsilon_{77}^{37}\right)^{-1}\left(1-\epsilon_{77}^{51}\right)^{-1}$$
$$\left(1-\epsilon_{77}^{58}\right)^{-1}\left(1-\epsilon_{77}^{71}\right)\left(1-\epsilon_{55}\right)^{-1}\left(1-\epsilon_{55}^{16}\right)^{-1}\left(1-\epsilon_{55}^{17}\right)^{-1}\left(1-\epsilon_{55}^{27}\right)$$
$$\left(1-\epsilon_{55}^{37}\right)\left(1-\epsilon_{55}^{42}\right)^{2}\left(1-\epsilon_{55}^{46}\right)\left(1-\epsilon_{55}^{47}\right)\left(1-\epsilon_{44}\right)^{-1}\left(1-\epsilon_{44}^{5}\right)\left(1-\epsilon_{44}^{13}\right)$$
$$\left(1-\epsilon_{35}\right)^{-1}\left(1-\epsilon_{35}^{17}\right)^{-2}\left(1-\epsilon_{35}^{22}\right)^{-2}\left(1-\epsilon_{35}^{31}\right)^{-2}\left(1-\epsilon_{35}^{32}\right)^{-2}\left(1-\epsilon_{33}\right)^{-2}$$
$$\left(1-\epsilon_{33}^{4}\right)^{-1}\left(1-\epsilon_{33}^{16}\right)^{-1}\left(1-\epsilon_{33}^{25}\right)^{-2}\left(1-\epsilon_{28}^{17}\right)^{2}\left(1-\epsilon_{21}\right)^{-1}\left(1-\epsilon_{15}\right)^{-1}$$
$$\frac{1-\epsilon_{11}}{1-\epsilon_{11}}\left(\frac{1-\epsilon_{11}^{2}}{1-\epsilon_{11}}\right)^{-1}\frac{1-\epsilon_{11}^{3}}{1-\epsilon_{11}}\left(\frac{1-\epsilon_{11}^{5}}{1-\epsilon_{11}}\right)^{-1}\frac{1-\epsilon_{7}}{1-\epsilon_{7}}\left(\frac{1-\epsilon_{7}^{3}}{1-\epsilon_{7}}\right)^{-1}\frac{1-\epsilon_{5}}{1-\epsilon_{5}}$$
$$\left(\frac{1-\epsilon_{5}^{2}}{1-\epsilon_{5}}\right)^{-1}.$$

A.4 Programmtechnische Aspekte

A.4.1 Optimierungen

Die realen Laufzeiten der Programme, die die Beispiele in Abschnitt A.3 berechnen, liegen im Sekundenbereich. Obwohl im Rahmen dieses Anhanges die theoretische Entwicklung des Algorithmus im Vordergrund steht, sollen an dieser Stelle einige Optimierungsmöglichkeiten angesprochen werden. Wir beziehen uns jeweils nur auf den Kreiszahlenalgorithmus, die genannten Verbesserungen gelten aber für Kreiseinheiten sinngemäß.

Optimierung durch τ-Werte

Die im Beweis zu Satz A.1.5 eingeführte Funktion τ, die jeder Kreiszahl u_k, ein Quadrupel $\tau(u_k)$ zuordnet, kann dadurch benutzt werden, daß man in Schritt 2

von Algorithmus A.1.1 jeweils ein k mit maximalem u_k wählt. Dies verhindert das eventuell doppelte Entwickeln des gleichen u_k.

Parallelisierung

Ein Vorteil von Algorithmus A.1.2 ist die Möglichkeit der Parallelisierbarkeit. Es können durchaus mehrere u_k gleichzeitig entwickelt werden. Beispielsweise können die Entwicklungen in (208) und anschließend in (210) und so weiter problemlos parallel auf verschiedenen Prozessoren ausgeführt werden.

Vermeidung der Rekursion

Am Beispiel der Entwicklung von $1-\epsilon_{60}^{41}$ wurde bereits verdeutlicht, wie man sich den Rekursionsschritt 5 in Algorithmus A.1.4 sparen kann, indem man statt der Darstellung von u die Basisdarstellung von u^2 berechnet und anschließend durch Ziehen der Quadratwurzel aus der Darstellung von u^2 eine Basisdarstellung von u erhält.

Datenbanken

Da die Basen von $C^{(n)}$ streng hierarchisch aufeinander aufbauen, lassen sich einmal in $C^{(n)}$ gemachte Entwicklungen wiederverwenden für Entwicklungen innerhalb von $C^{(m)}$ mit $n|m$. Somit lohnt sich das Abspeichern von besonders zeitintensiven Entwicklungen, beispielsweise der Ennolaentwicklungen.

Interne Darstellung

Schließlich sei noch erwähnt, daß die interne Realisierung der Datentypen Kreiszahl und Produkt der Kreiszahlen eine nicht unerhebliche Rolle spielt. Beispielsweise sollte das Produkt intern als eine *geordnete* Liste von Kreiszahlen dargestellt werden, um beim Zusammenmultiplizieren zweier Produkte eine Laufzeit zu erhalten, die linear in der Länge der beiden Produkte ist (und nicht quadratisch).

A.4.2 Laufzeit

Die Auflistung im Abschnitt "Optimierung" macht schon deutlich, daß die reale Laufzeit des Algorithmus sehr stark von der Implementierung abhängt. Eine gute theoretische Abschätzung läßt sich auch deswegen nur schwer angeben, weil nicht klar ist, von welchen Parametern die Laufzeit der Entwicklung von $1-\epsilon_n^a$ abhängig gemacht werden soll. Sicher spielt die Anzahl der Primfaktoren von n eine Rolle, jedoch ist beispielsweise die vollständige Entwicklung von $1-\epsilon_{420}$ schneller berechnet, als die von $1-\epsilon_{105}$, da ersteres Basiselement ist, letzteres nach Ennola entwickelt wird.

In der Praxis stellt sich heraus, daß der wesentliche Faktor, der die Berechnungen limitiert, die Anzahl der Faktoren der bei der Entwicklung auftretenden Produkte ist. Ab einer gewissen Größe ist der Rechner fast ausschließlich mit der internen Verwaltung der Produkte im Speicher beschäftigt. Da die Größe der Basis von $C^{(n)}$ nach Lemma 3.1.2 gleich $\frac{1}{2}\varphi(n)-1$ ist, muß im Prinzip mit Produkten dieser Größenordnung bei der Berechnung der Basisdarstellung gerechnet werden.

Nimmt man an, daß zwei Produkte von Kreiszahlen in $O(n)$ Schritten mul-

tipliziert werden können, und daß die Schritte 1-5 von Algorithmus A.1.1 höchstens n mal durchlaufen werden, erhält man zur Berechnung der Basisdarstellung von $1-\epsilon_n^a$ als theoretische Laufzeit $O(n^2)$.

A.4.3 Verifikation des Programmes

Da alle Implementierungen bekanntermaßen Fehler enthalten, sind einige Plausibilitätstests nützlich, durch die Programmierfehler entdeckt werden können. Wir geben im folgenden vier Tests an:

a) Bei der Berechnung der Ennolarelation muß aus einem Produkt Q die Quadratwurzel gezogen werden. An dieser Stelle sollte unbedingt geprüft werden, ob Q überhaupt Quadrat ist! Der Vorteil dieser relativ simplen Abfrage (Sind alle Exponenten durch 2 teilbar?) ist, daß Programmfehler so während des normalen Betriebes entdeckt werden. Dieser Test wurde implementiert.

b) Man rechne die linke und rechte Seite einer Relation im n-ten Kreisteilungskörper $\mathbf{Q}(\epsilon_n)$ aus. Die Relation ist korrekt, wenn sich beide Seiten höchstens um eine Einheitswurzel unterscheiden. Dies ist offensichtlich die sicherste Methode. Sie ist jedoch eventuell für größere n zu aufwendig. Dieser Test ist in SIMATH [14] durchführbar, da eine Arithmetik zum Rechnen in algebraischen Zahlkörpern zur Verfügung steht.

c) Man verfahre wie in b, rechne jedoch in den komplexen Zahlen $\mathbf{C}$, das heißt, man rechne die Produkte mit einer gewissen Rechengenauigkeit aus. In diesem Fall gilt die Sicherheit aber auch nur modulo dieser Rechengenauigkeit. Mit diesem Test wurden die in dieser Arbeit vorgestellten Beispiele überprüft. Insbesondere auch, weil die Rechengenauigkeit beliebig genau gewählt werden kann, ist dieser Test im Rahmen dieser Arbeit ausreichend, so daß auf einen Test nach b verzichtet werden konnte.

d) Schließlich rechne man Beispiele aus, deren Entwicklung bekannt ist. Beispielsweise das Produkt über alle $1-\epsilon_n^a$ mit $a \in G_n$ ist das Produkt aller Konjugierten von $1-\epsilon_n$, und muß daher 1 ergeben, wenn n keine Primzahlpotenz ist. Bei diesen Beispielen rechnete das Programm ebenfalls korrekt.

A.4.4 Der Algorithmus als Wortproblem

Interpretiert man die Menge der Erzeugenden modulo der Relationen als eine Grammatik, so ist der vorgestellte Algorithmus ein Beispiel für die Lösung des Wortproblems dieser Grammatik. Das heißt, zu jedem Produkt $\prod u_\nu^{a_\nu}$ läßt sich eine eindeutige Normalform bestimmen, und somit entscheiden, ob

zwei Produkte gleich sind, oder nicht. In dem speziellen Fall der Kreiszahlen läßt sich das auch durch bloßes Ausrechnen als Zahlen in $\mathbf{Q}(\epsilon_n)$ feststellen. Der Algorithmus läßt sich aber durchaus verallgemeinern, da die verwendeten Strategien im wesentlichen auf die im ersten Kapitel vorgestellten Strukturen zurückgreifen (Tensorprodukte, $\mathbf{Z}[\sigma]$-Moduln, Zeilenfaktormoduln, Differenzenmoduln und $M\&n$-Systeme), die in der Regel weitaus allgemeiner untersucht wurden, als dies speziell für Kreiseinheiten notwendig war.

Literaturverzeichnis

[1] H. Bass: *Generators and relations for cyclotomic units.* In: Nagoya Mathematical Journal 27 (1966), 401-407.

[2] M. Conrad: *Gruppenringe und ihre Anwendung auf die Gruppe der zyklotomischen Einheiten.* Diplomarbeit an der Universität des Saarlandes, Saarbrücken, 1992.

[3] C. W. Curtis, Irving Reiner: *Representation Theory of Finite Groups and Associative Algebras*, Interscience Publishers, New York, London, Sydney 1966.

[4] V. Ennola: *On Relations between Cyclotomic Units.* In: Journal of Number Theory 4 (1972), 236-247.

[5] R. Gold and J. Kim: *Bases for cyclotomic units.* In: Compositio Mathematica 71 (1989), 13-28.

[6] T. W. Hungerford: *Algebra*, Springer-Verlag, New York 1984.

[7] H. Hasse: *Zahlentheorie*, Akademie Verlag, Berlin 1963.

[8] R. Kučera: *On bases of the Stickelberger ideal and of the group of circular units of a cyclotomic field.* In: Journal of Number Theory 40 (1992), 284-316.

[9] J. Neukirch: *Algebraische Zahlentheorie*, Springer-Verlag, Berlin, Heidelberg 1992.

[10] J. Neukirch: *Klassenkörpertheorie*, Bibliographisches Institut AG, Mannheim 1969.

[11] K. Ramachandra: *On the units of cyclotomic fields.* In: Acta Arithmetica 12 (1966), 165–173.

[12] C.-G. Schmidt: *Die Relationsfaktorgruppen von Stickelberger-Elementen und Kreiszahlen.* In: Journal für die reine und angewandte Mathematik 315 (1980), 60–72.

[13] C.-G. Schmidt: *Die Relationen von Gaußschen Summen und Kreiseinheiten.* In: Archiv der Mathematik (Basel) 31 (1978/1979), 457-463.

[14] SIMATH: *Ein Computeralgebrasystem für algorithmische Zahlentheorie.* http://emmy.math.uni-sb.de/∼simath.

[15] W. Sinnot: *On the Stickelberger ideal and the circular units of a cyclotomic field.* In: Annals of Mathematics 108 (1978), 107-134.

[16] L. C. Washington: *Introduction to Cyclotomic Fields*, Springer-Verlag, New York 1982.

[17] E. Weiss: *Algebraic number theory*, McGraw-Hill, New York 1963.

[18] K. Yamamoto: *The gap group of multiplicative relationships of Gaussian sums.* In: Symposia Mathematica, 15 (1975), 427-440.