Endliche Untergruppen der Einheitengruppe ganzzahliger Gruppenringe

Von der Universität Stuttgart
zur Erlangung der Würde eines
Doktors der Naturwissenschaften
genehmigte Abhandlung

von

Alexander Zimmermann

geboren in Stuttgart

Hauptberichter:	Prof. Dr. rer. nat. K. W. Roggenkamp
Mitberichter:	Dr. rer. nat. habil. W. Kimmerle
Tag der Einreichung:	27. August 1992
Tag der mündlichen Prüfung:	7. Oktober 1992

Mathematisches Institut B der Universität Stuttgart

1 Einleitung

Gruppenringe sind ein Hauptgegenstand des Interesses der Darstellungstheorie endlicher Gruppen. Eines der zentralen Themen ist die Frage, welche Eigenschaften einer abstrakten Gruppe in ihrem Gruppenring gemessen werden können. Das Isomorphieproblem ganzzahliger Gruppenringe ist die Frage nach der stärksten Antwort, nämlich ob aus der Isomorphie der ganzzahligen Gruppenringe $\mathbb{Z}G \simeq \mathbb{Z}H$ zweier Gruppen G und H als augmentierte Algebren auf die Isomorphie der Gruppen G und H geschlossen werden kann. G. Higman bearbeitete in seiner Dissertation [Hi-39] dieses Problem erstmals. H. Zassenhaus vermutete ([Se-83]), daß aus $\mathbb{Z}G = \mathbb{Z}H$ als augmentierte Algebren für eine geeignete Einheit $a \in U(\mathbb{Q}G)$ sogar $G = a \cdot H \cdot a^{-1}$ folgt. K. W. Roggenkamp und L. L. Scott konstruierten in [RS-87c] eine Serie von metabelschen Gegenbeispielen zu dieser Vermutung: Die Gruppe der oberen Dreiecksmatrizen über dem Körper mit 4 Elementen mit Einsen in der Hauptdiagonalen, die geeignet auf der zyklischen Gruppe der Ordnung $3 \cdot 5 \cdot 7$ operiert, liefert ein solches. In einer Reihe von Arbeiten wurden in den letzten 10 Jahren wegweisende Ergebnisse von K. W. Roggenkamp und L. L. Scott [RS-87a, RS-86, RS-87b, Sc-85] sowie von A. Weiss [Wei-88] erzielt. Der Anwendung und Erweiterung zweier dieser Resultate ist der erste Teil der vorliegenden Arbeit gewidmet.

Genauer lautet das Hauptresultat des Kapitels 2:

Satz 1 *Sei $\mathcal{P}$ eine endliche Menge von n rationalen Primzahlen und sei*

$$G = H \times \prod_{p \in \mathcal{P}} G_p$$

ein direktes Produkt von $n+1$ Gruppen paarweiser relativ primer Ordnung, so daß für jedes p die Gruppen G_p p–auflösbar mit $O_{p'}(G_p) = 1$ sind. Eine p–Sylowuntergruppe von G_p sei mit P_p bezeichnet. $\mathbb{Z}H$ erfülle die Zassenhausvermutung. Weiterhin sei E eine endliche Gruppe mit abelschem Normalteiler N und $E/N \simeq G$, für den die Beziehung

$$(|N|, \frac{|G|}{\prod_{p \in \mathcal{P}} |P_p|}) = 1$$

gilt. Dann hat das Isomorphieproblem für $\mathbb{Z}E$ eine positive Antwort.

Ist G nilpotent, so ergibt sich das Resultat von K. W. Roggenkamp und L. L. Scott aus [RS-86, Sc-85] für $\mathbb{Z}$ als Koeffizientenring als Spezialfall. Genauer bewiesen K. W. Roggenkamp und L. L. Scott in [RS-86, Sc-85], daß für eine endliche Gruppe E mit abelschem Normalteiler N und nilpotentem E/N aus $RE = RE'$ für einen Dedekindbereich R, in dem kein Primteiler der Gruppenordnung invertierbar ist, die Isomorphie von E und E' folgt.

Die Frage nach der Gültigkeit der Zassenhausvermutung war lange Zeit und ist immer noch Leitfaden für Arbeiten über das Isomorphieproblem. Aus diesem Grunde sind viele positive Ergebnisse erzielt worden. Einige Beispiele seien explizit genannt: Das diesbezüglich weitreichendste Resultat ist das Ergebnis von K. W. Roggenkamp und L. L. Scott aus [RS-87b]. Für ganzzahlige Gruppenringe vieler einfacher Gruppen kann die Gültigkeit der Zassenhausvermutung aus der Untersuchung von Brauer-Bäumen abgeleitet werden [Ki-92b, §3]. Diese Gruppen eignen sich als Gruppen H ebenso wie Gruppen $A \wr S_n$ mit abelschem oder symmetrischen A und $n \in \mathbb{N}$ nach A. Giambruno, S.K. Sehgal, A. Valenti [GVS-91] und A. Valenti [Va-92].

Das Resultat von A. Weiss ([Wei-88]) zeigt für p–Gruppen G die Konjugiertheit endlicher Untergruppen U der Einheitengruppe p–adischer Gruppenringe zu einer Untergruppe einer Gruppenbasis[1], falls U Augmentation 1 besitzt.

Gilt dies auch ganzzahlig?

Ist genauer jede endliche Untergruppe der Einheitengruppe $V(\mathbb{Z}G)$[2] konjugiert zu einer Untergruppe einer Gruppenbasis, falls sie dies in $V(\hat{\mathbb{Z}}_q G)$ für jede Primzahl q und auch in $V(\mathbb{Q}G)$ ist? Diese Frage läßt sich natürlich sinnvoll nicht nur für p–Gruppen G sondern für alle Gruppen G, deren ganzzahliger Gruppenring der Zassenhausvermutung genügt, stellen. Andere Einheiten von RG sind in diesem Zusammenhang nicht relevant, da $U(RG) = V(RG) \times U(R)$ ([RS-87a, (1.1.1)]). Wir sprechen im Fall der Konjugiertheit in $V(\hat{\mathbb{Z}}_q G)$ für alle Primzahlen q beziehungsweise Konjugiertheit in $V(\mathbb{Q}G)$ von lokaler beziehungsweise von rationaler Konjugiertheit, während Konjugiertheit in $V(\mathbb{Z}G)$ mit ganzzahliger Konjugiertheit bezeichnet wird.

Man kann natürlich auch fragen, in wievielen Gruppenbasen eine feste Untergruppe von G liegt. Dazu finden sich in der Literatur zwei Beispiele:

[1] Eine Gruppenbasis von $\mathbb{Z}G$ ist eine Untergruppe der Einheitengruppe von $\mathbb{Z}G$ der Augmentation 1, die eine $\mathbb{Z}$-Basis von $\mathbb{Z}G$ bildet.

[2] Dabei bezeichnet $V(RG)$ die Gruppe der Einheiten mit Augmentation 1 im Gruppenring RG über dem Integritätsbereich R.

I. Hughes und K. E. Pearson ([HP-72]) bewiesen, daß in dem ganzzahligen Gruppenring der symmetrischen Gruppe der Ordnung 6 eine Involution existiert, die nicht in einer Gruppenbasis liegt. Sie ist aber sogar 2-adisch nicht zu einem Element einer ganzzahligen Gruppenbasis konjugiert.

C. Polcino Milies bewies in [PM-74], daß im ganzzahligen Gruppenring der Diedergruppe mit 8 Elementen zwei Konjugationsklassen von Gruppenbasen existieren und daß alle Einheiten endlicher Ordnung in einer Gruppenbasis liegen.

Im zweiten Teil der vorliegenden Arbeit werden für alle Diedergruppen von 2-Potenzordnung sowohl die Anzahl der Involutionen bis auf Konjugation als auch die Anzahl der Gruppenbasen bis auf Konjugation bestimmt, in der eine feste Involution liegt. Ebenso werden bis auf Konjugation alle Gruppenbasen explizit angegeben.

In [Ro-89, RT-92] wird eine von L. L. Scott und K. W. Roggenkamp entwickelte Theorie dargestellt, um die $V(\mathbb{Q}G)$–Konjugationsklasse einer festen Untergruppe $U \leq G$ auf Zerfall in $V(\mathbb{Z}G)$–Konjugationsklassen zu untersuchen.

Im einzelnen lassen sich die Ergebnisse aus [Ro-89], falls der Zentralisator $C_{\mathbb{Z}G}(U)$ von U in $\mathbb{Z}G$ abelsch ist und $\mathbb{Z}G$ lokal freie Kürzbarkeit erlaubt, wie folgt zusammenfassen. Für eine p–Gruppe G parametrisiert der Kern $Cl_{\mathbb{Z}G}(C_{\mathbb{Z}G}(U))$ des natürlichen Homomorphismus von der Klassengruppe $Cl(C_{\mathbb{Z}G}(U))$ des Zentralisators von U in $\mathbb{Z}G$ in die Klassengruppe $Cl(\mathbb{Z}G)$ von $\mathbb{Z}G$ die Menge der Konjugationsklassen einer $U(\mathbb{Q}G)$-Konjugationsbahn von U in $\mathbb{Z}G$. Diese Aussage verwendet den Satz von A. Weiss aus [Wei-88], der von K. W. Roggenkamp in [Ro-92] und unabhängig von G. Thompson unter Anleitung von L. L. Scott in [Th-89] verallgemeinert wurde. Ist G keine p–Gruppe, so liefert die Theorie Ergebnisse für die Anzahl der $V(\mathbb{Z}G)$–Konjugationsklassen lokal und gleichzeitig rational zu einer festen Untergruppe U von G konjugierter Untergruppen von $V(\mathbb{Z}G)$. Diese Theorie lehnt sich an die von A. Fröhlich entwickelte Theorie von Picardgruppen von Ordnungen ([Fr-73]) an.

Genauer untersucht man Isomorphieklassen von $\mathbb{Z}(U \times G^{op})$-Moduln[3] M mit $\mathbb{Q} \cdot M \simeq \mathbb{Q}G$ als $\mathbb{Q}(U \times G^{op})$-Moduln und $M \simeq \mathbb{Z}G$ als $\mathbb{Z}G^{op}$-Moduln. Man kann annehmen, daß $\mathbb{Q}M = \mathbb{Q}G$ ist. Dann ist $M \subseteq \mathbb{Q}G$ und sogar

[3]d.h. U operiert von links durch Multiplikation und G operiert von rechts durch Multiplikation mit dem Inversen.

$M = a \cdot \mathbb{Z}G$ für eine Einheit a von $\mathbb{Q}G$ als $\mathbb{Z}(U \times G^{op})$-Moduln. Man zeigt, daß zwei dieser Bimoduln $a \cdot \mathbb{Z}G$ und $a' \cdot \mathbb{Z}G$ genau dann isomorph sind, wenn $a = a' \cdot u$ für eine Einheit u von $\mathbb{Z}G$. Somit parametrisieren diese Isomorphieklassen von Moduln die Konjugationsklassen von Einbettungen von U in $V(\mathbb{Z}G)$, die durch Konjugationen mit Einheiten von $\mathbb{Q}G$ induziert werden. Man zeigt, daß $\hat{\mathbb{Z}}_p M \simeq \hat{\mathbb{Z}}_p G$ als $\hat{\mathbb{Z}}_p(U \times G^{op})$-Modul für alle Primzahlen p genau dann gilt, wenn $M = J \cdot \mathbb{Z}G$ für ein Ideal J mit Isomorphieklasse (J) in $Cl_{\mathbb{Z}G}(C_{\mathbb{Z}G}(U)) := ker(Cl(C_{\mathbb{Z}G}(U)) \longrightarrow Cl(\mathbb{Z}G))$. Dem Homomorphismus $Cl_{\mathbb{Z}G}(C_{\mathbb{Z}G}(G)) \longrightarrow Cl_{\mathbb{Z}G}(C_{\mathbb{Z}G}(U))$ entspricht hier die Einschränkung des $\mathbb{Z}(G \times G^{op})$-Moduls $J \cdot \mathbb{Z}G$ für ein Gitter J mit stabiler Isomorphieklasse in $Cl_{\mathbb{Z}G}(C_{\mathbb{Z}G}(G))$ als $\mathbb{Z}(U \times G^{op})$-Modul. Aus dieser Beobachtung erschließt man, daß eine Konjugationsklasse rational zu U konjugierter Untergruppen genau dann aus in lokal zu G konjugierten Gruppenbasen liegenden Elementen besteht, falls ihr zugehöriges Ideal im Bild des Homomorphismus der Klassengruppen, wie oben angegeben, liegt.

Diese Untersuchung wird in der vorliegenden Arbeit auf ganzzahlige Gruppenringe von Diedergruppen D_q mit der Ordnung $2q \in \{u \in \mathbb{N} | u = 2p$ oder $u = 2^{n+1}, n \in \mathbb{N}, p$ prim$\}$ und Untergruppen U der Ordnung 2 angewandt.

Die Klassengruppe des ganzzahligen Gruppenrings von Diedergruppen D_q der Ordnung $2q \in \{2p, 2^{n+1} \mid p$ prim$, n \in \mathbb{N}\}$ ist auf zahlentheoretische Größen reduziert durch Arbeiten von M. P. Lee [Lee-64], deren Arbeit von S. Galovich, I. Reiner und S. Ullom in [GRU-72] und Cassou-Nouguès in [CN-76] verallgemeinert wurde, im Fall einer Primzahl q sowie von A. Fröhlich, M. E. Keating und S. M. J. Wilson ([FKW-74]) im Fall einer 2-Potenz q. Die Klassengruppe des Zentrums von $\mathbb{Z}D_p$ und das Bild des Normhomomorphismus nach der Klassengruppe des maximalen reellen Teilkörpers des Körpers der p-ten Einheitswurzeln über $\mathbb{Q}$, $Cl(\mathbb{Z}[\eta(p)])$, wurde von A. Fröhlich, I. Reiner und S. Ullom in [FRU-74] bestimmt. Den Fall $\mathbb{Z}D_m$ für alle natürlichen Zahlen m behandelten diesbezüglich S. Endo, T. Miyata und K. Sekiguchi in [EMS-82]. Teile dieser Ergebnisse waren T. Miyata schon 1987 bekannt ([Miy-80]). H. Cohn vermutete ([ACH-65, Co-60]), daß $Cl(\mathbb{Z}D_{2^n}) = 1$ für alle $n \in \mathbb{N}$ ist.[4] A. Fröhlich, I. Reiner und S. Ullom zeigten in [FRU-74] die Isomorphie von $Cl(Z(\mathbb{Z}D_p))$ und $Picent(\mathbb{Z}D_p)$, S. Endo, T. Miyata und K.

[4] M. Pohst, P. Roquette und B. Volkmann danke ich für ihre Antwort auf meine Frage nach Ergebnissen zur Cohnschen Vermutung.

Sekiguchi bewiesen die Isomorphie von $Cl(Z(\mathbb{Z}D_{2^n}))$ und $Picent(\mathbb{Z}D_{2^n})$ in [EMS-82].

Es ergibt sich zum Vorkommen von Involutionen im Gruppenring $\mathbb{Z}D_{2^n}$ der

Satz 2 *Sei D_{2^n} die Diedergruppe mit 2^{n+1} Elementen.*

1. *Die $V(\mathbb{Q}D_{2^n})$–Bahn einer nicht zentralen Involution $b \in D_{2^n}$ zerfällt in $2^{n-1} \cdot \prod_{k \leq n} h_k^+$ Konjugationsklassen über $\mathbb{Z}D_{2^n}$, wobei h_k^+ die Klassenzahl des maximalen reellen Teilkörpers des 2^k–ten Kreisteilungskörpers über $\mathbb{Q}$ ist.*

2. *Von diesen Konjugationsklassen bestehen 2^{n-1} Klassen aus Involutionen, die in Gruppenbasen liegen.*

3. *$Cl(C_{\mathbb{Z}D_{2^n}}(b)) \simeq C_{2^{n-1}} \times \prod_{k \leq n} Cl(\mathbb{Z}[\zeta_{2^k} + \zeta_{2^k}^{-1}])^2$, wobei $\zeta_{2^n}^{2^{n-1}} + 1 = 0$.*

4. *$Cl_{\mathbb{Z}D_{2^n}}(C_{\mathbb{Z}D_{2^n}}(b)) \simeq C_{2^{n-1}} \times \prod_{k \leq n} Cl(\mathbb{Z}[\zeta_{2^k} + \zeta_{2^k}^{-1}])$.*

Eine unmittelbare Konsequenz ist

Korollar 1 *Die Vermutung von H. Cohn ([ACH-65]) ist genau dann richtig, wenn für alle $n \in \mathbb{N}$ jede Involution von $\mathbb{Z}D_{2^n}$ in einer Gruppenbasis liegt.*

Satz 2 ergänzt die Untersuchung von S. Endo, T. Miyata und K. Sekiguchi ([EMS-82]), die den Isomorphietyp der äußeren zentralen Automorphismengruppe[5] von $\mathbb{Z}D_m$ für alle Diedergruppen D_m der Ordnung $2m$ mit $m \in \mathbb{N}$ bestimmt haben. Dort wurde bewiesen, daß

$$Outcent(\mathbb{Z}D_{2^n}) \simeq C_{2^{n-1}} \times C_{2^{n-2}}.$$

(Ob die Arbeit von H. Weber [Web-1886] den Autoren von [EMS-82] bekannt war, wird aus der Arbeit [EMS-82] nicht klar, denn in [EMS-82] wird zudem noch eine Untergruppe der 2-Sylowuntergruppe von $\prod_{k \leq n} Cl(\mathbb{Z}[\zeta_{2^k} + \zeta_{2^k}^{-1}])$ als direkter Faktor angefügt. H. Weber zeigt jedoch in [Web-1886], daß die

[5]Ein Ringautomorphismus heißt zentral, wenn er das Zentrum des Rings punktweise fixiert. Ein Gruppenautomorphismus heißt zentral, wenn seine natürliche Erweiterung als Automorphismus des ganzzahligen Gruppenrings zentral ist.

2-Sylowuntergruppe von $Cl(\mathbb{Z}[\zeta_{2^k}+\zeta_{2^k}^{-1}])$ für alle Zahlen k einelementig ist.) Die Klassengruppe des Zentrums von $\mathbb{Z}D_{2^n}$ wurde in [EMS-82] zu

$$Cl(Z(\mathbb{Z}D_{2^n})) \simeq Outcent(\mathbb{Z}D_{2^n}) \times \prod_{k\leq n} Cl(\mathbb{Z}[\zeta_{2^k}+\zeta_{2^k}^{-1}])$$

berechnet. Damit liegt b in genau 2^{n-2} Repräsentanten verschiedener Konjugationsklassen von Gruppenbasen.

Erzeugende Elemente für $Outcent(\mathbb{Z}D_{2^n})$ wurden in [EMS-82] konkret nicht angegeben. Unter Verwendung von Satz 2 zeigen wir in der vorliegenden Arbeit den

Satz 3 *Die äußere zentrale Automorphismengruppe $Outcent(\mathbb{Z}D_{2^n})$ des ganzzahligen Gruppenrings der Diedergruppe D_{2^n} mit 2^{n+1} Elementen wird erzeugt von der Konjugation mit $a-b+1$, einem Automorphismus der Ordnung 2^{n-1} modulo inneren Automorphismen, und der Konjugation mit $1+b\cdot(a+a^{-1})$, einem Automorphismus der Ordnung 2^{n-2} modulo inneren Automorphismen. Dabei ist a ein Element der Ordnung 2^n in D_{2^n} und b eine nicht zentrale Involution in D_{2^n}.*

Unter Verwendung des Satzes von Roggenkamp und Scott [RS-87a] können hiermit für jedes $n \in \mathbb{N}$ Repräsentanten aller Konjugationsklassen von Gruppenbasen angegeben werden. J. Whitcomb untersuchte den Fall $n=2$ schon in [Wh-68] und erhielt eine zweite Gruppenbasis durch Konjugation mit $1+a+ba$. Diese Einheit kann durch einen Ringautomorphismus auf $a-b+1$ abgebildet werden. Eine globale Übersicht über das Konjugationsverhalten von Gruppenbasen ist in [Wh-68] im Gegensatz zu der Arbeit von C. Polcino Milies und der vorliegenden Diskussion nicht erzielt worden.

Im Beweis des Satzes 2 ist ein zentraler Punkt die Existenz eines Automorphismus σ von $\mathbb{Z}C_{2^n}$, der ein Erzeugendes a von C_{2^n} auf $-a$ abbildet.[6] Identifiziert man a mit der Drehung um den Winkel $2\pi/2^n$, so kommutiert σ mit der Operation von b, einer nicht zentralen Involution von D_{2^n}. Damit ist σ ein Automorphismus von

$$H^0(<b>, \mathbb{Z}D_{2^n}) = C_{\mathbb{Z}D_{2^n}}(b).$$

Außerdem ist

$$H^0(<\sigma>, \mathbb{Z}D_{2^n}) = \mathbb{Z}D_{2^{n-1}}$$

[6] C_m bezeichne die zyklische Gruppe mit m Elementen.

mit der kanonischen Identifikation $C_{2^{n-1}} \leq C_{2^n}$. Diese Beobachtung macht das Problem Induktionsmethoden zugänglich und wird im Beweis von Lemma 5 und im Beweis von Lemma 9 an zwei zentralen Stellen wesentlich verwendet.

Der kompliziertere Fall ungerader Diedergruppen der Ordnung $2 \cdot m$, wobei $(2, m) = 1$ wird in Kapitel 3.9 für Primzahlen m begonnen. Es sei für eine abelsche Gruppe A mit $A_{[2]}$ der Kern des durch $a \longrightarrow a^2$ für alle $a \in A$ definierten Endomorphismus von A bezeichnet. $\mathbb{Z}[\eta(p)]$ sei der Ring der algebraisch ganzen Zahlen im maximalen reellen Teilkörper des p-ten Einheitswurzelkörpers über $\mathbb{Q}$. Es konnte der folgende Satz gezeigt werden.

Satz 4 *Sei D_p die Diedergruppe mit $2p$ Elementen, wobei p eine ungerade Primzahl ist.*

1. *Es existieren in $\mathbb{Z}D_p$ genau*

$$\frac{|Cl(\mathbb{Z}[\eta(p)]C_2)|}{|Cl(\mathbb{Z}[\eta(p)])|}$$

   Konjugationsklassen von Involutionen, die lokal und rational zu b konjugiert sind.

2. *Eine Involution $b \in D_p$ ist in genau $\frac{p-1}{2}$ Repräsentanten von Konjugationsklassen von Gruppenbasen enthalten.*

3. *Von den Konjugationsklassen lokal und rational zu b konjugierter Involutionen in $\mathbb{Z}D_p$ bestehen genau $|(Cl(\mathbb{Z}[\eta(p)]))_{[2]}|$ Konjugationsklassen aus Involutionen, die in einer Gruppenbasis liegen.*

4. *Falls $p \in \{(2nq)^2 + 1 | n \in \mathbb{Z}, n \geq 2, q\mathbb{Z} \in Spec(\mathbb{Z})\}$ Primzahl ist, existiert eine Konjugationsklasse von Involutionen, deren Elemente in $V(\hat{\mathbb{Z}}_r D_p)$ für alle Primzahlen r konjugiert zu b sind, die aber in keiner Gruppenbasis von $\mathbb{Z}D_p$ liegen.*

Beispiele für Primzahlen $p = (2qn)^2 + 1$ sind einfach zu finden und alle Zahlen in $\{257, 401, 577, 1297, 1601, 2917, 3137, 4357, 7057, 8101\}$ sind Primzahlen von der obigen Form. Zum Beweis des letzten Punktes im Satz 4 wird im wesentlichen nur die Arbeit [ACH-65] angewendet. Damit erhält man leicht weitere Beispiele aus den Tafeln von K. Schaffenstein in [Sch-28]

oder aus den Abschätzungen von H. Hasse in [Ha-65]. Sehr viele Konjugationsklassen lokal zu b konjugierter Involutionen in $V(\mathbb{Z}D_p)$ (nämlich wenigstens $4 \cdot 3 \cdot 5 \cdot 179 \cdot 223 \cdot 6961 = 16671734220$) erhält man mit der Arbeit [CW-82, SWW-83] von G. Cornell und L. C. Washington sowie von E. Seah, L. C. Washington und H. Williams für $p = 11290018777$. Von diesen Konjugationsklassen bestehen höchstens 4 aus in Gruppenbasen liegenden Elementen. Die Arbeiten [CW-82, SWW-83] verwenden wesentlich Computerberechnungen.

Durch Verwendung des Computeralgebra-Programms 'maple V' konnte unter Anwendung eines Satzes von van der Linden ([Ma-78, vdL-82]) berechnet werden, daß es in $\mathbb{Z}D_{37}$ und, falls man die verallgemeinerte Riemannschen Vermutung voraussetzt, auch in $\mathbb{Z}D_{101}$ Involutionen gibt, die lokal konjugiert zu einer Involution in einem festen $D_p \subset \mathbb{Z}D_p$ sind, ganzzahlig jedoch in keiner Gruppenbasis liegen.

Hier ist jedoch auf die prinzipielle Schwierigkeit hinzuweisen, die sich oft bei Beweisen ergibt, die an wesentlicher Stelle Gebrauch von elektronischen Rechenmaschinen machen. Dabei ist ein "Verstehen" im Sinne von M. Atiyah[7] häufig nur eingeschränkt möglich.

Die Gliederung der Arbeit ist wie folgt: Kapitel 2 befaßt sich mit dem Beweis von Satz 1 während Kapitel 3 den Beweis der Sätze 2—4 zum Thema hat.

In Kapitel 2.1 wird zuerst der Fall zerfallender Erweiterungen halbeinfacher Normalteiler mit Gruppen, deren ganzzahliger Gruppenring der Zassenhausvermutung genügt, behandelt.

Automorphismen von $\mathbb{Z}G$, die von Automorphismen von $\mathbb{Z}E$ induziert werden, stehen im Mittelpunkt von Kapitel 2.2. Das Ergebnis dieses Kapitels stammt von K. W. Roggenkamp. Teile davon resultieren aus Arbeiten von L. L. Scott und K. W. Roggenkamp.

Wird $\mathcal{P}$ festgehalten, so genügt der Schnitt aller Normalteiler N, die den Voraussetzungen des Satzes 1 genügen, wieder den Voraussetzungen. Der Beweis dieser Aussage wird in Kapitel 2.3 geführt.

Satz 1 wird dann in Kapitel 2.4 bewiesen.

Der Inhalt des Kapitels 2 wurde in [RZ-91] veröffentlicht[8].

[7](cf. The Mathematical Intelligencer Vol. 6 No. 1 (1984).)

[8]Der Fakultät Mathematik sei für die Genehmigung der Veröffentlichung gedankt.

In Kapitel 3.2 wird der Zentralisator einer nicht zentralen Involution $b \in D_{2^n}$, der Diedergruppe der Ordnung 2^{n+1}, in $\mathbb{Z}\!\!\mathbb{Z}D_{2^n}$ iterativ als Pullback durch die Wedderburn-Komponenten von $\mathbb{Z}\!\!\mathbb{Z}D_{2^n}$ dargestellt.

In Kapitel 3.3 werden die Vorbereitungen zur Bestimmung einer oberen Schranke für die Klassenzahl von $C_{\mathbb{Z}\!\!\mathbb{Z}D_{2^n}}(b)$ weit vorangetrieben. Außerdem werden Vorarbeiten für die Diskussionen in Kapitel 3.7 geleistet. Dabei wird ein zahlentheoretisches Lemma bewiesen, das garantiert, daß in den Pullbackdiagrammen aus Kapitel 3.2 nicht alle Einheiten des gemeinsamen Quotienten der beiden Faktoren Bilder von Einheiten eines der beiden Faktoren, nämlich des Bildes von $C_{\mathbb{Z}\!\!\mathbb{Z}D_{2^n}}(b) \cdot \frac{1}{2}(1 + a^{2^{n-1}})$ im größten Wedderburnblock von $\mathbb{Z}\!\!\mathbb{Z}D_{2^{n-1}} = \mathbb{Z}\!\!\mathbb{Z}D_{2^n} \cdot \frac{1}{2}(1 + a^{2^{n-1}})$, sind.

Daß die nun leicht abzuleitende obere Schranke auch den tatsächlichen Wert liefert, wird in Kapitel 3.4 gezeigt, indem $C_{\mathbb{Z}\!\!\mathbb{Z}D_{2^n}}(b) \simeq \hat{C}(n) \otimes_{\mathbb{Z}} \mathbb{Z}\!\!\mathbb{Z}C_2$ für einen geeigneten Ring $\hat{C}(n)$ verwendet wird. In diesem Kapitel werden idèletheoretische Methoden benützt. Genauer werden die Mayer-Vietoris-Sequenzen der Pullbackdiagramme von $C_{\mathbb{Z}\!\!\mathbb{Z}D_{2^{n-1}}}(b)$ und von $C_{\mathbb{Z}\!\!\mathbb{Z}D_{2^n}}(b) \cdot \frac{1+a^{2^{n-1}}}{2}$ bezüglich des Quasiidempotents $1+b$ verglichen: Da $C_{\mathbb{Z}\!\!\mathbb{Z}D_{2^{n+1}}}(b) \cdot \frac{1+a^{2^n}}{2}$ eine Teilordnung von $C_{\mathbb{Z}\!\!\mathbb{Z}D_{2^n}}(b)$ in derselben Algebra ist, existieren Homomorphismen zwischen den Gruppen in den Mayer-Vietoris-Sequenzen der beiden Pullbackdiagramme. Diese führen auf die Diskussion des kommutativen Diagramms

$$
\begin{array}{ccccccccc}
 & & 1 & \to & U(\hat{B}_n) & \stackrel{\iota_n}{\to} & U(\hat{C}(n))/ < a^{2^{n-1}} > & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow \pi_B & & \downarrow \pi'_C & & \\
1 & \to & C_2 & \to & U(\hat{\overline{B}}_n) & \to & U(\hat{\overline{C}}(n))/ < a^{2^{n-1}} > & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & K_n & \to & \frac{U(\hat{\overline{B}}_n)}{\pi_B(U(\hat{B}_n))} & \to & \frac{U(\hat{\overline{C}}(n))}{\pi_C(U(\hat{C}(n)))} & \to & 1 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 1 & & 1 & &
\end{array},
$$

wobei die folgenden Bezeichnungen gewählt sind:

$$
\begin{aligned}
\hat{B}_n &:= C_{\mathbb{Z}\!\!\mathbb{Z}D_{2^{n+1}}}(b) \cdot \frac{1 + a^{2^n}}{2} \cdot \frac{1 + b}{2}, \\
\hat{C}(n) &:= C_{\mathbb{Z}\!\!\mathbb{Z}D_{2^n}}(b) \cdot \frac{1 + b}{2}, \\
\hat{\overline{B}}_n &:= \hat{B}_n / 2\hat{B}_n,
\end{aligned}
$$

$$\hat{\overline{C}}(n) \;:=\; \hat{C}(n)/2\hat{C}(n).$$

Dabei wird $a^{2^{n-1}} \in D_{2^n}$ mit seinem Bild in $\hat{C}(n)$ identifiziert. Weiter ist K_n der Kern des natürlichen Epimorphismus zwischen der Klassengruppe von $C_{\mathbb{Z}D_{2^{n+1}}}(b) \cdot \frac{1+a^{2^n}}{2}$ auf die Klassengruppe von $C_{\mathbb{Z}D_{2^n}}(b)$. Verwendet man jetzt noch, daß aus Kapitel 3.3 die Beziehung

$$Cl(C(n)) = Cl(B(n-1)) \times Cl(\mathbb{Z}[\zeta_{2^n} + \zeta_{2^n}^{-1}]C_2)$$

nachgewiesen wurde, lassen sich dann die Untersuchungen auf die Berechnung der Größen $Cl(\mathbb{Z}[\zeta_{2^k} + \zeta_{2^k}^{-1}]C_2)$ für alle $k \in \mathbb{N}$ zurückführen. Man zeigt genauer (Lemma 9), daß das nicht triviale Element im Kern der Abbildung

$$\rho_n : U(\hat{\overline{B}}_n) \longrightarrow U(\hat{\overline{C}}(n))/ < a^{2^{n-1}} >$$

nicht im Bild der Abbildung π_B liegt. Damit ist dann

$$\iota_n(\pi_B(U(\hat{B}_n))) \subseteq \pi'_C(U(\hat{C}_n)/ < a^{2^{n-1}} >),$$

wenn ι_n den natürlichen Homomorphismus von der Einheitengruppe $U(\hat{B}_n)$ nach $U(\hat{C}(n))/ < a^{2^{n-1}} >$ via der Einbettung von $\hat{B}_n$ in $\hat{C}(n)$ bezeichnet. Da ι_n aber ein Isomorphismus ist, ist ρ_n surjektiv und das Schlangenlemma zeigt, daß K_n zweielementig sein muß.

Die Berechnung von $Cl(\mathbb{Z}[\zeta_{2^k} + \zeta_{2^k}^{-1}]C_2)$ für alle $k \in \mathbb{N}$ wird in Kapitel 3.5 durchgeführt und die Berechnung von $Cl(C_{\mathbb{Z}D_{2^n}}(b))$ wird damit auf zahlentheoretische Größen zurückgeführt. Genauer wird gezeigt, daß

$$Cl(\mathbb{Z}[\zeta_{2^n} + \zeta_{2^n}^{-1}] < b >) = Cl(\mathbb{Z}[\zeta_{2^n} + \zeta_{2^n}^{-1}])^2.$$

Die Berechnung von $Cl_{\mathbb{Z}D_{2^n}}(C_{\mathbb{Z}D_{2^n}}(b))$ und damit die Bestimmung der Anzahl der Konjugationsklassen von Involutionen erfolgt in Kapitel 3.6 und geht weitgehend unter Verwendung universeller Argumente, da die Klassengruppe der Diedergruppe D_{2^n} gleich der einer maximalen Ordnung in $\mathbb{Q}D_{2^n}$ ist.

In Kapitel 3.7 wird die Anzahl der Konjugationsklassen von Gruppenbasen, die einen Repräsentanten besitzen, der b enthält, bestimmt. Wieder kommen idèletheoretische Methoden, diesmal wesentlich, zum Einsatz.

Mit den dadurch gewonnenen Kenntnissen ist es möglich, die äußere Automorphismengruppe von $\mathbb{Z}D_{2^n}$ explizit anzugeben. Dies wird in Kapitel 3.8

durchgeführt. Dabei ist der Fall $n = 2$ und der Fall $n = 3$ zuerst elementar durchzuführen, danach ist der allgemeine Fall eine einfache Folgerung.

Kapitel 3.9 ist der Untersuchung ganzzahliger Gruppenringe ungerader Diedergruppen gewidmet. Eine besondere Schwierigkeit ist dabei die Bestimmung der Klassenzahl von $\mathbb{Z}[\zeta_p+\zeta_p^{-1}] < b >$, für die keine allgemeine Formel hergeleitet werden konnte.

Im Anhang finden sich die Computerprogramme und die Ergebnisse der damit durchgeführten Berechnungen für einige kleine Diedergruppen D_p.

An dieser Stelle möchte ich Herrn Professor Dr. K. W. Roggenkamp meinen aufrichtigen Dank nicht nur für zahlreiche Hinweise, den Inhalt des für Satz 1 unentbehrlichen Kapitels 2.2, sondern auch für die Auswahl des interessanten Themas, der stetigen Anteilnahme an dem Fortgang der Arbeit und der freien Arbeitsatmosphäre am 3. Lehrstuhl des Mathematischen Instituts B zum Ausdruck bringen.

Inhaltsverzeichnis

2 Isomorphie von Gruppenringen

2.1 Halbeinfache Normalteiler

Der erste Schritt zu unserem Ziel, das Isomorphieproblem einer positiven Lösung für einige Gruppen zuzuführen, wird das folgende Lemma sein. Ein R–Modul M, dessen R–Operation durch $\sigma \in Aut(R)$ getwistet[9] ist, wird mit ${}^{\sigma}M$ bezeichnet. Ein $R-S$–Bimodul M, dessen R–Operation mit $\sigma \in Aut(R)$ und dessen S–Operation mit $\tau \in Aut(S)$ getwistet ist, wird mit ${}_{\sigma}M_{\tau}$ bezeichnet ([Fr-73]).

Lemma 1 *Sei G eine endliche Gruppe und sei M ein einfacher $\mathbb{Z}G$–Modul, dann ist für jeden zentralen Automorphismus σ von $\mathbb{Z}G$ der Modul ${}^{\sigma}M$ zu M isomorph.*

Beweis. Da M einfach ist, existiert eine Primzahl p von $\mathbb{Z}$, so daß M ein $\mathbb{F}_pG$–Modul ist. Sei $P_M =: P$ die projektive Decke von M als $\hat{\mathbb{Z}}_pG$–Modul. Dann ist natürlich ${}^{\sigma}P_M =: P'$ die projektive Decke von ${}^{\sigma}M$ als $\hat{\mathbb{Z}}_pG$–Modul. Es ist nämlich

$$ {}_{\sigma}(\hat{\mathbb{Z}}_pG)_1 \simeq {}_1(\hat{\mathbb{Z}}_pG)_{\sigma^{-1}} $$

als Bimoduln und daher ist P' projektiv. Nun ist aber $\mathbb{Q} \otimes_{\mathbb{Z}} P' \simeq \mathbb{Q} \otimes_{\mathbb{Z}} P$ nach dem Skolem–Noether Theorem, da σ zentral ist. Also ist nach [Sw-60, Theorem 1] $P \simeq P'$ und somit $M \simeq {}^{\sigma}M$. q.e.d.

Bemerkung 1 K. W. Roggenkamp bemerkte, daß dieses Lemma leicht für charakteristische Schnitte eines projektiven Moduls verallgemeinert werden kann und daß die Aussage nicht für jeden Modul M gilt.

Dieses Resultat wird für die folgende vorbereitende Proposition verwendet:

Proposition 1 *Sei G eine endliche Gruppe, für deren ganzzahligen Gruppenring die Zassenhausvermutung gilt und sei N ein halbeinfacher endlicher $\mathbb{Z}G$–Modul. Dann hat das Isomorphieproblem ganzzahliger Gruppenringe für $\mathbb{Z}(N \rtimes G)$ eine positive Antwort.*

[9] d.h. für alle $r \in R$ und alle $m \in {}^{\sigma}M$ ist $r \cdot m := \sigma(r)m$

Beweis. Wir setzen $E := N \rtimes G$. Sei $\mathbb{Z}E = \mathbb{Z}E_1$ als augmentierte Algebren und sei der in der Normalteilerkorrespondenz ([Pa-65, Theorem D], [RT-92, part1, section V], [Ki-92a]) zu N gehörige Normalteiler N_1 von E_1 vorgelegt. Dann ist $I(N)E = I(N_1)E_1$ und somit ist E_1/N_1 isomorph zu einer Gruppenbasis G_1 von $\mathbb{Z}G$. Da für $\mathbb{Z}G$ die Zassenhausvermutung gilt, existiert ein zentraler Automorphismus α von $\mathbb{Z}G$ mit $\alpha(G) = G_1$. Da nach Voraussetzung $I(N)E = I(N_1)E_1$ und $I(E) = I(E_1)$, ist auch

$$N \simeq I(N)E/(I(N)I(E)) = I(N_1)E_1/(I(N_1)I(E_1)) \simeq N_1$$

eine Kette von $\mathbb{Z}G$–Isomorphismen.

Daher ist mit dem obigen Lemma ${}^{\alpha}N_1 \simeq N$ als $\mathbb{Z}G$–Moduln. Daher folgt die Behauptung mit einem wohlbekannten Lemma (cf. z.B. [Zi-90, Kriterium 5.3]). Es ist nämlich für diesen Isomorphismus ϕ dann $\hat{\phi} : N \rtimes G \longrightarrow N_1 \rtimes G_1$ mit $\hat{\phi}(n, g) := (\phi(n), \alpha(g))$ ein Gruppenisomorphismus. q.e.d.

Diese Proposition gilt auch für allgemeinere Koeffizientenringe S, nämlich für Dedekindbereiche R, in denen kein Primteiler der Ordnung von E invertierbar ist. Der Beweis ist wörtlich der gleiche, wenn man statt $\mathbb{Q}$ den Quotientenkörper von R verwendet und zusätzlich [Ro-80] heranzieht.

2.2 Automorphismen auf Bildern des Gruppenringes

Wir diskutieren in diesem Abschnitt Automorphismen ganzzahliger Gruppenringe direkter Produkte von Gruppen, wie sie für den in diesem Kapitel zu beweisenden Satz von Bedeutung sind. Die wesentlichen Argumente dieses Unterabschnittes sind auf Ideen von L. L. Scott und K. W. Roggenkamp zurückzuführen.

Sei $G = G_1 \times G_2$ ein direktes Produkt endlicher Gruppen relativ primer Ordnung. Weiter soll $\mathbb{Z}G$ der Zassenhaus–Vermutung genügen und es sei G_1 p–auflösbar und $O_{p'}(G) = G_2$.

Ein normierter Automorphismus α von $\mathbb{Z}G$ erweitert sich zu einem Automorphismus von $\hat{\mathbb{Z}}_pG$ und ist nach [Zi-90, Behauptung 6.3.1] p–adisch von der Form

$$\alpha = \gamma \cdot (\prod_{i=1}^{k(p)} \sigma_i(p)) \cdot \rho,$$

wobei $\sigma_i(p)$ zentrale Gruppenautomorphismen von G_1 sind, γ einen inneren Automorphismus von $\hat{\mathbb{Z}}_pG$ bezeichnet und ρ ein Gruppenautomorphismus

von G ist. Dabei sind die Automorphismen $\sigma_i(p)$ von G_1 so zu verstehen, daß die zentralen Idempotente von $\hat{\mathbb{Z}}_pG$ alle von der Form $1 \otimes_{\hat{\mathbb{Z}}_p} e$ für Idempotente e von $\hat{\mathbb{Z}}_pG_2$ sind und somit $\hat{\mathbb{Z}}_pG_1$ Teilring jedes Blockes von $B_i(p)$, $(i = 1, .., k(p))$ von $\hat{\mathbb{Z}}_pG$ ist, denn $O_{p'}(G_1) = 1$ und somit ist $\hat{\mathbb{Z}}_pG_1$ der Hauptblock.

Diese Methode findet sich im wesentlichen schon in [RS-87a].

Sei jetzt α' ein normierter Automorphismus des ganzzahligen Gruppenringes $\mathbb{Z}E$, wobei E durch eine p–auflösbare Gruppenerweiterung $E \longrightarrow\!\!\!\!\!\rightarrow G$ mit Kern N definiert ist.

Es sei in diesem Unterkapitel vorausgesetzt, daß α' das von N auf $\mathbb{Z}E$ induzierte Augmentationsideal $I(N)E$ normalisiert, d.h.

$$\alpha'(I(N)E) = I(N)E.$$

Dann induziert α' einen normalisierten Automorphismus α auf $\mathbb{Z}G$. Dieser ist, da für $\mathbb{Z}G$ die Zassenhaus–Vermutung gilt, Produkt eines zentralen Automorphismus β und eines von einem Automorphismus ρ der Gruppenbasis G induzierten Ringautomorphismus:

$$\alpha = \beta \cdot \rho.$$

Da $O_{p'}(E)$ ein Normalteiler von E ist, dessen Ordnung ihn im Normalteilerverband von E auszeichnet, fixiert α' das Ideal $I(O_{p'})E$ als Menge und induziert einen Automorphismus $\overline{\alpha}$ von $\mathbb{Z}E/O_{p'}(E)$. Da aber E nach Voraussetzung p–auflösbar ist und $O_{p'}(E/O_{p'}(E)) = 1$ gilt, ist für $\mathbb{Z}E/O_{p'}(E)$ die Zassenhausvermutung richtig. Es ist also

$$\overline{\alpha} = \delta(p) \cdot \tau(p)$$

für einen p–adisch inneren Automorphismus $\delta(p)$ von $\mathbb{Z}E/O_{p'}(E)$ und einen von einem Automorphismus der Gruppenbasis $E/O_{p'}(E)$ induzierten Automorphismus $\tau(p)$ von $\mathbb{Z}E/O_{p'}(E)$ wie in der obigen Diskussion von α. Da nun aber α' sowohl $I(N)E$ als auch $I(O_{p'}(E))E$ fixiert, induziert α einen Automorphismus $\underline{\alpha}$ von

$$\mathbb{Z}E/(I(N)E + I(O_{p'}(E))E) = \mathbb{Z}(E/(N \cdot O_{p'}(E))) \ .$$

Da aber

$$\frac{\mathbb{Z}E/I(N)E}{(I(O_{p'}(E))E + I(N)E)/I(N)E} = \mathbb{Z}E/(I(N)E + I(O_{p'}(E))E)$$

ebenso wie

$$\frac{\mathbb{Z}E/I(O_{p'}(E))E}{(I(O_{p'}(E))E + I(N)E)/I(O_{p'}(E))E} = \mathbb{Z}E/(I(N)E + I(O_{p'}(E))E),$$

ist p–adisch

$$\underline{\alpha} = \gamma(p)(\prod_{i=1}^{t(p)} \sigma_i(p))\rho = \delta(p)\tau(p)$$

für innere Automorphismen $\gamma(p)$ und $\delta(p)$ von $\hat{\mathbb{Z}}_pE/(N \cdot O_{p'}(E))$ und zentralen Gruppenautomorphismen $\sigma_i(p)$ von G_1 für $i = 1, ..., t(p)$, für jeden $\hat{\mathbb{Z}}_pG$–Block im Bild des $\hat{\mathbb{Z}}_pE$–Hauptblockes.

Offensichtlich ist $\tau(p)\rho^{-1}$ zentraler Gruppenautomorphismus von G und fixiert daher jedes zentrale Idempotent von $\hat{\mathbb{Z}}_pE/(N \cdot O_{p'}(E))$.

Daher unterscheiden sich die Automorphismen $\sigma_i(p)$ für $i = 2, ..., t(p)$ von $\sigma_1(p)$ nur durch innere Automorphismen von G_1.

2.3 Ein gruppentheoretisches Hilfsmittel

Bekanntlich ([Hu-67, III, 2.5 Satz c]) existiert ein eindeutiger minimaler Normalteiler einer endlichen Gruppe G mit nilpotentem Quotienten. Diese Eigenschaft endlicher Gruppen geht an wesentlicher Stelle in den Beweis von K. W. Roggenkamp und L. L. Scott [RS-86] zum Isomorphieproblem von nilpotenten auf abelschen Gruppen ein. Da diese Arbeit hier verallgemeinert werden soll, ist ein entsprechender Satz für Gruppen, die in unserer Situation auftreten, zu zeigen.

Sei G eine endliche Gruppe, die die folgende Struktur besitzt:

$$G = H \times \prod_{p \in \mathcal{P}} G_p$$

mit

1. einer Gruppe H, für deren ganzzahligen Gruppenring $\mathbb{Z}H$ die Zassenhausvermutung gilt,

2. einer n–elementigen Menge $\mathcal{P}$ von rationalen Primzahlen,

3. p-auflösbaren Gruppen G_p mit $O_{p'}(G_p) = 1$,

4. so daß alle $n+1$ Gruppen paarweise relativ prime Ordnung besitzen.

5. Sei weiter N ein abelscher Normalteiler der endlichen Gruppe E mit $E/N \simeq G$, so daß
$$(|N|, \frac{|G|}{\prod_{p\in\mathcal{P}} |P_p|}) = 1$$
wobei P_p eine p–Sylowuntergruppe von G_p ist.

Man beachte, daß dadurch G eine p–auflösbare Gruppe für alle $p \in \mathcal{P}$ ist.

Wir zeigen, daß bei fest gehaltenem $\mathcal{P}$ ein *eindeutiger Normalteiler* N_0 *minimaler Ordnung* in E mit Faktorgruppe G_0 existiert, so daß sowohl N_0 als auch G_0 den obigen Bedingungen genügen.

Wir fixieren einige Bezeichnungen, um die Gedankenführung durchsichtiger zu machen:

- π_p ist die Menge der Primzahlen, die die Ordnung von G_p teilen.
- $G_{p'} := G/G_p$.
- Nach Voraussetzung ist $\pi_p \cap \pi_q = \emptyset$ für alle $p \neq q; p, q \in \mathcal{P}$.
- Mit N_p ist mit der obigen Bezeichnung die p–Sylowgruppe von N bezeichnet, denn die Voraussetzungen an N und G garantieren, daß unter den Primzahlen in π_p nur p die Ordnung von N teilt.
- $\pi(E) := \{q \text{ prim } : q | \, |E|\}$.

Seien jetzt in E zwei abelsche Normalteiler N und M mit $E/N = G$ und $E/M = \Gamma$ gegeben, so daß die Paare (N, G) und (M, Γ) den obigen Voraussetzungen 1 — 5 genügen. Zu zeigen ist, daß $(N \cap M, E/(N \cap M))$ auch diesen Voraussetzungen genügt.

Behauptung 1 *Es ist* $E/(N \cap M) \simeq K = K_0 \times \prod_{p\in\mathcal{P}} K_p$ *und* K_p *sind* π_p*–Gruppen,* $|K_0|$ *ist relativ prim zu* $|K/K_0|$.

Beweis. Es ist sicher K isomorph zu einer Untergruppe von $G \times \Gamma$ durch die natürliche Einbettung von $E/(N \cap M)$ in $E/N \times E/M$. Da E aber π_p–auflösbar nach Voraussetzung ist, enthält $E/(N \cap M)$ wenigstens eine π_p–Halluntergruppe. Diese ist in der einzigen π_p–Halluntergruppe von $E/N \times E/M$ enthalten. Alle π_p–Halluntergruppen von $E/(N \cap M)$ sind konjugiert in $E/(N \cap M)$.

Nun ist aber die π_p–Halluntergruppe von $E/(N \cap M)$ in dem Schnitt der π_p–Halluntergruppe Π_p von $E/N \times E/M$ und $E/(N \cap M)$ enthalten. $\Pi_p \cap E/(N \cap M)$ ist sicher eine normale π_p–Untergruppe von $E/(N \cap M)$. Also existiert nur eine π_p–Halluntergruppe von $E/(N \cap M)$, welche dann als direkter Faktor abspaltet, da analog auch ihr Komplement normal ist.

Für K_0 definiert man

$$\pi_0 := \pi(E) \setminus \cup_{p \in \mathcal{P}} \pi_p$$

und führt analoge Schlüsse. q.e.d.

Behauptung 2 *Es ist* $E/(N_p \times M_{p'}) \simeq G_p \times \Gamma_{p'}$.

Beweis. Sicherlich ist $N_p \cdot M_{p'} = N_p \times M_{p'}$, da sowohl N_p als auch $M_{p'}$ normale Untergruppen relativ primer Ordnung sind.

Es sei U das volle Urbild von G_p in E. Da $(|N_{p'}|, |U/N_{p'}|) = 1$, ist $U/N_{p'}$ isomorph zu einer π_p–Halluntergruppe von E nach dem Satz von Schur–Zassenhaus.

Nach der Behauptung 1 ist $E/(N \cap M) = K_p \times K_{p'}$ für eine π_p–Gruppe K_p und eine $\pi_{p'}$–Gruppe $K_{p'}$. Da aber $N \cap M$ Untergruppe von $N_p \times M_{p'}$ ist, ist der natürliche Homomorphismus $E/(N \cap M) \longrightarrow E/(N_p \times M_{p'})$ surjektiv. Also ist $E/(N_p \times M_{p'}) =: X = X_p \times X_{p'}$ wieder eine Zerlegung wie oben.

Sei nun V das volle Urbild von X_p in E, dann ist wegen $(|V/M_{p'}|, |M_{p'}|) = 1$ auch $V/M_{p'}$ isomorph zu einer π_p–Halluntergruppe von E wieder nach dem Satz von Schur–Zassenhaus.

Somit sind $U/N_{p'}$ und $V/M_{p'}$ konjugiert in E. Da N_p eine normale π_p–Gruppe ist, liegt sie in jeder π_p–Halluntergruppe. Also ist

$$\begin{aligned} G_p &= U/(N_p \times N_{p'}) \\ &= (U/N_{p'})/N_p \\ &\simeq (V/M_{p'})/N_p \\ &= V/(N_p \times M_{p'}) \\ &= X_p, \end{aligned}$$

und wenn man noch die Rollen von π_p und $\pi_{p'}$ vertauscht, erhält man das Ergebnis. q.e.d.

Behauptung 3 *Falls $M_{p'} = N_{p'}$, folgt aus $O_{p'}(G_p) = 1$ die Gleichung $O_{p'}((E/(N \cap M))_p) = 1$.*

Beweis. Die Isomorphie von $G_{p'}$ und $\Gamma_{p'}$ folgt aus Behauptung 2.

Nach der Behauptung 1 ist $E/(N \cap M) = X_p \times X_{p'}$ mit der obigen Notation. Wir faktorisieren $N_{p'}$ und verändern die Situation dadurch nicht.

Sei U das volle Urbild von G_p in E und V das volle Urbild von $(E/(N \cap M))_p$ in E. Dann sind sowohl U als auch V zwei π_p–Halluntergruppen von E und somit konjugiert. Da N eine normale π_p–Gruppe ist, liegt sie in $U \cap V$. Also ist

$$\begin{aligned} 1 &= O_{p'}(G_p) \\ &= O_{p'}(U/N) \\ &= O_{p'}(V/N) \\ &= O_{p'}((V/(N \cap M))/(N/(N \cap M))) \\ &\geq O_{p'}(V/(N \cap M)) \\ &= O_{p'}(X_p), \end{aligned}$$

da in Bildern von Gruppen Bilder von Normalteilern wieder Normalteiler sind. Dies war jedoch die Behauptung. q.e.d.

Nun kann das Gesamtziel ins Auge gefaßt werden: Normalteiler N heißen geeignet, wenn N zusammen mit E/N die Voraussetzungen 1 — 5 von oben erfüllen. Falls nun N und M geeignete Normalteiler von E sind, so ist nach Behauptung 2 auch $N_p \times M_{p'}$ ein geeigneter Normalteiler. Mit Behauptung 3 sind dann aber auch $(N_p \cap M_p) \times N_{p'}$ sowie $(N_p \cap M_p) \times M_{p'}$ geeignete Normalteiler. Mit diesen werde das Verfahren fortgeführt und man erhält, daß $N \cap M$ ein geeigneter Normalteiler ist.

Proposition 2 *Es existiert in E ein eindeutiger minimaler Normalteiler N_0, der den Voraussetzungen 1 — 5 von oben genügt.*

Beweis.

$$N_0 := \bigcap_{N \text{ geeignet}} N.$$

q.e.d.

Lemma 2 *N_0 besitzt ein Komplement.*

Beweis. Es ist N abelsch und somit gilt für alle natürlichen Zahlen i mit $G_0 = E/N_0$ für die i-te Kohomologiegruppe

$$H^i(G_0, N_0) \simeq \prod_{p|\,|N_0|} H^i(G_0, (N_0)_p).$$

Wir zeigen, daß $H^i(G_0, N_0) = 0$ ist und können daher annehmen, daß N_0 eine p–Gruppe ist.

Da nun aber

$$Ext^i_{\hat{\mathbb{Z}}_p G_0}(\hat{\mathbb{Z}}_p, N_0) = Ext^i_{\mathbb{Z}G_0}(\mathbb{Z}, N_0) = H^i(G_0, N_0)$$

gilt, ist man fertig, wenn N_0 keinen Beitrag zum $\hat{\mathbb{Z}}_p G_0$ Hauptblock besitzt.

Da $\hat{\mathbb{Z}}_p G_{p'}$ separabel und $\hat{\mathbb{Z}}_p G_p$ eine unzerlegbare Algebra ist, ist die Einschränkung des $\hat{\mathbb{Z}}_p G$ Hauptblocksummanden $N_0(0)$ von N_0 auf $G_{p'}$ ein trivialer Modul. Sei $N_0(0) \oplus N_R = N_0$. Es sei Y das volle Urbild von $G_{p'}$ in E/N_R. Nach dem Satz von Schur–Zassenhaus besitzt $N_0(0)$ in Y ein zu $G_{p'}$ isomorphes Komplement. Zudem ist $N_0(0)$ zentraler Normalteiler von Y, da $G_{p'}$ trivial auf $N_0(0)$ operiert. Somit ist $N_0(0)$ direkter Faktor von Y und $G_{p'}$ ist normale $\pi_{p'}$–Halluntergruppe von Y. Da Y Normalteiler von E/N_R ist und da $G_{p'}$ charakteristischer Normalteiler von Y ist, ist $G_{p'}$ normale $\pi_{p'}$–Halluntergruppe von E/N_R.

Sei $\tilde{G}_p$ das volle Urbild von G_p in E/N_R. Offensichtlich ist $\tilde{G}_p$ normale π_p–Halluntergruppe von E/N_R. Da außerdem G_p Bild von $\tilde{G}_p$ ist und $O_{p'}(G_p) = 1$ gilt, ist $O_{p'}(\tilde{G}_p) = 1$.

Da nun aber $\tilde{G}_p$ und $G_{p'}$ Normalteiler relativ primer Ordnung von E/N_R sind, zerfällt E/N_R in ein direktes Produkt von Gruppen, so daß N_R zusammen mit E/N_R den Voraussetzungen 1–5 genügen. Mit der Minimalität von N_0 folgt $N_0(0) = 1$. q.e.d.

Wir können daher das folgende Korollar formulieren:

Korollar 2 *Es ist $H^i(G_0, N_0) = 0$ für alle positiven ganzen Zahlen i.*

2.4 Der Isomorphiesatz

Wir zeigen in diesem Unterabschnitt mit den bisher bereitgestellten Hilfsmitteln den

Satz 1 *Sei $\mathcal{P}$ eine endliche Menge von n rationalen Primzahlen und sei*

$$G = H \times \prod_{p \in \mathcal{P}} G_p$$

ein Produkt von $n+1$ Gruppen paarweise relativ primer Ordnung, so daß für jedes p die Gruppen G_p p–auflösbar mit $O_{p'}(G_p) = 1$ sind. Eine p–Sylowuntergruppe von G_p sei mit P_p bezeichnet. $\mathbb{Z}H$ erfülle die Zassenhausvermutung. Weiterhin sei E eine endliche Gruppe mit abelschem Normalteiler N und $E/N \simeq G$, für den die Beziehung

$$(|N|, \frac{|G|}{\prod_{p \in \mathcal{P}} |P_p|}) = 1$$

gilt. Dann hat das Isomorphieproblem für $\mathbb{Z}E$ eine positive Antwort.

Beweis. Ohne Beschränkung der Allgemeinheit ist $N = N_0$ in der Bezeichnungsweise von Unterabschnitt 2.3. Sei weiter

$$A := rad_{\mathbb{Z}G} N = \prod_{p|\,|N|} rad_{\hat{\mathbb{Z}}_p G} N_p,$$

so daß N/A ein halbeinfacher $\mathbb{Z}G$–Modul ist. In Anlehnung an Unterabschnitt 2.3 bezeichnet N_p die p–Sylowuntergruppe von N und $(N/A)_p$ die p–Sylowuntergruppe von N/A. Falls für ein $\hat{\mathbb{Z}}_p G$–Blockidempotent e nun

$$eN_p/eA_p = 0$$

gilt, so ist wegen der Additivität des Radikals $eN_p = 0$. Also gehört $(N/A)_p$ zu genau denselben $\hat{\mathbb{Z}}_p G$–Blöcken wie N_p.

Sei nun $\mathbb{Z}E = \mathbb{Z}E_1$ für eine normalisierte Untergruppe E_1 der Einheiten von $\mathbb{Z}E$, so existiert zu $N \trianglelefteq E$ ein Normalteiler $M \trianglelefteq E_1$ von E_1, so daß die induzierten Augmentationsideale von N und M übereinstimmen ([Pa-65, Theorem D][RT-92, Ki-92a]):

$$I(N)E = I(M)E_1.$$

Ebenso existiert zu $A \trianglelefteq E$ ein $B \trianglelefteq E_1$ mit

$$I(A)E = I(B)E_1.$$

Es seien

$$\overline{N} := N/A\,, \overline{E} := E/A\,, \overline{E}_1 \simeq E_1/B\,, \overline{M} := M/B \text{ und } G^1 \simeq E_1/M$$

Gruppen der Augmentation 1, so daß $\mathbb{Z}\!\!\mathbb{Z}G = \mathbb{Z}\!\!\mathbb{Z}G^1$ und $\mathbb{Z}\!\!\mathbb{Z}\overline{E} = \mathbb{Z}\!\!\mathbb{Z}\overline{E}_1$ sind.

Sicherlich ist für $\mathbb{Z}\!\!\mathbb{Z}G$ die Zassenhausvermutung richtig [Zi-90, Bemerkung 3.2.2.] und [RS-87b].

Da N der kleinste Normalteiler in E ist, der den Vorraussetzungen des Satzes genügt, ist $\overline{N}$ der kleinste Normalteiler von $\overline{E}$, der den Voraussetzungen des Satzes genügt. Wäre das nicht der Fall, so würde in $\overline{E}$ ein kleinerer Normalteiler $\overline{N}_0$ existieren, der den Voraussetzungen des Satzes genügt. Dieser besitzt das volle Urbild N_0' in E mit isomorphem Quotienten:

$$\overline{E}/\overline{N}_0 \simeq E/N_0'.$$

Es ist nur noch zu zeigen, daß die Bedingung 5 aus Unterabschnitt 2.3 nicht verletzt ist. Dies folgt aus dem Beweis von Lemma 2: N hat keinen Beitrag zum $\hat{\mathbb{Z}}_pG$–Hauptblock, fehlte aber in $\overline{N}_0$ eine p–Sylowgruppe, die in N nicht fehlt, so gehörte $\overline{N}_p$ zum $\hat{\mathbb{Z}}_pG$–Hauptblock.

Somit fixiert jeder augmentierte Automorphismus α von $\mathbb{Z}\!\!\mathbb{Z}\overline{E}$ das induzierte Augmentationsideal $I(\overline{N})\overline{E}$ als Ganzes. Es würde sonst zu $I(\overline{N})\overline{E}$ einen Normalteiler $\overline{N}'$ von $\overline{E}$ mit derselben Ordnung wie $\overline{N}$ geben, der der Beziehung

$$I(\overline{N}')\overline{E} = \alpha(I(\overline{N})\overline{E})$$

genügt. Da dann aber

$$\mathbb{Z}\!\!\mathbb{Z}\overline{E}/\overline{N} \simeq \mathbb{Z}\!\!\mathbb{Z}\overline{E}/\overline{N}'$$

und mithin

$$\overline{E}/\overline{N} \simeq \overline{E}/\overline{N}'$$

aus der positiven Antwort auf das Isomorphieproblem für $\mathbb{Z}\!\!\mathbb{Z}\overline{E}/\overline{N}$ folgt, ist daher, verwendet man $|\overline{N}| = |\overline{N}'|$, auch $\overline{N}'$ geeignet, die Voraussetzungen des Satzes anzuwenden. Aus der Minimalität von $\overline{N}$ ist dann sogar $\overline{N} = \overline{N}'$ zu folgern. Damit ist die Zwischenbehauptung gezeigt.

Mit Proposition 1 erhält man einen Ringautomorphismus α' von $\mathbb{Z}\!\!\mathbb{Z}\overline{E}$, der $\overline{E}$ auf $\overline{E}_1$ abbildet und daher augmentiert ist. Dieser induziert dann mit der obigen Diskussion einen Automorphismus α von $\mathbb{Z}\!\!\mathbb{Z}G$, der dann G auf G^1 abbildet.

Die Diskussion in Unterabschnitt 2.2 erlaubt uns nun, die p–adische Erweiterung von α für jedes $p \in \mathcal{P}$ als

$$\alpha = \gamma(p)(\prod_{i=1}^{k(p)} \sigma_i(p))\rho$$

für jeden $\hat{\mathbb{Z}}_pG$–Block $B_1, .., B_{k(p)}$ und zentrale Gruppenautomorphismen $\sigma_i(p)$ von G_p, innere Automorphismen $\gamma(p)$ von $\hat{\mathbb{Z}}_pG$ und einen Gruppenautomorphismus ρ von G zu schreiben. Dabei unterscheiden sich für festes p die $\sigma_i(p)$ auf dem Bild des $\hat{\mathbb{Z}}_p\overline{E}$–Hauptblockes $B_1 \oplus B_2 \oplus ... \oplus B_{t(p)}$ nur durch innere Automorphismen, die durch Variation von $\gamma(p)$ beschrieben werden können.

Nun müssen noch die verschiedenen Primstellen ausgeglichen werden. Da $\sigma_1(p)$ ein zentraler Gruppenautomorphismus von G_p ist, ist er global definierbar und an der Primstelle $q \neq p$ ist er inner: Da $|G/G_p| \cdot \hat{\mathbb{Z}}_p = \hat{\mathbb{Z}}_p$, ist die Gruppe der äußeren Automorphismen $Outcent(\hat{\mathbb{Z}}_pG/G_p)$ trivial ([RS-87a, (1.2.13)]).

Daher ist

$$\sigma := \prod_{p \in \mathcal{P}} \sigma_1^{-1}(p)$$

ein zentraler Gruppenautomorphismus von G und

$$\varphi := \alpha\rho^{-1}\sigma^{-1}$$

ein Ringautomorphismus von $\mathbb{Z}G$, der G auf G^1 abbildet und der auf dem Bild des $\hat{\mathbb{Z}}_p\overline{E}$–Hauptblockes an den Primstellen $p \in \mathcal{P}$ innerer Automorphismus ist.

Nun ist aber

$$[(\overline{N})_p, O_{p'}(\overline{E})] \leq ((\overline{N})_p \cap O_{p'}(\overline{E})) = 1,$$

da die beiden Gruppen Normalteiler relativ primer Ordnung in E sind, und somit $(\overline{N})_p$ zum $\hat{\mathbb{Z}}_p\overline{E}$ Hauptblock gehörig ist. Da aber $(\overline{N})_p$ und N_p zu den gleichen $\hat{\mathbb{Z}}_pG$–Blöcken gehören, gehört N_p zum $\hat{\mathbb{Z}}_p\overline{E}$–Hauptblock.

Da nun aber

$${}^{\varphi}N \simeq N$$

als $\mathbb{Z}G$–Moduln und unter Benützung des kleinen Gruppenrings $\mathbb{Z}E/(I(N)I(E))$ die $\mathbb{Z}G$–Modulisomorphie

$$N \simeq I(N)E/(I(N)I(E)) = I(M)E_1/(I(M)I(E_1)) \simeq M$$

gilt ([RS-87a]), schließt man

$$E \simeq E_1$$

aus [Zi-90, Kriterium 5.3]. q.e.d.

Unter den vielen Konsequenzen des Satzes sei eine besonders hervorgehoben:

Korollar 3 *[Sc-85, RS-86] Sei E eine endliche Gruppe mit abelscher Hyperkommutatorgruppe*[10] *N. Dann hat $\mathbb{Z}E$ eine positive Antwort auf das Isomorphieproblem.*

Beweis. Mit $H = 1$ und $G_p = P_p$ für alle $p \in \mathcal{P}$ ist der obige Satz auf E anwendbar. q.e.d.

Beispiele für Gruppen E, die den Voraussetzungen des Satzes aber nicht den Voraussetzungen des Korollars genügen, sind leicht in vielfältiger Ausprägung zu gewinnen. Für die Rolle als G_p prädestiniert sind zum Beispiel affine Gruppen $C_p \rtimes C_q$ für Primzahlen p, q und $q|(p-1)$ mit Galoisoperation.

Für $\mathcal{P} = \emptyset$ ist das Ergebnis von Sehgal, Sehgal und Zassenhaus [SSZ-84] in Satz 1 enthalten.

[10] das ist der Kern des Epimorphismus auf den größten nilpotenten Quotienten

3 Involutionen in Gruppenringen

3.1 Präliminarien

Wir beginnen mit einem wohlbekannten Lemma, das wegen seiner Bedeutung für die vorliegende Arbeit angegeben werden soll:

Lemma 3 *Sei K ein Körper und sei A eine K–Algebra mit zentralem Idempotent e verschieden von 1 und 0. Sei R ein Dedekindbereich und sei Λ eine R–Ordnung in A mit $K = frac(R)$. Dann gilt für jede R–flache, kommutative R–Algebra S*

$$\begin{array}{ccc} S \otimes_R \Lambda & \longrightarrow & S \otimes_R \Lambda \cdot e \\ \downarrow & & \downarrow \\ S \otimes_R \Lambda \cdot (1-e) & \longrightarrow & S \otimes_R \overline{\Lambda} \end{array}$$

mit $\overline{\Lambda} := \Lambda \cdot e/(\Lambda \cap \Lambda \cdot e)$ ist ein Pullbackdiagramm.

Als nächstes werden wir ein weiteres Lemma in Anlehnung an [GR-87b, Theorem 2.7] beweisen, das uns die Arbeit sehr erleichtern wird:

K sei der Quotientenkörper des Dedekindbereiches R der Charakteristik 0.

Lemma 4 *Seien Λ eine R–Ordnung in einer endlich dimensionalen K–Algebra A und Δ eine R–Ordnung in der endlich dimensionalen K–Algebra B, so daß $\Lambda \leq \Delta$ und $A \leq B$ und sei J ein lokal freies Λ–Rechtsideal. Dann ist $J \otimes_\Lambda \Delta \simeq J \cdot \Delta$ ausgewertet in B.*

Beweis. Es ist

$$0 \longrightarrow \Delta \longrightarrow B \longrightarrow B/\Delta \longrightarrow 0$$

eine exakte Sequenz von Δ–Moduln und somit auch von Λ-Moduln. Dann ist eine exakte Sequenz von Λ–Moduln induziert:

$$Tor_1^\Lambda(J, B/\Delta) \longrightarrow J \otimes_\Lambda \Delta \longrightarrow J \otimes_\Lambda B$$

Da aber J projektiv ist, gilt

$$Tor_1^\Lambda(J, B/\Delta) = 0.$$

Somit ist mit

$$\begin{aligned} J \otimes_\Lambda B &\simeq (J \otimes_\Lambda \Delta) \otimes_R K \\ &\simeq K \otimes_R J \otimes_\Lambda \Delta \\ &\simeq (J \otimes_R K) \otimes_\Lambda \Delta \\ &\simeq A \otimes_\Lambda \Delta \\ &\simeq K \otimes_R \Lambda \otimes_\Lambda \Delta \\ &\simeq K \otimes_R \Delta \\ &\simeq B \end{aligned}$$

die Behauptung bewiesen, wenn man die Isomorphismen in den exakten Sequenzen verfolgt. q.e.d.

Im Verlaufe der folgenden Untersuchungen wird ein zahlentheoretisches Lemma benötigt werden. Wir definieren für alle $i \in \mathbb{Z}$ die Zahl $\eta_i(n) := \zeta_{2^n}^i + \zeta_{2^n}^{-i}$. Manchmal wird auch η_i statt $\eta_i(n)$ und η statt $\eta(n)$ geschrieben.

Lemma 5 *Sei ζ_{2^n} eine primitive 2^n–te Einheitswurzel.*

$$\eta(n) := \zeta_{2^n} + \zeta_{2^n}^{-1}$$

Dann gilt für alle $k \geq 2$ und alle $x \in \mathbb{Z}[\eta(n)]$:

$$(1 + 2^k x) \in U(\mathbb{Z}[\eta(n)]) \Longrightarrow x \in \eta(n)\mathbb{Z}[\eta(n)]$$

für alle $n \geq 2$.

Beweis von Lemma 5. Wir führen eine Induktion über n durch.

Sei $n = 2$: Dann ist die Behauptung trivial, da $\eta(2) = 0$.

Sei die Behauptung bewiesen für $n-1$. Dann sei jetzt die Körpererweiterung $\mathbb{Q}[\eta(n)] : \mathbb{Q}[\eta(n-1)]$ betrachtet. Die Ganzheitsringe in diesen Körpern sind $\mathbb{Z}[\eta(n)]$ bzw. $\mathbb{Z}[\eta(n-1)]$, welche den $\mathbb{Z}$–Rang 2^{n-2} bzw. 2^{n-3} haben. Damit ist unsere Körpererweiterung quadratisch. Mit Nr sei die Norm dieser Erweiterung und mit tr die Spur bezeichnet. Sei $x \in \mathbb{Z}[\eta(n)]$ mit

$$x = \alpha + \sum_i \alpha_i \eta_{2i} + \sum_j \beta_j \eta_{2j+1}$$

mit ganzzahligen Koeffizienten. Sei σ Erzeugendes der Galoisgruppe der Erweiterung von $\mathbb{Z}[\eta(n)] : \mathbb{Z}[\eta(n-1)]$. Da diese Untergruppe der zyklischen

Galoisgruppe von $\mathbb{Z}[\eta(n)]$ über $\mathbb{Z}$ ist ([Hu-67, I,13.19]) und die Ordnung 2 hat, ist

$$x^\sigma = \alpha + \sum_i \alpha_i \eta_{2i} - \sum_j \beta_j \eta_{2j+1}.$$

Das Hauptargument des Beweises ist das folgende: Es berechnet sich die Norm von $1 + 2^k x$ zu

$$\begin{aligned} Nr(1+2^k x) &= (1+2^k x)\cdot(1+2^k x^\sigma) \\ &= 1 + 2^k tr(x) + 2^{2k} Nr(x) \\ &\in U(\mathbb{Z}[\eta(n-1)]). \end{aligned}$$

Es ist

$$tr(x) = 2 \cdot (\alpha + \sum_i \alpha_i \eta_{2i})$$

und somit

$$\begin{aligned} Nr(1+2^k x) &= 1 + 2^{k+1}(\alpha + \sum_i \alpha_i \eta_{2i}) + 2^{2k} Nr(x) \\ &= 1 + 2^{k+1}(\alpha + \sum_i \alpha_i \eta_{2i} + 2^{k-1} Nr(x)). \end{aligned}$$

Mit der Induktionsannahme ist

$$\alpha + \sum_i \alpha_i \eta_{2i} + 2^{k-1} Nr(x) \in \eta(n-1)\mathbb{Z}[\eta(n-1)].$$

Da $k \geq 2$ gilt, ist $2^{k-1} Nr(x) \in \eta(n-1)\mathbb{Z}[\eta(n-1)]$ und somit wegen $\eta_{2i}(n) \in \eta(n-1)\mathbb{Z}[\eta(n-1)]$ auch

$$\alpha \in (\eta(n-1)\mathbb{Z}[\eta(n-1)]) \cap \mathbb{Z} = 2\mathbb{Z}.$$

Damit ist jedoch auch $x \in \eta(n)\mathbb{Z}[\eta(n)]$. Es folgt die Behauptung. q.e.d.

Es wurde dabei verwendet, daß $Nr(\eta(n)) = 2$ — die Norm nach $\mathbb{Z}$— und daß die Galoisgruppe von $\mathbb{Z}[\eta(n)]$ über $\mathbb{Z}$ auf $\eta(n)\mathbb{Z}[\eta(n)]$ operiert. Dies ist jedoch eine lange bekannte Tatsache (z.B. [Ha-49, III §27 c2. Seite 391]).

Bemerkung 2 Man vergleiche diesen Beweis mit dem Beweis von Lemma 9, da auch dort der Galoisautomorphismus σ und die Norm Nr die Schlüsselrolle spielen.

3.2 Grundlegende Definitionen

Es sei für ein festes $n \in \mathbb{N}$

$$D_{2^n} =< a, b | a^{2^n}, b^2, baba >$$

die Diedergruppe der Ordnung 2^{n+1}. Dann ist

$$C(n) := C_{\mathbb{Z}D_{2^n}}(b) =< 1, a^i + a^{-i}, a^{2^{n-1}} | 1 \leq i \leq 2^{n-1} - 1 >_{\mathbb{Z}<b>}$$

der Zentralisator von b in $\mathbb{Z}D_{2^n}$. Mit Lemma 3 und einem zentralen Idempotent $e = \frac{1}{2}(1 + a^{2^{n-1}})$ in $\mathbb{Q}D_{2^n}$ ist $\mathbb{Z}D_{2^n}$ ein Pullback mit einer $\mathbb{Z}$-Ordnung Λ_n und $\mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}$ wie folgt ([Ro-89]):

$$\begin{array}{ccc} \mathbb{Z}D_{2^n} & \xrightarrow{\sigma_n} & \mathbb{Z}D_{2^{n-1}} \\ \downarrow \tau_n & & \downarrow \phi_n \\ \Lambda_n & \xrightarrow{\psi_n} & \mathbb{F}_2 D_{2^{n-1}} \end{array}$$

Dabei ist σ_n Multiplikation mit e gefolgt von dem Isomorphismus

$$D_{2^n} / < a^{2^{n-1}} > \simeq D_{2^{n-1}}$$

und τ_n ist die Multiplikation mit $(1 - e)$. Wir schreiben $C(n)$ iterativ als Pullback in Ringen algebraisch ganzer Zahlen $\mathbb{Z}[\eta(k)]$. Mit Lemma 3 ist damit ein Pullbackdiagramm von $C(n)$ induziert:

$$\begin{array}{ccc} C(n) & \xrightarrow{\sigma_n} & B_{n-1} \\ \downarrow \tau_n & & \downarrow \overline{\phi}_n \\ \Gamma_n & \xrightarrow{\overline{\psi}_n} & \overline{B}_{n-1} \end{array}$$

Es ist Λ_n äquivalent zur Darstellung

$$a \longrightarrow \begin{pmatrix} cos\frac{2\pi}{n} & sin\frac{2\pi}{n} \\ -sin\frac{2\pi}{n} & cos\frac{2\pi}{n} \end{pmatrix}, b \longrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

und somit

$$\tau_n(a^k + a^{-k}) = (\zeta_{2^n}^k + \zeta_{2^n}^{-k}) \cdot 1 \text{ für alle } k \in \mathbb{N}.$$

Daher ist $\Gamma_n = \mathbb{Z}[\eta(n)] < b >$ mit $\eta_i(n) := \zeta_{2^n}^i + \zeta_{2^n}^{-i}$ und $\eta(n) := \eta_1(n)$. Weiter ist

$$B_{n-1} = \sigma_n(C(n)) =< 1, a^i + a^{-i}, 2a^{2^{n-2}} | i = 1, .., 2^{n-2} - 1 >_{\mathbb{Z}<b>} .$$

Man beachte den Unterschied zu $C(n)$:

$$C(n)/B_n = (\mathbb{Z} < b > a^{2^{n-1}})/(2\mathbb{Z} < b > a^{2^{n-1}}).$$

Da $C(n)e = B_n e$ und $C(n)(1-e) = B_n(1-e)$, ist ein Pullbackdiagramm wie folgt gegeben:

$$\begin{array}{ccc} B_n & \longrightarrow & B_{n-1} \\ \downarrow & & \downarrow \tilde{\phi} \\ \Gamma_n & \xrightarrow{\tilde{\psi}_n} & \tilde{B}_{n-1} \end{array}$$

Zum Beweis von Satz 2 benötigen wir noch weitere Ringe, die als Pullbacks geschrieben werden sollen. Wir setzen $\hat{C}(n) := C(n)/((1-b)C(n))$ und $\hat{B}_n := B(n)/((1-b)B(n))$. Dann erhalten wir Pullbackdiagramme

$$\begin{array}{ccc} \hat{B}_n & \longrightarrow & \hat{B}_{n-1} \\ \downarrow & & \downarrow \\ \mathbb{Z}[\eta(n)] & \longrightarrow & \tilde{\hat{B}}_{n-1} \end{array} \quad , \quad \begin{array}{ccc} \hat{C}(n) & \longrightarrow & \hat{B}_{n-1} \\ \downarrow & & \downarrow \\ \mathbb{Z}[\eta(n)] & \longrightarrow & \overline{\hat{B}}_{n-1}. \end{array}$$

Damit ist

$$(1-e)\hat{C}(n) =< \frac{1}{2}(1-a^{2^{n-1}}), \frac{1}{2}(a^i+a^{-i}-a^{2^{n-1}-i}-a^{2^{n-1}+i}) | 1 \leq i \leq 2^{n-2}-1 >_{\mathbb{Z}}$$

und

$$(1-e)\hat{C}(n) \cap \hat{C}(n) =< 1-a^{2^{n-1}},\ a^i+a^{-i}-a^{2^{n-1}-i}-a^{2^{n-1}+i} | 1 \leq i \leq 2^{n-2}-1 >_{\mathbb{Z}}.$$

In $\mathbb{Z}[\eta(n)]$ ist dies gleich $2\mathbb{Z}[\eta(n)]$.
Genauso verfahren wir mit $\hat{B}_n$:

$$(1-e)\hat{B}_n =< \frac{1}{2}(1-a^{2^{n-1}}), \frac{1}{2}(a^i+a^{-i}-a^{2^{n-1}-i}-a^{2^{n-1}+i}) | 1 \leq i \leq 2^{n-2}-1 >_{\mathbb{Z}}$$

und

$$(1-e)\hat{B}_n \cap \hat{B}_n =< 2-2a^{2^{n-1}},\ a^i+a^{-i}-a^{2^{n-1}-i}-a^{2^{n-1}+i} | 1 \leq i \leq 2^{n-2}-1 >_{\mathbb{Z}}.$$

In $\mathbb{Z}[\eta(n)]$ ist dies gleich $2\eta(n)\mathbb{Z}[\eta(n)]$.

Damit ist

$$\overline{\hat{B}}_{n-1} = \mathbb{Z}[\eta(n)]/(2\mathbb{Z}[\eta(n)]) \text{ und } \tilde{\hat{B}}_{n-1} = \mathbb{Z}[\eta(n)]/(2\eta(n)\mathbb{Z}[\eta(n)]).$$

Da $C(n) = \mathbb{Z} < b > \otimes_{\mathbb{Z}} \hat{C}(n)$ und $B_n = \mathbb{Z} < b > \otimes_{\mathbb{Z}} \hat{B}_n$, ist

$$\overline{B}_{n-1} = \mathbb{Z} < b > \otimes_{\mathbb{Z}} \mathbb{Z}[\eta(n)]/(2\mathbb{Z}[\eta(n)])$$

und

$$\tilde{B}_{n-1} = \mathbb{Z} < b > \otimes_{\mathbb{Z}} \mathbb{Z}[\eta(n)]/(2\eta(n)\mathbb{Z}[\eta(n)]).$$

Präziser:

$$\overline{B}_n = \mathbb{Z}/2\mathbb{Z} < b > + \sum_{i=1}^{2^{n-1}-1} \mathbb{Z}/2\mathbb{Z} < b > (a^i + a^{-i}),$$

$$\tilde{B}_n = \mathbb{Z}/4\mathbb{Z} < b > + \sum_{i=1}^{2^{n-1}-1} \mathbb{Z}/2\mathbb{Z} < b > (a^i + a^{-i}).$$

Für spätere $K-$theoretische Anwendungen beweisen wir das

Lemma 6 *Es ist* $2 - b \in U(\tilde{B}_{n-1})$ *kein Bild einer Einheit von* Γ_n.

Beweis. Die Faser von $2 - b$ in Γ_n ist

$$2 - b + 2\eta(n)\mathbb{Z}[\eta(n)] < b >$$

und ein Element x aus dieser Menge also von der Form:

$$x = 2 - b + 2x_1\eta(n) + 2y_1 b\eta(n) \text{ mit } x_1, y_1 \in \mathbb{Z}[\eta(n)].$$

Da $\mathbb{Z}[\eta(n)] < b > \subseteq \mathbb{Z}[\eta(n)] \oplus \mathbb{Z}[\eta(n)]$, drückt sich x in den Wedderburn Komponenten wie folgt aus:

$$x = (1 + 2x_1\eta(n) + 2y_1\eta(n), 3 + 2x_1\eta(n) - 2y_1\eta(n)).$$

Falls es solch ein x gibt, so auch eines mit Augmentation 1:

Es existieren nämlich zwei kommutative Diagramme wie folgt:

$$\begin{array}{ccc} \Gamma_n & \xrightarrow{\tilde{\phi}} & \tilde{B}_n \\ \downarrow \epsilon & & \tilde{\epsilon} \downarrow \\ \mathbb{Z}[\eta(n)] & \xrightarrow{\tilde{\pi}} & \tilde{\hat{B}}_n \end{array} \quad \text{und} \quad \begin{array}{ccc} \Gamma_n & \xrightarrow{\tilde{\phi}} & \tilde{B}_n \\ \uparrow \sigma & & \tilde{\sigma} \uparrow \\ \mathbb{Z}[\eta(n)] & \xrightarrow{\tilde{\pi}} & \tilde{\hat{B}}_n \end{array}$$

mit $\sigma(x) = x \cdot 1$. Außerdem ist $\epsilon\sigma = id_{\mathbb{Z}[\eta(n)]}$ und $\tilde{\epsilon}\tilde{\sigma} = id_{\tilde{B}_n}$. Jetzt ist für irgend ein Urbild x von $2 - b$

$$\tilde{\phi}((\sigma\epsilon)(x)) = (\tilde{\phi}\sigma\epsilon)(x) = \tilde{\sigma}(\tilde{\pi}\epsilon(x)) = \tilde{\sigma}(1) = 1$$

und es wäre daher mit $x \cdot ((\sigma\epsilon(x))^{-1}$ ein Urbild mit Augmentation 1 gefunden.

Man kann also ohne Beschränkung der Allgemeinheit

$$2x_1\eta(n) + 2y_1\eta(n) = 0$$

annehmen, wodurch dann die Projektion auf die zweite Komponente eine Einheit

$$u = -1 + 4z \text{ mit } z = 1 + \eta(n)y_1$$

wäre.
Die Bedingung an z definiert genau die Elemente in $\mathbb{Z}[\eta(n)] \setminus \eta(n)\mathbb{Z}[\eta(n)]$. Solch ein Element gibt es aber nicht wie man mit Lemma 5 sieht.

3.3 Einheiten aus der Zahlentheorie

Lemma 7 *Es sei $C_2 =< b >$ gegeben. Dann sind $1+\zeta_{2^n}^i+\zeta_{2^n}^{-i}$ und $b+\zeta_{2^n}^i+\zeta_{2^n}^{-i}$ Einheiten in $\mathbb{Z}[\zeta_{2^n} + \zeta_{2^n}^{-1}]C_2 = \Gamma_n$.*

Beweis von Lemma 7. Für $n = 2$ ist die Aussage klar, da dann die fraglichen Einheiten gleich 1 oder b sind. Sonst ist mit

$$(1 + \zeta_{2^n}^i + \zeta_{2^n}^{-i}) \cdot (1 - \zeta_{2^n}^i - \zeta_{2^n}^{-i}) = -1 \cdot (1 + \zeta_{2^n}^{2i} + \zeta_{2^n}^{-2i})$$

und

$$(b + \zeta_{2^n}^i + \zeta_{2^n}^{-i}) \cdot (b - \zeta_{2^n}^i - \zeta_{2^n}^{-i}) = -1 \cdot (1 + \zeta_{2^n}^{2i} + \zeta_{2^n}^{-2i})$$

die Aussage induktiv bewiesen.

Lemma 8 *Es ist*

1. $|U(\tilde{B}_{n-1}) : \tilde{\psi}_n(U(\Gamma_n))| = 2$.
2. $\overline{\psi}_n(U(\Gamma_n)) = U(\overline{B}_{n-1})$.

für alle $n \geq 3$.

Beweis von Lemma 8. Zuerst folgern wir aus Teil 2 die Aussage von Teil 1. Sei

$$\tilde{B}_n \xrightarrow{\varrho_n} \overline{B}_n$$

die natürliche Projektion. Da ϱ_n surjektiv ist und $ker\varrho_n$ im Radikal von $\tilde{B}_n$ liegt, ist jedes Urbild einer Einheit von $\overline{B}_n$ Einheit in $\tilde{B}_n$. Falls $\overline{u} = 1+x$ mit $x \in rad\ \overline{B}_n$ eine Einheit in $\overline{B}_n$ ist, hat sie vier Urbilder in $\tilde{B}_n : 1+x, -1+x, 1+2b+x, -1+2b+x$. Somit ist

$$|U(\tilde{B}_n)| = 4 \cdot |U(\overline{B}_n)|.$$

Dann sieht man: Es hat also $\tilde{\psi}_n(U(\Gamma_n))$ in $U(\tilde{B}_{n-1})$ den Index 1,2 oder 4. Da aber -1 im Kern von $\overline{\psi}_n$ aber nicht im Kern von $\tilde{\psi}_n$ liegt, ist der Index höchstens 2, denn mit u ist auch $-u$ eine Einheit von Γ_n.

Nach Lemma 6 ist der Index aber mindestens 2 also ist

$$|U(\tilde{B}_{n-1}) : \tilde{\psi}_n(U(\Gamma_n))| = 2.$$

Somit ist dann auch 1. bewiesen.

Wir zeigen jetzt Teil 2. in mehreren Schritten. Dies erfolgt durch den Beweis der Behauptungen 4–7 unter Verwendung von Lemma 7:

Behauptung 4 *Es ist*

$$U(\overline{B}_n) = U(\overline{\hat{B}}_n) + (1+b) \cdot \overline{\hat{B}}_n.$$

Beweis von Behauptung 4. Da $\overline{B}_n = \overline{\hat{B}}_n + b \cdot \overline{\hat{B}}_n$, folgt die Behauptung aus der Nilpotenz von $(1+b) \cdot \overline{\hat{B}}_n$. q.e.d.

Da $(1+b) \cdot \overline{\hat{B}}_n$ nilpotent vom Grade zwei ist, rechnet man

$$(1+(b+1)x) \cdot (1+(b+1)y) = 1+(b+1)(x+y)$$

und somit wird $U(\overline{B}_n)$ von $U(\overline{\hat{B}}_n), b$ und $1+(b+1)y_i$ für eine $I\!F_2$–Basis $\{y_i\}$ von $\overline{\hat{B}}_n$ erzeugt. Denn $\{1+(b+1)y_i, b\}$ erzeugen $1+(b+1)\overline{\hat{B}}_n$ und

$$< U(\overline{\hat{B}}_n), 1+(b+1)\overline{\hat{B}}_n >= U(\overline{B}_n)$$

nach Behauptung 4.

Wir definieren

$$x_i := a^i + a^{-i} \in \overline{B}_n \subseteq I\!F_2 C_{2^n}.$$

Behauptung 5 *Es ist* $\{x_i(1+x_i)^{-1} | i \text{ ungerade}\}$ *eine* 2^{n-2}*–elementige linear unabhängige Menge in* $\overline{\hat{B}}_n/\overline{\hat{B}}_{n-1}$.

Beweis von Behauptung 5. Es sei G die Automorphismengruppe der zyklischen Gruppe der Ordnung 2^n. Nach [Hu-67, I,13.19] ist

$$G \simeq C_2 \times C_{2^{n-2}}.$$

Diese operiert auf $X := \sum_{i \text{ ungerade}} I\!F_2 x_i$ auf offensichtliche Weise. Dabei werde $C_2 \times 1 \trianglelefteq G$ von $a \longrightarrow a^{-1}$ erzeugt. Das operiert jedoch trivial auf X. Somit sind X und

$$\tilde{Y} := \sum_i I\!F_2 \frac{x_i}{1+x_i} \leq \sum_i I\!F_2 x_i$$

$I\!F_2 C_{2^{n-2}}$–Moduln. Wir betrachten nun den $I\!F_2 C_{2^{n-2}}$-Modulhomomorphismus

$$\sum_{\text{alle } i} I\!F_2 x_i \xrightarrow{\mu} \sum_{\text{alle } i} I\!F_2 x_i / \sum_{\text{gerade } i} I\!F_2 x_i$$

(μ ist nichts anderes als die Restklassenabbildung von $\overline{\hat{B}}_n$ modulo $\overline{\hat{B}}_{n-1}$) und stellen fest, daß der natürliche Homomorphismus

$$\sum_{\text{alle } i} I\!F_2 x_i / \sum_{\text{gerade } i} I\!F_2 x_i \xrightarrow{\nu} X$$

ein $I\!F_2 C_{2^{n-2}}$-Modulisomorphismus ist. (Es ist nämlich X ein moduldirekter Summand von $\sum_{\text{alle } i} I\!F_2 x_i$.)

Sei Y das Bild von $\tilde{Y}$ in X via $\nu\mu$. Wir wollen zeigen, daß $Y = X$ gilt und nehmen an, daß Y ein echter Teilmodul von X ist. Offensichtlich ist $X \simeq I\!F_2 C_{2^{n-2}}$ unzerlegbar. Damit ist dann Y im Radikal von X und daher von $\sum_{\tau \in C_{2^{n-2}}} \tau$ annuliert.

Es ist

$$\frac{x_1}{1+x_1} = x_1 + x_1^3 + x_1^5 + \dots ,$$

die geraden Potenzen weglassend, denn diese liegen im Teilraum der x_{2i}.

Nun ist aber

$$x_1^{2i+1} = x_1 \cdot x_1^{2i} = x_1 \cdot (\sum_j \alpha_{2j} x_{2j}) = \sum_j \alpha_{2j} \cdot (x_{2j-1} + x_{2j+1})$$

für geeignete $\alpha_{2j} \in I\!F_2$, also eine *gerade* Anzahl von Summanden x_k. Summiert man über alle Konjugierten bezüglich $C_{2^{n-2}}$, ergibt sich, sobald $i > 0$ ist, das Ergebnis $2 \cdot \Delta = 0$, wobei $\Delta := \sum_{i \text{ ungerade}} x_i$. Insgesamt erhält man also $(\sum_{\tau \in C_{2^{n-2}}} \tau)(Y) \in \Delta \neq 0$. q.e.d.

Behauptung 6 *Es ist* $< 1, \frac{x_i}{1+x_i} >$ *eine* $\mathbb{F}_2$*–Basis von* $\overline{\hat{B}}_n$.

Beweis. Es ist $\{\frac{x_i}{1-x_i} |\ i \text{ ungerade }\}$ eine linear unabhängige Menge in $\overline{\hat{B}}_n/\overline{\hat{B}}_{n-1}$ nach Behauptung 5. Damit spannen sie $\overline{\hat{B}}_n/\overline{\hat{B}}_{n-1}$ linear auf. Nach Induktion ist $< 1, \frac{x_i}{1+x_i} |\ i$ gerade $>= \overline{\hat{B}}_{n-1}$. Daher folgt die Behauptung. q.e.d.

Behauptung 7 $\{1 + a^i + a^{-i}, 1 + b(a^i + a^{-i}), b | i = 1, .., 2^{n-1} - 1\} \subseteq \overline{B}_n$ *erzeugt ganz* $U(\overline{B}_n)$.

Beweis von Behauptung 7. Nach [GR-87a, Lemma 3.12], (siehe auch [Ta-84, 7, (2.10)]) wird $U(\overline{\hat{B}}_n)$ von $\{1 + a^i + a^{-i} | i \in \mathbb{N}\}$ erzeugt. Wegen

$$1 + b(a^i + a^{-i}) = (1 + a^i + a^{-i}) \cdot (1 + (b+1)\frac{a^i + a^{-i}}{1 + a^i + a^{-i}})$$

ist unter Verwendung der bisherigen Untersuchungen

$$< U(\overline{\hat{B}}_n), 1 + b(a^i + a^{-i}), b | i \text{ ungerade} >= U(\overline{B}_n).$$

q.e.d.

Faßt man jetzt alles zusammen sieht man das folgende: Die Bilder der Einheiten $1+\eta_i(n+1), b+\eta_i(n+1); i \in \mathbb{N}$ aus Lemma 7 erzeugen zusammen mit b die Einheiten von $U(\overline{B}_n)$ und das Lemma 8 ist bewiesen.

3.4 Zentralisatoren als Tensorprodukte

Die Bestimmung der Einheiten von B_n ist überaus schwierig und ein weiterer Ansatz scheint geboten.

$$\begin{array}{ccc} \mathbb{Z}C_2 & \longrightarrow & \mathbb{Z} \\ \downarrow & & \downarrow \\ \mathbb{Z} & \longrightarrow & \mathbb{F}_2 \end{array}$$

ist ein Pullbackdiagramm und man erhält durch Tensorieren mit $\hat{C}(n)$ beziehungsweise mit $\hat{B}_n$ die induzierten Pullbackdiagramme

$$\begin{array}{ccc} C(n) & \longrightarrow & \hat{C}(n) \\ \downarrow & & \downarrow \psi_2 \\ \hat{C}(n) & \xrightarrow{\psi_1} & \mathbb{F}_2 \otimes_{\mathbb{Z}} \hat{C}(n) =: \overline{\hat{C}}(n) \end{array} \quad \text{und} \quad \begin{array}{ccc} B_n & \longrightarrow & \hat{B}_n \\ \downarrow & & \downarrow \phi_2 \\ \hat{B}_n & \xrightarrow{\phi_1} & \mathbb{F}_2 \otimes_{\mathbb{Z}} \hat{B}_n =: \overline{\hat{B}}_n \end{array}$$

Bemerkung 3 I. Reiner und S. Ullom stellten in [RU-74] ihre Theorie der Mayer-Vietoris-Sequenzen für Klassengruppen vor, die in der vorliegenden Arbeit eine zentrale Rolle spielen wird: Falls R ein Dedekindbereich ist mit einem globalen Quotientenkörper K der Charakteristik 0, und falls Λ eine R-Ordnung in der separablen, endlich dimensionalen K-Algebra A ist, falls weiter ein Pullbackdiagramm

$$\begin{array}{ccc} \Lambda & \xrightarrow{\alpha} & \Lambda_1 \\ \downarrow & & \downarrow \pi_1 \\ \Lambda_2 & \xrightarrow{\pi_2} & \overline{\Lambda} \end{array}$$

von Ringen mit einer surjektiven Abbildung α und endlichem Ring $\overline{\Lambda}$ gegeben ist und weiter $\mathbb{Q}\Lambda$ die Eichler-Bedingung über R erfüllt, so besagt der Satz von I. Reiner und S. Ullom, daß die folgende Sequenz von Gruppen exakt ist:

$$U(\Lambda_1) \times U(\Lambda_2) \longrightarrow U(\overline{\Lambda}) \xrightarrow{\delta} Cl(\Lambda) \longrightarrow Cl(\Lambda_1) \oplus Cl(\Lambda_2) \longrightarrow 0$$

Dabei ist

$$\delta(u) = \{(\lambda_1, \lambda_2) \in \Lambda_1 \times \Lambda_2 | \pi_1(\lambda_1) = u \cdot \pi_2(\lambda_2)\}$$

Diese Theorie fußt auf Milnors Mayer-Vietoris-Sequenzen für K-Gruppen wie sie in [Mil-71] dargestellt ist. Die Eichler-Bedingung ist sicherlich für kommutative Ordnungen erfüllt.

Eine erste Anwendung erhält man aus den Vorarbeiten in Kapitel 3.3 durch Betrachtung des Pullbackdiagramms

$$\begin{array}{ccc} C(n) & \longrightarrow & B_{n-1} \\ \downarrow & & \downarrow \\ \Gamma_n & \longrightarrow & \overline{B}_{n-1} \end{array} .$$

Dabei verwendet man nun Lemma 8 und erhält, daß

$$Cl(C(n)) \simeq Cl(B_{n-1}) \oplus Cl(\Gamma_n)$$

ist. Außerdem ist dadurch gewährleistet, daß

$$|Cl(B_n)| \leq 2 \cdot |Cl(B_{n-1})| \cdot |Cl(\Gamma_n)|$$

gilt. Dies folgt aus dem Pullbackdiagramm

$$\begin{array}{ccc} B_n & \longrightarrow & B_{n-1} \\ \downarrow & & \downarrow \\ \Gamma_n & \longrightarrow & \tilde{B}_{n-1} \end{array}$$

und Reiner Ulloms Mayer-Vietoris-Sequenz hierzu.

Alle Ringe in den obigen Pullbacks sind kommutativ und daher sind

$$U(\hat{C}(n)) \xrightarrow{\pi_C} U(\hat{\overline{C}}(n)) \longrightarrow Cl(C(n)) \longrightarrow (Cl(\hat{C}(n)))^2 \longrightarrow 0$$

und

$$U(\hat{B}_n) \xrightarrow{\pi_B} U(\hat{\overline{B}}_n) \longrightarrow Cl(B_n) \longrightarrow (Cl(\hat{B}_n))^2 \longrightarrow 0$$

die zugehörigen Mayer-Vietoris-Sequenzen.

Außerdem ist $C(n)$ eine Oberordnung von B_n in $\mathbb{Q}\,B_n$. Dann ist

$$Cl(B_n) \longrightarrow\!\!\!\!\rightarrow Cl(C(n))$$

ein Epimorphismus durch Induzieren (z.B. [Ta-84, 1. (3.8)]). Man erhält

$$Cl(\hat{B}_n) = Cl(\hat{B}_{n-1}) \oplus Cl(\mathbb{Z}[\eta(n)]) = \prod_{k \le n} Cl(\mathbb{Z}[\eta(k)]),$$

da $U(\mathbb{Z}[\eta(n)])$ surjektiv auf $\mathbb{Z}/4\mathbb{Z} + \sum_i \mathbb{Z}/2\mathbb{Z}(a^i + a^{-i})$ abbildet ([GR-87a, Lemma 3.12, Lemma 3.14], [Ta-84, 7, (2.10)]).

Daher sieht man

$$Cl(\hat{C}(n)) = Cl(\hat{B}_{n-1}) \oplus Cl(\mathbb{Z}[\eta(n)]) = \prod_{k \le n} Cl(\mathbb{Z}[\eta(k)]).$$

Da Induzieren einen Epimorphismus von $Cl(\hat{B}_n)$ auf $Cl(\hat{C}(n))$ vermittelt ([Ta-84, 1. (3.8)]), ist $Cl(\hat{B}_n) \simeq Cl(\hat{C}(n))$.

Man hat also das *kommutative* Diagramm mit exakten Zeilen:

$$\begin{array}{ccccccccc} U(\hat{C}(n)) & \xrightarrow{\pi_C} & U(\hat{\overline{C}}(n)) & \xrightarrow{\delta_C} & Cl(C(n)) & \longrightarrow & (Cl(\hat{C}(n)))^2 & \longrightarrow & 0 \\ & & \uparrow \pi & & \uparrow \alpha & & \| & & \\ U(\hat{B}_n) & \xrightarrow{\pi_B} & U(\hat{\overline{B}}_n) & \xrightarrow{\delta_B} & Cl(B_n) & \longrightarrow & (Cl(\hat{B}_n))^2 & \longrightarrow & 0 \end{array}$$

Die Mayer-Vietoris-Sequenzen von I. Reiner und S. Ullom entspringen aus der allgemeineren Theorie der Mayer-Vietoris-Sequenzen, die von J. Milnor in

[Mil-71] algebraisiert wurde. Daher ist die Kommutativität wegen der Funktorialität der dort auftauchenden K–Gruppen nur an den Verbindungshomomorphismen δ_B und δ_C zu zeigen. Sei

$$J = \{(b_1, b_2) \in (\hat{B}_n)^2 | \phi_1(b_1) = u\phi_2(b_2)\}$$

ein Ideal welches zu $u \in U(\hat{\overline{B}}_n)$ via δ_B korrespondiert. Gesucht ist das zu J gehörige Idèle. Sei v ein beliebiges Urbild von u^{-1} in $\hat{\mathbb{Z}}_2\hat{B}_n$. Dann ist

$$(1, v) \times 1 \times 1 \times 1 \times ...$$

ein Idèle. Wegen $\phi_1(1) \neq \phi_2(v) = u^{-1}$ ist es nur dann das triviale Idèle, wenn $u = 1$ ist. Da sicherlich $J_p = (B_n)_p$ für alle $p \neq 2$ und

$$\begin{aligned}(J \cdot C(n))_2 &= J_2 \cdot (C(n))_2 \\ &= (B_n)_2 \cdot (1, v) \cdot (C(n))_2 \\ &= (B_n)_2 \cdot ((C(n))_2 \cdot (1, v))\end{aligned}$$

und somit

$$\begin{aligned}(C(n))_2 \cdot (1, v) &= \{(c_1, c_2 \cdot v) \in (\hat{C}(n))^2 | \psi_1(c_1) = \psi_2(c_2)\} \\ &= \{(c_1, c_2 \cdot v) \in (\hat{C}(n))^2 | \psi_1(c_1) = \psi_2(c_2 \cdot v)\pi(u)\} \\ &= \{(x_1, x_2) \in (\hat{C}(n))^2 | \psi_1(x_1) = \psi_2(x_2)\pi(u)\},\end{aligned}$$

bildet das zu diesem Idèle gehörige Ideal auf $\delta_C(\pi(u))$ ab.

Analog sieht man, daß das obige Idèle zu J gehört:

$$\begin{aligned}(B_n)_2 \cdot (1, v) &= \{(c_1, c_2 \cdot v) \in (\hat{B}_n)^2 | \phi_1(c_1) = \phi_2(c_2)\} \\ &= \{(c_1, c_2 \cdot v) \in (\hat{B}_n)^2 | \phi_1(c_1) = \phi_2(c_2 \cdot v)u\} \\ &= \{(x_1, x_2) \in (\hat{B}_n)^2 | \phi_1(x_1) = \phi_2(x_2)u\}.\end{aligned}$$

Sei $x = (\lambda_1, \lambda_2) \in J$ mit $\phi_1(\lambda_1) = \phi_2(\lambda_2)u$. Dann ist

$$(\lambda_1, \lambda_2 v^{-1}) \in (B_n)_2,$$

denn

$$\phi_2(\lambda_2 v^{-1}) = \phi_2(\lambda_2)u = \phi_1(\lambda_1).$$

Die Wahl des Urbildes v beeinflußt das Ideal J nicht, da (v, v) eine Einheit in $\hat{\mathbb{Z}}_2 B_n$ ist.

Bezüglich dieser Untersuchung sei auf [CR-82-87, Exercise 53.1] verwiesen.

Zu untersuchen ist $ker(\alpha)$. Das ist aber isomorph zu

$$ker[U(\hat{\overline{B}}_n)/\pi_B(U(\hat{B}_n)) \longrightarrow U(\hat{\overline{C}}(n))/\pi_C(U(\hat{C}(n))].$$

Die Einheitengruppe von $\hat{\overline{B}}_n$ ist genau

$$1 + 2\mathbb{Z}/4\mathbb{Z}a^{2^{n-1}} + \sum_{i=1}^{2^{n-1}-1} \mathbb{Z}/2\mathbb{Z}(a^i + a^{-i})$$

und die von $\hat{\overline{C}}(n)$ ist

$$(1 + \sum_{i=1}^{2^{n-1}-1} \mathbb{Z}/2\mathbb{Z}(a^i + a^{-i})) \dot{\cup} (a^{2^{n-1}} + \sum_{i=1}^{2^{n-1}-1} \mathbb{Z}/2\mathbb{Z}(a^i + a^{-i})).$$

Da $a^{2^{n-1}}$ eine Einheit in $\hat{C}(n)$ ist, sieht man, daß

$$1 \longrightarrow C_2 \longrightarrow U(\hat{\overline{B}}_n) \longrightarrow U(\hat{\overline{C}}(n))/ < a^{2^{n-1}} > \longrightarrow 1$$

exakt ist. Man erhält also ein kommutatives Diagramm mit exakten Zeilen:

$$\begin{array}{ccccccccc}
 & & 1 & \to & U(\hat{B}_n) & \stackrel{\iota_n}{\to} & U(\hat{C}(n))/ < a^{2^{n-1}} > & \longrightarrow\!\!\!\to & \gamma_n \\
 & & \downarrow & & \downarrow \pi_B & & \downarrow \pi'_C & & \\
1 & \to & C_2 & \to & U(\hat{\overline{B}}_n) & \stackrel{\varrho_n}{\to} & U(\hat{\overline{C}}(n))/ < a^{2^{n-1}} > & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & K_n & \to & \frac{U(\hat{\overline{B}}_n)}{\pi_B(U(\hat{B}_n))} & \to & \frac{U(\hat{\overline{C}}(n))}{\pi_C(U(\hat{C}(n)))} & \to & 1 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 1 & & 1 & &
\end{array}$$

Sei jetzt

$$x = k_0 + l_0 \cdot a^{2^{n-1}} + \sum_i k_i \cdot (a^i + a^{-i})$$

eine Einheit in $\hat{C}(n)$. Ihr Bild in $\hat{\overline{C}}(n)$ ist wieder eine Einheit. Daher ist $k_0 + l_0$ ungerade. Durch Multiplikation mit $a^{2^{n-1}}$ kann man erreichen, daß

k_0 ungerade ist. Bildet man wieder das Inverse zu x nach $\overline{\hat{C}}(n)$ ab, sieht man, daß auch das Inverse einen ungeraden Koeffizienten der 1 hat. Somit ist modulo $< a^{2^{n-1}} >$ jede Einheit von $\hat{C}(n)$ eine Einheit von $\hat{B}_n$. Also ist $\gamma_n = 1$.

Das Schlangenlemma ist auf das obige Diagramm nicht anwendbar, da $\pi_B(U(\hat{B}_n))$ Kern der Projektion modulo $\pi_B(U(\hat{B}_n))$ von $U(\overline{\hat{B}}_n)$ ist und nicht $U(\hat{B}_n))$, sowie $\pi'_C(U(\hat{C}(n))/ < a^{2^{n-1}} >)$ Kern der Projektionsabbildung ist und nicht etwa $U(\hat{C}(n))/ < a^{2^{n-1}} >$.

Wir benötigen noch ein Lemma:

Lemma 9 $U(\hat{B}_n) \cap (1 + 2\mathbb{Z} + 2(2\mathbb{Z}+1)a^{2^{n-1}} + 2\sum_i \mathbb{Z}(a^i + a^{-i})) = \emptyset$.

Beweis. Wir zeigen sogar, daß es kein Element aus $\hat{B}_n$ gibt, das modulo $2^l\hat{B}_n$ auf $1 + 2^l a^{2^{n-1}}$ abbildet für $l \geq 1$.

Man definiert $\sigma : \mathbb{Z}C_{2^n} \longrightarrow \mathbb{Z}C_{2^n}$ via $a \longrightarrow -a$, falls

$$C_{2^n} =< a | a^{2^n} = 1 > .$$

Dadurch wird ein Ringautomorphismus definiert und schränkt man diesen auf $\hat{B}_n \subseteq \mathbb{Z}C_{2^n}$ ein, gilt $\sigma \in Aut(\hat{B}_n)$.

Für $n = 2$ ist die Behauptung trivial, da $U(\hat{B}_2) = \{1, -1\}$.

Die Behauptung sei für alle Zahlen kleiner n für alle l bewiesen. Falls nun $x \in U(\hat{B}_n)$ modulo $2^l\hat{B}_n$ auf $1 + 2^l a^{2^{n-1}}$ abbildet, ist

$$x = 1 + 2^l a^{2^{n-1}} + 2^l y$$

für ein $y \in \hat{B}_n$. Damit ist wegen $y + \sigma(y) \in 2\hat{B}_n$

$$\begin{aligned} x \cdot \sigma(x) &= (1 + 2^l a^{2^{n-1}} + 2^l y) \cdot (1 + 2^l a^{2^{n-1}} + 2^l \sigma(y)) \\ &= 1 + 2^{l+1} a^{2^{n-1}} + 2^l(y + \sigma(y)) + 2^{2l}(1 + a^{2^{n-1}}(y + \sigma(y)) + y \cdot \sigma(y)) \\ &= 1 + 2^{l+1} a^{2^{n-1}} + 2^{l+1} z \end{aligned}$$

für ein $z \in \hat{B}_n$.

Da nun aber

$$H^0(< \sigma >, \hat{B}_n) = \hat{B}_{n-1}$$

mit der kanonischen Einbettung $\hat{B}_{n-1} \subseteq \hat{B}_n$ via $C_{2^{n-1}} \leq C_{2^n}$ gilt, ist wegen

$$\sigma(x \cdot \sigma(x)) = x \cdot \sigma(x)$$

in $U(\hat{B}_{n-1})$ ein Urbild von $1+2^{l+1}a^{2^{n-2}}$ modulo 2^{l+1} existent, ein Widerspruch zur Induktionsannahme!

Das Lemma ist somit bewiesen. q.e.d.

Bemerkung 4 Man vergleiche diesen Beweis mit dem von Lemma 5, denn auch dort wurde die Norm eines Elements berechnet und man konnte Induktion anwenden. Ähnliche Argumente werden hier verwendet.

Somit ist gezeigt, daß $ker\,\pi_B\varrho_n = ker\,\pi_B$: Sicher ist $ker\,\pi_B \subseteq ker\,\pi_B\varrho_n$. Sei $x \in ker\,\pi_B\varrho_n \setminus ker\,\pi_B$. Dann ist $\pi_B(x) = 1 + 2a^{2^{n-1}}$. Dies ist ein Widerspruch zu unserem Lemma. Somit ist

$$\iota_n(ker\,\pi_B) = \iota_n(ker\,\pi_B\varrho_n) = \iota_n(ker\,\iota_n\pi'_C) = ker(\pi'_C),$$

da ι_n ein Isomorphismus ist. (In der letzten Gleichung gilt "$\subseteq$" immer und mit $x \in ker\,\pi'_C$ ist $\iota_n\iota_n^{-1}(x) \in \iota_n(ker\,\iota_n\pi'_C)$.)

Daher sieht man, daß ι_n den Kern L_n der Abbildungen $U(\hat{B}_n) \longrightarrow U(\hat{\overline{B}}_n)$ isomorph auf den Kern L'_n von

$$(U(\hat{C}(n))/ < a^{2^{n-1}} >) \longrightarrow (U(\hat{\overline{C}}(n))/ < a^{2^{n-1}} >)$$

abbildet. Daher ist das folgende Diagramm kommutativ mit exakten Zeilen und Spalten:

$$\begin{array}{ccccccccc}
 & & & & 1 & & 1 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & 1 & \longrightarrow & U(\hat{B}_n)/L_n & \longrightarrow & (U(\hat{C}(n))/ < a^{2^{n-1}} >)/L'_n & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & C_2 & \longrightarrow & U(\hat{\overline{B}}_n) & \longrightarrow & U(\hat{\overline{C}}(n))/ < a^{2^{n-1}} > & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & K_n & \longrightarrow & \frac{U(\hat{\overline{B}}_n)}{\pi_B(U(\hat{B}_n))} & \longrightarrow & \frac{U(\hat{\overline{C}}(n))}{\pi_C(U(\hat{C}(n)))} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

und daher ist $K_n = C_2$.

Somit ist

$$|Cl(B_n)| = 2|Cl(C(n))|.$$

Da wir aber früher schon gesehen haben, daß

$$Cl(C(n)) = Cl(B_{n-1}) \oplus Cl(\Gamma_n),$$

ist

$$|Cl(C(n))| = |Cl(B_{n-1})| \cdot |Cl(\Gamma_n)| = 2|Cl(C(n-1))| \cdot |Cl(\Gamma_n)|.$$

Insgesamt erhält man induktiv:

$$|Cl(C(n))| = 2^{n-1} \cdot \prod_{k \leq n} |Cl(\Gamma_k)|.$$

Bemerkung 5 Man beachte auch das Licht, das dieses Resultat auf die Einheiten von B_n wirft. Sie sind nämlich vollständig im Urbild von $\tilde{\psi}_n(U(\Gamma_n))$ unter $\tilde{\phi}_n$ enthalten und haben daher eine entsprechende Form. Insbesondere bildet keine Einheit von B_n auf eine Einheit der Form $(2-b) \cdot x$ ab, wobei x Bild einer Einheit in Γ_n ist.

Lemma 10 *Es ist* $\tilde{\phi}_n(U(B_n)) \leq \tilde{\psi}_n(U(\Gamma_n))$.

3.5 Die Klassenzahl von $\mathbb{Z}[\eta(n)]C_2$

Es ist jetzt nur noch $Cl(\Gamma_n)$ zu berechnen. Dazu erinnert man sich, daß

$$\begin{array}{ccc} \mathbb{Z}C_2 & \longrightarrow & \mathbb{Z} \\ \downarrow & & \downarrow \\ \mathbb{Z} & \longrightarrow & \mathbb{F}_2 \end{array}$$

ein Pullbackdiagramm ist und somit, wenn man Lemma 3 verwendet,

$$\begin{array}{ccc} \Gamma_n & \longrightarrow & \mathbb{Z}[\eta(n)] \\ \downarrow & & \downarrow \\ \mathbb{Z}[\eta(n)] & \longrightarrow & \overline{\hat{B}_n} \end{array}$$

auch Pullbackdiagramm ist. Da offensichtlich $\mathbb{Q}\Gamma_n$ die Eichler Bedingung über $\mathbb{Z}$ erfüllt, sieht man jetzt, da nach [GR-87a, Ta-84] die untere Zeile einen Epimorphismus von Einheiten induziert, mit Milnors Mayer-Vietoris-Sequenz

$$Cl(\mathbb{Z}[\eta(n)])^2 \simeq Cl(\Gamma_n).$$

Sei $h_n := h_n^+$ die Klassenzahl des maximalen reellen Teilkörpers der 2^n-ten Einheitswurzeln über $\mathbb{Q}$. Es ist somit die folgende Gleichheit gezeigt:

Proposition 3 *Es ist*

$$|Cl(C(n))| = |Cl(B_{n-1})| \cdot h_n^2 \text{ und } |Cl(B_n)| = 2 \cdot |Cl(B_{n-1})| \cdot h_n^2.$$

Bemerkung 6 Da nach [ACH-65] $h_n = 1$ für alle $n \in \mathbb{N}$ von H. Cohn vermutet wurde, wäre dann, sollte sich die Cohnsche Vermutung bestätigen, $|Cl(C(n))| = 2^{n-1}$.

Falls also $h_n = 1$ für jedes n, ist für ein $(\mathcal{A}) \in Cl(C(n))$ die Gleichung

$$\mathcal{A} \cdot \mathbb{Z}G \simeq \mathbb{Z}G$$

als $\mathbb{Z}G$–Rechtsmodul richtig ([FKW-74, Remark (4)]).

Bemerkung 7 H. Cohn schreibt in [Co-60]: "We still have obtained no evidence to doubt that every $h_t = 1$."

3.6 Picardgruppen und zentrale Automorphismen

Wir sind interessiert an

$$Cl_{\mathbb{Z}D_{2^n}}(C(n)) := \{I \in Cl(C(n)) | I \cdot \mathbb{Z}D_{2^n} \simeq \mathbb{Z}D_{2^n}\}.$$

Dies ist genau der Kern des natürlichen Homomorphismus:

$$\begin{array}{rcl} Cl(C(n)) & \longrightarrow & Cl(\mathbb{Z}D_{2^n}) \\ (J) & \longrightarrow & (J \otimes_{C(n)} \mathbb{Z}D_{2^n}) \end{array}$$

Dieser sei mit K_n abgekürzt und wird induktiv berechnet:

$$\begin{array}{ccccccccccc} & & 0 & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & 0 & \to & K_n & \to & K'_{n-1} & \oplus & K''_n & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & 0 & \to & Cl(C(n)) & \to & Cl(B_{n-1}) & \oplus & Cl(\Gamma_n) & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & D(\mathbb{Z}D_{2^n}) & \to & Cl(\mathbb{Z}D_{2^n}) & \to & Cl(\mathbb{Z}D_{2^{n-1}}) & \oplus & Cl(\Lambda_n) & \to & 0 \end{array}$$

ist ein kommutatives Diagramm mit exakten Zeilen und Spalten. Dabei ist nach A. Fröhlich, M. E. Keating und S. M. J. Wilson [FKW-74] $D(\mathbb{Z}D_{2^n}) = 0$ und $\Lambda_n = (\mathbb{Z}[\eta(n)])_{2\times 2}$.

Die ersten beiden Zeilen sind exakt nach dem letzten Paragraph wie man aus Milnors Mayer-Vietoris-Sequenz sieht. Es gilt also K_n'' und K_n' zu berechnen.

Dazu sieht man, daß

$$\begin{array}{ccccccccccc}
 & & 0 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & C_2 & \to & K_n' & \to & K_{n-1}' & \oplus & K_n'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & C_2 & \to & Cl(B_n) & \to & Cl(B_{n-1}) & \oplus & Cl(\Gamma_n) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & 0 & \to & Cl(\mathbb{Z}D_{2^n}) & \to & Cl(\mathbb{Z}D_{2^{n-1}}) & \oplus & Cl(\Lambda_n) & \to & 0
\end{array}$$

wiederum ein kommutatives Diagramm mit exakten Zeilen und Spalten ist.

Zu berechnen ist K_n''. Nach A. Fröhlich, M. E. Keating und S. M. J. Wilson [FKW-74] und R. G. Swan ([Sw-62, Corollary 4]), da die Strahlklassengruppe hier gleich der Klassengruppe ist, ist $Cl(\Lambda_n) \simeq Cl(\mathbb{Z}[\eta(n)])$ via der reduzierten Norm–Abbildung nr. Sei jetzt ein lokal freies $\mathbb{Z}[\eta(n)]$–Ideal J gegeben, dann betrachten wir

$$(J \otimes_{\mathbb{Z}[\eta(n)]} \Gamma_n) \otimes_{\Gamma_n} (\mathbb{Z}[\eta(n)])_{2\times 2} = J \otimes_{\mathbb{Z}[\eta(n)]} (\mathbb{Z}[\eta(n)])_{2\times 2} = \begin{pmatrix} J & J \\ J & J \end{pmatrix} \xrightarrow{nr} J^2$$

und sehen ein, daß wenigstens $(Cl(\mathbb{Z}[\eta(n)]))^{[2]}$ im Bild der Abbildung liegt. (Dabei sei für eine abelsche Gruppe A die Sequenz

$$1 \longrightarrow A_{[2]} \longrightarrow A \xrightarrow{a \to a^2} A^{[2]} \longrightarrow 1$$

exakt). Auf der anderen Seite ist aber $|Cl(\mathbb{Z}[\eta(n)])|$ ungerade ([Web-1886, Seite 244, Satz C]) und daher $Cl(\mathbb{Z}[\eta(n)]) = (Cl(\mathbb{Z}[\eta(n)]))^{[2]}$.

Somit sehen wir ein, daß $Cl(\Gamma_n) \longrightarrow Cl(\Lambda_n)$ surjektiv ist. Da $Cl(\Gamma_n) = Cl(\mathbb{Z}[\eta(n)])^2$, ist $|K_n''| = h_n$. Außerdem ist K_n'' Untergruppe von $Cl(\mathbb{Z}[\eta(n)]^2$. Dies berechtigt jedoch nicht, auf den Isomorphietyp von K_n'' zu schließen, es ist also nicht klar, ob $K_n'' \simeq Cl(\mathbb{Z}[\eta(p)])$ ist.

Daher ist

$$|K_n| = 2^{n-1} \cdot \prod_{i=1}^{n} h_i = \frac{|Cl(C(n))|}{\prod_{i=1}^{n} h_i} = \frac{|Cl(C(n))|}{|Cl(\mathbb{Z}D_{2^n})|}$$

mit $h_i := |Cl(\mathbb{Z}[\eta(i)])|$.

Wir können jedoch einiges mehr sagen: Ein Ideal $\mathcal{A}$ von $\mathbb{Z}[\eta(n)]$ ist isomorph zu $2 \cdot \mathcal{A}$, denn 2 erzeugt nach Definition ein Hauptideal. Es sei (α) das zu $\mathcal{A}$ gehörige Idèle und (β) das zu einem zweiten Ideal $\mathcal{B}$ von $\mathbb{Z}[\eta(n)]$ gehörige Idèle.

Dann induziert das Paar $(\mathcal{A}, \mathcal{B})$ ein Ideal von $\mathbb{Z}[\eta(n)]C_2$. Es seien

$$(\alpha) = \prod_{\wp \in Spec(\mathbb{Z}[\eta(n)])} \alpha_\wp \text{ und } (\beta) = \prod_{\wp \in Spec(\mathbb{Z}[\eta(n)])} \beta_\wp$$

die zugehörigen Id'ele. Dann gehört

$$\prod_{\wp} [(1+b) \cdot 1 + (1-b) \cdot \alpha_\wp]$$

zu einem Urbild von $(\mathcal{A}, \mathbb{Z}[\eta(n)])$ in $Cl(\mathbb{Z}[\eta(n)]C_2)$. Verwendet man die Darstellung aus [Ro-83] ist

$$(\gamma) := \prod_{\wp} \begin{pmatrix} 2\alpha_\wp & 0 \\ (2+\eta(n)) \cdot (\beta_\wp - \alpha_\wp) & 2\beta_\wp \end{pmatrix}$$

ein zu $(\mathcal{A}, \mathcal{B})$ gehöriges Idèle. Da aber

$$\begin{pmatrix} 1 & 0 \\ (2+\eta(n)) & 2 \end{pmatrix}$$

eine Einheit in $\mathbb{Q}\Lambda_n$ ist, ist (γ) aufgefaßt als Idèle von $\mathbb{Q}\Lambda_n$ äquivalent zum Idèle

$$\begin{pmatrix} 1 & 0 \\ (2+\eta(n)) & 2 \end{pmatrix} \cdot (\gamma) = \prod_{\wp} \begin{pmatrix} 2\alpha_\wp & 0 \\ 2(2+\eta(n))\beta_\wp & 4\beta_\wp \end{pmatrix} =: (\gamma').$$

Mit $R := \mathbb{Z}[\eta(n)]$ induziert (γ') das Ideal

$$\mathcal{C} := \bigcap_{\wp} \begin{pmatrix} 2\alpha_\wp & 0 \\ 2(2+\eta(n))\beta_\wp & 4\beta_\wp \end{pmatrix} \cdot \begin{pmatrix} R_\wp & R_\wp \\ R_\wp & R_\wp \end{pmatrix}.$$

Dies ist aber gleich

$$\bigcap_{\wp} \begin{pmatrix} 2\alpha_\wp R_\wp & 2\alpha_\wp R_\wp \\ 2(2+\eta(n))\beta_\wp R_\wp + 4\beta_\wp R_\wp & 2(2+\eta(n))\beta_\wp R_\wp + 4\beta_\wp R_\wp \end{pmatrix}.$$

Da aber $2 \in (2+\eta(n))R$, vereinfacht sich dies zu

$$\bigcap_{\wp} \begin{pmatrix} 2\alpha_\wp R_\wp & 2\alpha_\wp R_\wp \\ 2\eta(n)\beta_\wp R_\wp & 2\eta(n)\beta_\wp R_\wp \end{pmatrix} = \begin{pmatrix} 2\mathcal{A} & 2\mathcal{A} \\ 2\cdot\eta(n)\cdot\mathcal{B} & 2\cdot\eta(n)\cdot\mathcal{B} \end{pmatrix}.$$

Dessen reduzierte Norm ist dann aber $4\cdot\eta(n)\cdot\mathcal{A}\cdot\mathcal{B} \simeq \mathcal{A}\cdot\mathcal{B}$. Also ist

$$ker[Cl(\Gamma_n) \longrightarrow Cl(\mathbb{Z}[\eta(n)])] = \{[\mathcal{A}]\times[\mathcal{A}^{-1}] \in Cl(\mathbb{Z}[\eta(n)])^2\} \simeq Cl(\mathbb{Z}[\eta(n)]).$$

3.7 Involutionen und Gruppenbasen

Wir berechnen den Kern und den Kokern des natürlichen Homomorphismus

$$Cl(Z(\mathbb{Z}D_{2^n})) \longrightarrow Cl(C_{\mathbb{Z}D_{2^n}}(< b >)).$$

Dazu beweisen wir jetzt Teile[11] der Ergebnisse von Ergebnisse von S. Endo, T. Miyata und K. Sekiguchi [EMS-82] mit unseren Methoden.

Es ist

$$Z(\mathbb{Z}D_{2^n}) =< 1, a^{2^{n-1}}, a^i + a^{-i}, \delta_n b, \delta_n ab | i = 1, .., 2^n - 1 >_{\mathbb{Z}} =: Z_n;$$

mit $\delta_n := 1 + a^2 + a^4 + ... + a^{2^n-2}$ und es sei

$$Z_n(k) :=< 1, 2a^{2^{n-1}}, a^i + a^{-i}, 2^k\delta_n b, 2^k\delta_n ab | i = 1, .., 2^n - 1 >_{\mathbb{Z}}$$

Dann erhalten wir die Pullbackdiagramme

$$\begin{array}{ccc} Z_n & \longrightarrow & Z_{n-1}(1) \\ \downarrow & & \downarrow \\ \mathbb{Z}[\eta(n)] & \longrightarrow & \overline{\hat{B}}_{n-1} \end{array}$$

sowie

$$\begin{array}{ccc} Z_n(k) & \longrightarrow & Z_{n-1}(k+1) \\ \downarrow & & \downarrow \\ \mathbb{Z}[\eta(n)] & \longrightarrow & \tilde{\hat{B}}_{n-1}, \end{array}$$

[11] Auf allgemeine metazyklische Gruppen gehen wir im Gegensatz zu S. Endo, T. Miyata und K. Sekiguchi nicht ein.

denn mit $e := \frac{1}{2}(1 + a^{2^{n-1}})$ und $f := 1 - e$ ist

$$Z_n f = \frac{1}{2}\mathbb{Z}(1 - a^{2^{n-1}}) + \sum_i \frac{1}{2}\mathbb{Z}(a^i + a^{-i} - a^{2^{n-1}-i} - a^{2^{n-1}+i})$$

ebenso ist

$$Z_n(k) f = \frac{1}{2}\mathbb{Z}(1 - a^{2^{n-1}}) + \sum_i \frac{1}{2}\mathbb{Z}(a^i + a^{-i} - a^{2^{n-1}-i} - a^{2^{n-1}+i})$$

Damit ist aber

$$Z_n f \cap Z_n = \mathbb{Z}(1 - a^{2^{n-1}}) + \sum_i \mathbb{Z}(a^i + a^{-i} - a^{2^{n-1}-i} - a^{2^{n-1}+i})$$

sowie

$$Z_n(k) f \cap Z_n(k) = 2\mathbb{Z}(1 - a^{2^n}) + \sum_i \mathbb{Z}(a^i + a^{-i} - a^{2^{n-1}-i} - a^{2^{n-1}+i})$$

Damit ergeben sich die obigen Pullbackdiagramme.

Nach [GR-87a, Ta-84] ist damit, schreibt man Mayer-Vietoris-Sequenzen zu diesen Pullbacks an,

$$Cl(Z_n) = Cl(Z_{n-1}(1)) \oplus Cl(\mathbb{Z}[\eta(n)])$$

und

$$Cl(Z_n(k)) = Cl(Z_{n-1}(k+1)) \oplus Cl(\mathbb{Z}[\eta(n)])$$

für alle $n \geq 2$. Für $n = 0$ erhält man auf die gleiche Weise durch Zerlegung modulo b das Pullbackdiagramm

$$\begin{array}{ccc} \mathbb{Z} + 2^k\mathbb{Z}b & \longrightarrow & \mathbb{Z} \\ \downarrow & & \downarrow \\ \mathbb{Z} & \longrightarrow & \mathbb{Z}/(2^{k+1}\mathbb{Z}) \end{array} .$$

Für $n = 1$ erhält man das Pullbackdiagramm

$$\begin{array}{ccc} Z_1(k) = \mathbb{Z} + 2^k\mathbb{Z}b + 2^k\mathbb{Z}ab + 2\mathbb{Z}a & \longrightarrow & \mathbb{Z} + 2^k\mathbb{Z}b = Z_0(k) \\ \downarrow & & \downarrow \\ Z_0(k) = \mathbb{Z} + 2^k\mathbb{Z}b & \longrightarrow & \mathbb{Z}/4\mathbb{Z} + 2^k\mathbb{Z}/2^{k+1}\mathbb{Z}b \end{array} .$$

Daher ist

$$|Cl(Z_1(k))| = 2|Cl(\mathbb{Z} + 2^k\mathbb{Z}b)|^2$$

und

$$Cl(\mathbb{Z} + 2^k\mathbb{Z}b) = \mathbb{Z}/2^{k-1}\mathbb{Z}$$

wieder mit der Mayer-Vietoris-Sequenz. Nach dem eben bewiesenen ist

$$Cl(Z(\mathbb{Z}D_{2^n})) = \mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times Cl(\mathbb{Z}D_{2^n})$$

oder

$$Cl(Z(\mathbb{Z}D_{2^n})) = \mathbb{Z}/2^{n-1}\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} \times Cl(\mathbb{Z}D_{2^n})$$

je nach dem ob die Mayer-Vietoris-Sequenz zum obigen Pullbackdiagramm zerfällt oder nicht. S. Endo, T. Miyata und K. Sekiguchi ([EMS-82]) zeigen, daß diese Sequenz nicht zerfällt. Später sind wir in der Lage, diese Aussage auch mit unseren Methoden zu beweisen (cf. Bemerkung 8). S. Endo, T. Miyata und K. Sekiguchi führen detaillierte Untersuchungen über die Kerne der Pullbacks durch und erhalten so das Ergebnis. Wir können darauf verzichten, da unser idèletheoretischer Zugang den Isomorphietyp von $Picent(\mathbb{Z}D_{2^n})$ direkt ergibt. Da wir jedoch auch wesentlich tiefere Aussagen machen können, ist unser Beweis etwas länger als der von S. Endo, T. Miyata und K. Sekiguchi.

Nun sind wir in der Lage, die Klassengruppe des Zentrums Z_n mit der Klassengruppe des Zentralisators der Involution b, $C(n)$, zu vergleichen.

Wir erhalten mit den Mayer-Vietoris-Sequenzen ein kommutatives Diagramm mit exakten Zeilen und Spalten wie folgt:

(1)

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & 1 \\
 & & \uparrow & & \uparrow & & \uparrow \\
 & & C_2 & \longrightarrow & \gamma_n(k) & \longrightarrow\!\!\!\!\rightarrow & \gamma_{n-1}(k+1) \oplus V(n) \\
 & & \uparrow & & \uparrow & & \uparrow \\
1 & \longrightarrow & C_2 & \longrightarrow & Cl(B_n) & \longrightarrow\!\!\!\!\rightarrow & Cl(B_{n-1}) \oplus Cl(\Gamma_n) \\
 & & \uparrow & & \uparrow & & \uparrow \\
1 & \longrightarrow & 1 & \longrightarrow & Cl(Z_n(k)) & \longrightarrow\!\!\!\!\rightarrow & Cl(Z_{n-1}(k+1)) \oplus Cl(\mathbb{Z}[\eta(n)]) \\
 & & \uparrow & & \uparrow & & \uparrow \\
1 & \longrightarrow & 1 & \longrightarrow & K_n(k) & \longrightarrow & K_{n-1}(k+1) \\
 & & & & \uparrow & & \uparrow \\
 & & & & 1 & & 1
\end{array}$$

mit einer zu $|Cl(\mathbb{Z}[\eta(n)])|$ isomorphen Gruppe $V(n)$, da $|Cl(\mathbb{Z}[\eta(n)])|$ ungerade ist. Dabei ist der nach dem Schlangenlemma existierende Homomorphismus abelscher Gruppen $K_{n-1}(k+1) \longrightarrow C_2$ noch zu bestimmen. Es wird sich zeigen, daß dieser surjektiv ist.

Wir beginnen mit einer allgemeinen Betrachtung, wie aus iterativen Pullbacks die zugehörigen Ideale aus den Verschränkungen der zugehörigen Mayer-Vietoris-Sequenzen in idèletheoretischer Formulierung bestimmt werden können.

Sei J ein lokal freies Ideal in einer $\mathbb{Z}$–Ordnung Λ in einer kommutativen separablen $\mathbb{Q}$–Algebra A. Das Idèle $\alpha = \prod_p a_p$ gehöre zu J. Wir können annehmen, daß $J \subseteq A$. Dann ist $J_p = \Lambda_p \cdot a_p$ für alle p wiederum mittels einer Identifikation. Sei e ein zentrales Idempotent in A.

Da

$$0 \longrightarrow \Lambda \cdot e \longrightarrow A \cdot e \longrightarrow (A \cdot e)/(\Lambda \cdot e) \longrightarrow 0$$

exakt ist und da ein lokal freies Ideal J von Λ flach ist, ist auch

$$0 \longrightarrow J \otimes_\Lambda \Lambda \cdot e \longrightarrow J \otimes_\Lambda A \cdot e$$

exakt und wegen

$$\begin{aligned} J \otimes_\Lambda (A \cdot e) &= J \otimes_\Lambda ((\Lambda \cdot e) \otimes_{\mathbb{Z}} \mathbb{Q}) \\ &= (J \otimes_\Lambda (\Lambda \cdot e)) \otimes_{\mathbb{Z}} \mathbb{Q} \\ &= \mathbb{Q} \otimes_{\mathbb{Z}} (J \otimes_\Lambda (\Lambda \cdot e)) \\ &= (\mathbb{Q} \otimes_{\mathbb{Z}} J) \otimes_\Lambda (\Lambda \cdot e) \\ &= (\mathbb{Q} \otimes_{\mathbb{Z}} \Lambda) \otimes_\Lambda (\Lambda \cdot e) \\ &= \mathbb{Q} \otimes_{\mathbb{Z}} (\Lambda \otimes_\Lambda (\Lambda \cdot e)) \\ &= \mathbb{Q} \otimes_{\mathbb{Z}} (\Lambda \cdot e) \\ &= A \cdot e \end{aligned}$$

ist $J \cdot e \simeq J \otimes_\Lambda (\Lambda \cdot e)$.

Weiterhin ist daher

$$(J \cdot e)_p = J_p \cdot e = \Lambda_p \cdot a_p \cdot e = (\Lambda_p \cdot e) \cdot (a_p \cdot e).$$

Somit ist ein zu $J \cdot e$ gehöriges Idèle in $A \cdot e$ gleich $\alpha \cdot e$.

In unserem vorliegendem Fall ist

$$Cl(Z_n(k)) = Cl(Z_{n-1}(k+1)) \oplus Cl(\mathbb{Z}[\eta(n)]),$$

falls $n \geq 2$. Somit erhält man also, falls ein Paar von Idèlen α und β von $\mathbb{Q}\,Z_{n-1}(k+1)$ und von $\mathbb{Q}\,[\eta(n)]$ gegeben ist, das Urbild als Idèle $\alpha \cdot e + \beta \cdot (1-e)$, falls $Z_n(k) \cdot e = Z_{n-1}(k+1)$. Für $n = 1$ ist die Situation ähnlich, denn obige Konstruktion gibt eines der Urbilder. Das andere erhält man durch Multiplikation mit dem Idèle

$$(1, 1 + 2^k b) \times 1 \times 1 \times 1 \times ...,$$

falls die diskutierte Ordnung $Z_{n-1}(k)$ ist, wie man aus der Diskussion in Kapitel 3.4 ersieht.

Gesucht ist also ein Ideal von $Z_n(k)$, das durch Induktion auf B_n auf den Pullback von B_{n-1} mit Γ_n via $(2-b)$ abbildet. Genau dann, wenn es dieses Ideal gibt, vergrössert sich der Kokern dieser Abbildung aus Diagramm (1) nicht. In $Z_0(k)$ hat man 2^{k-1} Ideale, nämlich die mit den Einheiten von $\mathbb{Z}/2^{k+1}\mathbb{Z}$ modulo $< -1 >$ getwisteten Pullbacks der Wedderburn Komponenten.[12] Die die Klassengruppe von $Z_0(k)$ erzeugende Idèle können wie folgt angegeben werden:

$$\frac{1}{2}(1+b) \cdot r + \frac{1}{2}(1-b),$$

wobei $r = (r_0, 1, 1, 1, ...)$ und $r_0 \in \{1, 3, 5, ..., 2^{k+1} - 1\}$.

Zum Pullback

$$\begin{array}{ccc} Z_1(k) & \xrightarrow{e_0} & Z_0(k) \\ \downarrow (1-e_0) & & \downarrow \\ Z_0(k) & \longrightarrow & \mathbb{Z}/4\mathbb{Z} + 2^k\mathbb{Z}/2^{k+1}\mathbb{Z}b \end{array}$$

erhält man alle lokal freien Ideale von $Z_1(k)$ durch die Idèle

$$e_0 \cdot (\frac{1}{2}(1+b) \cdot r + \frac{1}{2}(1-b)) + (1-e_0) \cdot (\frac{1}{2}(1+b) \cdot s + \frac{1}{2}(1-b))$$

und deren Produkt mit

$$(e_0 + (1-e_0) \cdot (1 + 2^k b)) \times 1 \times 1 \times 1 \times ...$$

Zum Pullback

$$\begin{array}{ccc} Z_2(k) & \xrightarrow{e_0} & Z_1(k) \\ \downarrow (1-e_0) & & \downarrow \\ \mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} \end{array}$$

[12] cf. Bemerkung 3

erhält man also alle lokal freien Ideale J durch

$$(1-e_1)+e_1\cdot[e_0\cdot(\frac{1}{2}(1+b)\cdot r+\frac{1}{2}(1-b))+(1-e_0)\cdot(\frac{1}{2}(1+b)\cdot s+\frac{1}{2}(1-b))]=$$

$$=(1-e_1)+(e_1-e_0)\cdot(\frac{1}{2}(1+b)\cdot s+\frac{1}{2}(1-b))+e_0\cdot(\frac{1}{2}(1+b)\cdot r+\frac{1}{2}(1-b)),$$

sowie dem getwisteten von oben auf analoge Weise. Dies ist auch die Form aller weiteren Idèle in der 2-Sylowgruppe von $Cl(Z(\mathbb{Z}D_{2^n}))$ bei allen höheren Pullbacks wie man leicht sieht bei Verwendung der Beziehung $e_n\cdot e_{n-1}=e_{n-1}$. Dabei bildet die Multiplikation mit e_k auf den Gruppenring $\mathbb{Z}D_{2^k}$ ab.

Weiter zeigen wir mit diesen idèletheoretischen Methoden, daß die Klassengruppe $Cl(C_{\mathbb{Z}D_{2^n}}(b))$ eine zyklische 2–Sylow Gruppe besitzt. Zuerst jedoch geben wir ein einfaches Lemma an. Sei dazu

$$\alpha_k:=((1-e_k+e_k\cdot(1+2b))\times\prod_{p\neq 2}1).$$

Lemma 11 *Seien $(J),(J')\in Cl(B_n)$ mit $e_k\cdot J\simeq e_k\cdot J'$ in B_k. Dann existiert ein $u\in<(\alpha_{n-1}),...,(\alpha_k)>$, so daß $(J)\cdot(u)=(J')$ in $Cl(B_n)$.*

Beweis. Für $k=n-1$ ist die Aussage klar, denn sie entspricht genau der Definition von α_{n-1}.
Sei die Aussage für alle k zwischen $n-1$ und k_0+1 bewiesen und sei $(e_{k_0}\cdot J)=(e_{k_0}\cdot J')$ in $Cl(B_{k_0})$. Nach Definition existiert ein $\delta\in\{0,1\}$ mit

$$(e_{k_0+1}\cdot J)=(e_{k_0+1}\cdot J')\cdot(\alpha_{k_0})^\delta.$$

Nach Induktionsvoraussetzung existiert ein $u\in<\alpha_{n-1},...,\alpha_{k_0+1}>$ mit

$$(J)=(J')\cdot(\alpha_{k_0})^\delta\cdot(u).$$

Die Aussage ist mit Induktion bewiesen, wenn $u_0:=\alpha_{k_0}\cdot u$ gewählt wird. q.e.d.

Lemma 12 *Die 2–Sylowgruppe von $Cl(C_{\mathbb{Z}D_{2^n}}(b))$ ist zyklisch. Das erzeugende Ideal ist das zu*

$$(1-e_0+e_0\cdot(1-2b))\times\prod_{p\mathbb{Z}\in Spec\mathbb{Z}\setminus\{2\mathbb{Z}\}}1$$

gehörige Idèle.

Beweis. Wir zeigen, daß α_k die Ordnung 2^{n-k} in $Cl(B_n)$ hat. Sicher hat α_{n-1} die Ordnung 2 in $Cl(B_n)$, da ja α_{n-1} genau das zur Einheit $1+2b$ in $Cl(B_n)$ korrespondierende Idèle ist.

Dann gilt

$$\begin{aligned}\frac{1}{2}(1-a^{2^k})+\frac{1}{2}(1+a^{2^k})\cdot(1+2b)^2 &= \frac{1}{2}(1-a^{2^k})+\frac{1}{2}(1+a^{2^k})\cdot(5+4b)\\ &= 1+\frac{1}{2}(1+a^{2^k})\cdot(4+4b)\\ &= 1+2\cdot(1+a^{2^k})\cdot(1+b)\\ &= 3+2b+2\cdot a^{2^k}\cdot(1+b),\end{aligned}$$

was in $\tilde{B}_{k+1}$ kongruent $-1+2b$ ist. Nun ist aber -1 in $\tilde{B}_{k+1}$ Bild einer globalen Einheit und daher ist $e_{k+2}(\alpha_k)^2 \simeq e_{k+2}(\alpha_{k+1})$ und mithin ist $(\alpha_k)^2$ modulo einem u in $<\alpha_{n-1},...,\alpha_{k+2}>$ nach Lemma 11 äquivalent zum Idèle α_{k+1}. Dieses besitzt mit Induktion die Ordnung 2^{n-k-1}. Die Ordnung von u ist aber nach der Induktionsannahme ein Teiler von $2^{n-(k+2)}$. Dies ist dann aber der Beweis der obigen Aussage. q.e.d.

Da aber für $r_0 = s_0 = 3$ das Idèle α_1 im Bild der Abbildung

$$Cl(Z(\mathbb{Z}D_{2^n})) \longrightarrow Cl(C_{\mathbb{Z}D_{2^n}}(b))$$

liegt und für $s_0 = 3, r_0 = 1$ liegt $\alpha_1 \cdot \alpha_0^{-1}$ im Bild, so auch α_0 und die obige Abbildung der 2–Sylowuntergruppen der Klassengruppen ist surjektiv.

Den Fall $n = 2$ behandelt man separat, da dort die Idèle, die in der vorangegangenen Untersuchung die führende Rolle gespielt haben, nicht auftauchen. Jedoch taucht das Idèle α_0 direkt auf bei der Wedderburn Zerlegung von $Z_2(1)$. Damit liefert die Induktion einen Isomorphismus der 2–Sylowuntergruppen der Klassengruppen des Zentrums von D_{2^n} und des Zentralisators von b für alle n. Der Cokern der Induktionsabbildung ist also ordnungsgleich zu $Cl(\mathbb{Z}D_{2^n})$ und der Kern ist trivial.

Bemerkung 8 Die Surjektivität der Restriktion dieses Homomorphismus auf die 2-Sylowuntergruppen impliziert dann aber auch die Struktur der äußeren Automorphismengruppe von $\mathbb{Z}D_{2^n}$ als $C_{2^{n-1}} \times C_{2^{n-2}}$, eines der Ergebnisse von S. Endo, T. Miyata und K. Sekiguchi ([EMS-82]).

Wie im letzten Abschnitt gesehen, ist die 2–Sylowgruppe von $Cl(C(n))$ gleich der 2–Sylowgruppe des Kerns der natürlichen Abbildung $Cl(C(n)) \longrightarrow$

$Cl(\mathbb{Z}D_{2^n})$. Daher ist die analoge Rechnung wie oben mit dem Kern dieser Abbildung statt mit dem Kern der Abbildung nach $Cl(C(n))$ direkt zu machen und das Ergebnis ist ebenfalls das gleiche, denn $Outcent(\mathbb{Z}D_{2^n})$ ist die 2–Sylowgruppe von $Picent(\mathbb{Z}D_{2^n})$ ([EMS-82] in Kombination mit [Web-1886]).

Da nach [RS-87a] $Cl(Z(\mathbb{Z}D_{2^n})) = Picent(\mathbb{Z}D_{2^n})$ via des natürlichen Homomorphismus ist und durch die Restriktion $Picent(\mathbb{Z}D_{2^n}, < b >)$ nach $Picent(\mathbb{Z}D_{2^n})$ abbildet, und da D_{2^n} eine 2–Gruppe ist, die Automorphismengruppe von $< b >$ trivial ist, ist das Bild der Restriktionsabbildung genau das Bild der auf den Klassengruppen induzierten Abbildung $Cl(Z(\mathbb{Z}D_{2^n})) \longrightarrow Cl(C(n))$. Diese ist jedoch genau die natürliche Induktion durch $(J) \longrightarrow (J \otimes_{Z_n} C(n))$.

Liegt eine Isomorphieklasse eines Ideals J im Bild des Homomorphismus, so ist ein Repräsentant der Konjugationsklasse der zugehörigen Involutionen in einem Reprsentanten der zugehörigen Konjugationsklasse von Gruppenbasen enthalten.

Die Restriktionsabbildung

$$Outcent(\mathbb{Z}D_{2^n}) \longrightarrow Outcent(\mathbb{Z}D_{2^n}, < b >)$$

ist die Abbildung, die einem $aD_{2^n}a^{-1}$ das aba^{-1} zuweist. Es sind dabei zwei Phänomene denkbar:

1. $aD_{2^n}a^{-1} \neq D_{2^n}$ aber $aba^{-1} = b$ modulo Konjugation in $\mathbb{Z}D_{2^n}$.
2. $aba^{-1} \in \mathbb{Z}D_{2^n}$ aber $aD_{2^n}a^{-1} \not\subseteq \mathbb{Z}D_{2^n}$ modulo Konjugation in $\mathbb{Z}D_{2^n}$.

Das erste Phänomen wird im Kern der Restriktionsabbildung gemessen, das zweite im Kokern. Falls $aba^{-1} = ubu^{-1}$ für eine ganzzahlige Einheit u, so ist mit $u^{-1}a =: a'$ ein b fixierendes konjugierendes Element gefunden, das aber genau dann D_{2^n} in eine nicht konjugierte Gruppenbasis abbildet, wenn a dies bewirkt.

Faßt man nun alles zusammen, so erhält man den

Satz 2 *Sei D_{2^n} die Diedergruppe mit 2^{n+1} Elementen.*

1. *Eine $V(\mathbb{Q}D_{2^n})$–Bahn einer nicht zentralen Involution $b \in D_{2^n}$ zerfällt in $2^{n-1} \cdot \prod_{k \leq n} h_k^+$ Konjugationsklassen über $\mathbb{Z}D_{2^n}$, wobei h_k^+ die Klassenzahl des maximalen reellen Teilkörpers des 2^k–ten Kreisteilungskörpers über $\mathbb{Q}$ ist.*

2. *Von diesen Konjugationsklassen bestehen 2^{n-1} aus Involutionen, die in Gruppenbasen liegen.*

3. *Die Vermutung von H. Cohn ([ACH-65]) ist genau dann richtig, wenn für alle $n \in \mathbb{N}$ jede Involution in einer Gruppenbasis liegt.*

4. $Cl(C_{\mathbb{Z}D_{2^n}}(b)) \simeq C_{2^{n-1}} \times \prod_{k \leq n} Cl(\mathbb{Z}[\zeta_{2^k} + \zeta_{2^k}^{-1}])^2$, *wobei* $\zeta_{2^n}^{2^{n-1}} + 1 = 0$.

5. $Cl_{\mathbb{Z}D_{2^n}}(C_{\mathbb{Z}D_{2^n}}(b)) \simeq C_{2^{n-1}} \times \prod_{k \leq n} Cl(\mathbb{Z}[\zeta_{2^k} + \zeta_{2^k}^{-1}])$.

Teile der Ergebnisse von S. Endo, T. Miyata, K. Sekiguchi seien hier noch einmal angegeben, um ein höheres Maß an Vollständigkeit zu erreichen. Es sei nur noch einmal bemerkt, daß wir in der Lage waren, mit unseren Methoden diese Teile der Ergebnisse aus [EMS-82] zu beweisen.

Lemma 13 *([EMS-82])*

1. $\mathbb{Z}D_{2^n}$ *besitzt* 2^{2n-3} *Konjugationsklassen von Gruppenbasen.*

2. $Picent(\mathbb{Z}D_{2^n}) \simeq C_{2^{n-1}} \times C_{2^{n-2}} \times \prod_{k \leq n} Cl(\mathbb{Z}[\zeta_{2^k} + \zeta_{2^k}^{-1}])$.

3. $Outcent(\mathbb{Z}D_{2^n}) \simeq C_{2^{n-1}} \times C_{2^{n-2}}$.

Bemerkung 9 Die Cohnsche Vermutung wurde von F. J. van der Linden für $n \leq 7$ bewiesen, für $n = 8$ wird die verallgemeinerte Riemann-Vermutung benötigt ([vdL-82]).

3.8 Explizite Berechnungen

Ziel dieses Unterabschnitts ist, die zentrale Automorphismengruppe von $\mathbb{Z}D_{2^n}$ bis auf innere Automorphismen so explizit wie möglich zu beschreiben. Dabei wird sich zeigen, daß wir erzeugende Elemente der äusseren Automorphismengruppe explizit in Termen der Gruppenbasis D_{2^n} angeben können.

Es ist

$$\begin{array}{ccc} \mathbb{Z}D_{2^n} & \longrightarrow & \mathbb{Z}D_{2^{n-1}} \\ \downarrow & & \downarrow \phi_n \\ \Lambda_n & \xrightarrow{\psi_n} & \mathbb{F}_2 D_{2^{n-1}} \end{array}$$

ein Pullbackdiagramm und wir zeigen folgendes Lemma:

Lemma 14 *Sei u eine Einheit von $\hat{\mathbb{Z}}_2 D_{2^n}$ im Normalisator der Oberordnung $\mathbb{Z}V_4 \times \prod_{n\geq k\geq 2} \Lambda_k$ in $\hat{\mathbb{Q}}_2 D_{2^n}$ von $\mathbb{Z}D_{2^n}$, die man erhält, wenn man das Produkt der Projektionen von $\mathbb{Z}D_{2^n}$ in die Wedderburnkomponenten von $\mathbb{Q}D_{2^n}$ bildet. Dann ist u im Normalisator von $\mathbb{Z}D_{2^n}$:*

$$N_{U(\hat{\mathbb{Q}}_2 D_{2^n})}(\mathbb{Z}V_4 \times \prod_{n\geq k\geq 2} \Lambda_k) \cap U(\hat{\mathbb{Z}}_2 D_{2^n}) = N_{U(\hat{\mathbb{Z}}_2 D_{2^n})}(\mathbb{Z}D_{2^n})$$

Beweis. Wir verwenden vollständige Induktion. Sicher normalisiert u den Ring $\mathbb{Z}V_4$.

Es ist

$$\hat{\mathbb{Z}}_2 D_{2^n} = \{(\lambda, x) \in \hat{\mathbb{Z}}_2 \Lambda_n \times \hat{\mathbb{Z}}_2 D_{2^{n-1}} | \phi_n(x) = \psi_n(\lambda)\}$$

und somit

$$\begin{aligned}(\Lambda_n \times \mathbb{Z}D_{2^{n-1}}) \cap \hat{\mathbb{Z}}_2 D_{2^n} &= \{(\lambda, x) \in \Lambda_n \times \hat{Z}_2 D_{2^n} | \phi_n(x) = \psi_n(\lambda)\} \\ &= \mathbb{Z}D_{2^n}.\end{aligned}$$

Daher, da u aber sowohl $\Lambda_n \times \mathbb{Z}D_{2^{n-1}}$ (nach der Induktionsannahme) als auch $\hat{\mathbb{Z}}_2 D_{2^{n-1}}$ normalisiert, normalisiert u auch den Schnitt der beiden Ringe, folgt also die Behauptung. q.e.d.

Beispiele für ein solches u sind, legt man die Darstellung aus [Ro-83] zugrunde, $a - b + 1$—dieses ist gleich

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 + \eta(k) \end{pmatrix}$$

im Block Λ_k—sowie $1 + b \cdot (a + a^{-1})$, denn

$$1 + b \cdot (a + a^{-1}) = \begin{pmatrix} 1 - \eta(k) & 0 \\ \eta(k) \cdot (2 + \eta(k)) & 1 + \eta(k) \end{pmatrix}$$

in Λ_k.

Wir zeigen nun, daß Konjugation mit $u = 1 + b \cdot (a + a^{-1})$ nicht inner ist in $\mathbb{Z}D_8$.

Falls es eine Einheit $v \in \mathbb{Z}D_8$ gibt mit ${}^v x = {}^u x$ für alle $x \in \mathbb{Z}D_8$, so ist $v^{-1}u$ im Zentrum von $\mathbb{Z}D_8$.

Die Zerlegung von u in die Wedderburn–Komponenten bezüglich der Darstellung aus [Ro-83] ist

$$u = \begin{pmatrix} 1-\sqrt{2} & 0 \\ 2+\sqrt{2} & 1+\sqrt{2} \end{pmatrix} \oplus \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \oplus (1+2ab).$$

Sei $u \cdot \mu = v$. In der Wedderburn–Zerlegung ist

$$\mu = \mu_3 \oplus \mu_2 \oplus \mu_1.$$

Es ist aber mit $\pi : \mathbb{Z}D_8 \longrightarrow \mathbb{Z}D_4$.

$$\pi(u) \in Z(\mathbb{Z}D_4) \leq C_{\mathbb{Z}D_4}(b) \leq \mathbb{Z}(C_4 \times C_2),$$

wobei $\leq$ eine Inklusion von Ringen bezeichnet. Da $\mathbb{Z}(C_4 \times C_2)$ nur triviale Einheiten besitzt, erkennt man, daß die Projektion von v in $\mathbb{Z}D_4$ Element von $\{\pm 1, \pm a^2\}$ sein muß.

Somit ist

$$\pi(u) \cdot (\mu_2 \oplus \mu_1) \in \pm\{1, a^2\}.$$

Nun ist aber

$$(1 + b(a + a^7)) \cdot (\alpha_0 + \alpha_1(a + a^7)) = \alpha_0 + \alpha_1(a + a^7) + b(\alpha_0(a + a^7) + 2\alpha_1)$$

in Λ_3. Damit v aber ganzzahlige Einheit in $\mathbb{Z}D_8$ wird, müssen α_1, der Koeffizient von $a + a^7$, und α_0, der Koeffizient von $b \cdot (a + a^7)$, beide gerade ganze Zahlen sein. Obiges Element stellt aber die Komponente von v in Λ_3 dar. Falls v ganzzahlige Einheit sein soll, muß auch diese Projektion in Λ_3 ganzzahlige Einheit sein. Dies ist bei geradem α_0 und geradem α_1 nicht gegeben.

Daß Konjugation mit $u' = a - b + 1$ nicht innerer Automorphismus von $\mathbb{Z}D_4$ sein kann, zeigt man ähnlich: Sei $v' = u' \cdot \lambda$ ganzzahlige Einheit mit einer zentralen rationalen Einheit λ. Zentrale Einheiten von Λ_2 sind nur Vielfache der Einheitsmatrix. Projektion von $a - b + 1$ nach $\mathbb{Z}V_4$, erzwingt, daß die Projekton von v' nach $\mathbb{Z}V_4$ in $\{\pm 1, \pm a, \pm b, \pm ab\}$ liegt. Jedoch mit $\alpha_0 \in \mathbb{Q}$,

$$(\alpha_0 \cdot (a - b + 1) \cdot \frac{1}{2}(1 - a^2) \pm \frac{1}{2}(1 + a^2) \cdot \{1, a, b, ab\}) \cap \mathbb{Z}D_4 = \emptyset.$$

Wir zeigen im folgenden, daß Konjugation mit $1+a-b$ und $1+b\cdot(a+a^{-1})$ die Gruppe $Outcent(\mathbb{Z}D_{2^n})$ erzeugt.

Es sei bei einer abelschen Gruppe A deren 2-Sylowgruppe mit A_2 bezeichnet und wir definieren weiterhin $e := (1 + a^{2^{n-1}})/2$, ein zentrales Idempotent in $\mathbb{Z}D_{2^n}$. Wir behaupten, daß der Homomorphismus

$$\begin{array}{rcl} Outcent(\mathbb{Z}D_{2^n}) & \longrightarrow & Outcent(\mathbb{Z}D_{2^{n-1}}) \\ (M) & \longrightarrow & (M \cdot e) \end{array}$$

surjektiv ist. Aus einer Mayer-Vietoris-Sequenz erhält man, daß für ein Ideal J von $Z(\mathbb{Z}D_{2^n})$

$$\begin{array}{rcl} (Cl(Z(\mathbb{Z}D_{2^n})))_2 & \longrightarrow & (Cl(Z_{n-1}(1)))_2 \\ (J) & \longrightarrow & (J \cdot e) = (J \otimes_{Z(\mathbb{Z}D_{2^n})} Z(\mathbb{Z}D_{2^n})e) \end{array}$$

surjektiv ist. Da aber $Z_{n-1}(1)$ und $Z(\mathbb{Z}D_{2^{n-1}}))$ Ordnungen in derselben separablen Algebra sind, ist der Homomorphismus

$$\begin{array}{rcl} (Cl(Z_{n-1}(1)))_2 & \longrightarrow & (Cl(Z(\mathbb{Z}D_{2^{n-1}})))_2 \\ (J) & \longrightarrow & (J \otimes_{Z_{n-1}(1)} Z(\mathbb{Z}D_{2^{n-1}})) = (J \cdot Z(\mathbb{Z}D_{2^{n-1}})) \end{array}$$

ebenfalls surjektiv. Nun ist aber mit $\Lambda := \mathbb{Z}D_{2^n}$, $Z_n := Z(\mathbb{Z}D_{2^n})$ und $\Lambda^G = H^0(D_{2^n}, \Lambda)$ sowie $(\Lambda e)^G = H^0(D_{2^n}, \Lambda e)$

$$\begin{array}{rcl} ((J \otimes_{Z_n} Z_n e) \otimes_{Z_n e} (\Lambda e)^G) \otimes_{(\Lambda e)^G} \Lambda e & = & (J \otimes_{Z_n} Z_n e) \otimes_{Z_n e} \Lambda e \\ & = & J \otimes_{Z_n} \Lambda e \\ & = & (J \otimes_{Z_n} \Lambda) \otimes_{\Lambda} \Lambda e \end{array}$$

und somit das folgende Diagramm kommutativ:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & (Cl(Z(\mathbb{Z}D_{2^n})))_2 & \tilde{\longrightarrow} & Outcent(\mathbb{Z}D_{2^n}) & \longrightarrow & 1 \\ & & \downarrow \cdot e & & \downarrow \cdot e & & \\ & & (Cl(Z_{n-1}(1)))_2 & & Outcent(\mathbb{Z}D_{2^{n-1}}) & & \\ & & \downarrow & & \| & & \\ 1 & \longrightarrow & (Cl(Z(\mathbb{Z}D_{2^{n-1}})))_2 & \tilde{\longrightarrow} & Outcent(\mathbb{Z}D_{2^{n-1}}) & \longrightarrow & 1 \end{array}$$

Dabei sind die vertikalen Homomorphismen links surjektiv und die mittleren horizontalen Homomorphismen bijektiv, also ist die Behauptung gezeigt. Man beachte, daß falls $(M) = (a \cdot \mathbb{Z}D_{2^n})$ mit einem $a \in U(\mathbb{Q}D_{2^n})$, $(Me) = ((a \cdot e) \cdot (\mathbb{Z}D_{2^n} \cdot e))$ abgebildet wird und somit die Konjugation mit a auf die Konjugation mit $a \cdot e$ abgebildet wird.

Es ist

$$Outcent(\mathbb{Z}D_{2^n}) \simeq C_{2^{n-1}} \times C_{2^{n-2}} =: < \alpha_n > \times < \beta_n >$$

Sei $\gamma_a(x) = a \cdot x \cdot a^{-1}$ für ein $a \in U(\mathbb{Q}D_{2^n})$ und alle $x \in \mathbb{Z}D_{2^n}$. Aus $\gamma_a(b) = b$ folgt unmittelbar $\gamma_{a \cdot \frac{1}{2} \cdot (1+a^{2^{n-1}})}(b) = b$. Nach den vorangegangenen Untersuchungen kann angenommen werden, daß $1 \times C_{2^{n-2}} \leq Outcent(\mathbb{Z}D_{2^n})$ auf b trivial operiert.

Ohne Beschränkung der Allgemeinheit parametrisiert wieder $C_{2^{n-1}} \times 1$ die ganzzahligen Konjugationsklassen von Gruppenbasen, die die der Standardinvolution b enthalten. Sei β'_n ein Urbild eines Erzeugendes β'_{n-1} von $1 \times C_{2^{n-3}}$ in $Outcent(\mathbb{Z}D_{2^{n-1}})$, das die Standardinvolution b stabilisiert. Da aber β'_{n-1} die Ordnung 2^{n-3} hat, muß β'_n wenigstens die Ordnung 2^{n-3} haben. Hätte β'_n die Ordnung 2^{n-3}, so wäre

$$\beta'_n = \beta_n^j \cdot \alpha_n^i$$

mit natürlichen Zahlen i und j. Da

$$(\beta'_n)^{2^{n-3}} = \beta_n^{j \cdot 2^{n-3}} \cdot \alpha_n^{i \cdot 2^{n-3}} = 1,$$

wäre dann $i \equiv 0 \bmod 4$ und $j \equiv 0 \bmod 2$, also hätte β'_n eine Wurzel

$$\gamma_n := \beta_n^{\frac{j}{2}} \cdot \alpha_n^{\frac{i}{2}},$$

was unter Epimorphie erhalten bleibt. Nun hat aber β_{n-1} keine Wurzel und wir erhalten einen Widerspruch. Dieses Argument zeigt auch, daß $j \not\equiv 0 \bmod 2$, da β'_n die Standardinvolution b fixiert und die Untergruppe der Automorphismen, die die Eigenschaft haben, b zu fixieren, die Ordnung 2^{n-2} hat, und somit $i \equiv 0 \bmod 2$ gilt. Daher hätte dann β_{n-1} eine Wurzel, Widerspruch. Da sowohl β'_n als auch β das Element b fixieren, ist $i \equiv 0 \bmod 2^{n-1}$.

Wir zeigen als nächsten Schritt, daß jedes Urbild α'_n von α_{n-1} in $Outcent(\mathbb{Z}D_{2^n})$ die Ordnung 2^{n-1} hat. Da

$$\pi'_3 \cdot \pi'_4 \cdots \pi'_n : Outcent(\mathbb{Z}D_{2^n}) \longrightarrow\!\!\!\!\!\rightarrow Outcent(\mathbb{Z}D_4)$$

ein Epimorphismus mit β_n im Kern ist, wäre mit

$$\alpha'_n = \alpha_n^{2 \cdot j} \cdot \beta_n^i$$

auch $\alpha_n^{2 \cdot j}$ ein Urbild von α_2. Es ist nämlich, da β_{n-1} im Kern von $\pi'_3 \cdots \pi'_{n-1}$ liegt, α_{n-1} ein Urbild von α_2 in $Outcent(\mathbb{Z}\!\!\mathbb{Z} D_{2^{n-1}})$. Damit ist jedoch α_2 wie $\alpha_n^{2 \cdot j} = (\alpha_n^j)^2$ ein Quadrat. Das ist ein Widerspruch.

Somit erzeugen die Konjugation mit $a - b + 1$ zusammen mit der Konjugation mit $1 + b \cdot (a + a^{-1})$ die Gruppe $Outcent(\mathbb{Z}\!\!\mathbb{Z} D_{2^n})$ für alle $n \in \mathbb{N}$. Die Gruppe $Outcent(\mathbb{Z}\!\!\mathbb{Z} D_{2^n})$ ist somit vollkommen in Gruppenringelementen beschrieben.

Falls die Cohnsche Vermutung nicht richtig ist, so stört das die Diskussion in diesem Unterabschnitt nicht, da die Terme, die durch die Klassengruppen der Ringe $\mathbb{Z}[\eta(n)]$ auftreten, nicht zu Involutionen gehören, die sich in Gruppenbasen befinden. Unsere Einheiten sind aber so angelegt, daß sie den Gruppenring normalisieren und somit Involutionen in Gruppenbasen erzeugen.

Satz 3 *Die äußere zentrale Automorphismengruppe $Outcent(\mathbb{Z}\!\!\mathbb{Z} D_{2^n})$ des ganzzahligen Gruppenrings der Diedergruppe D_{2^n} mit 2^{n+1} Elementen wird erzeugt von der Konjugation mit $a - b + 1$, einem Automorphismus der Ordnung 2^{n-1} modulo inneren Automorphismen, und der Konjugation mit $1 + b \cdot (a + a^{-1})$, einem Automorphismus der Ordnung 2^{n-2} modulo inneren Automorphismen. Dabei ist a ein Element der Ordnung 2^n in D_{2^n} und b eine nicht zentrale Involution in D_{2^n}.*

3.9 Einige ungerade Diedergruppen

Sei D_p die Diedergruppe der Ordnung $2p$ für eine ungerade Primzahl p: $D_p :=< a, b | a^p, b^2, baba >$. Es soll die Klassengruppe des Zentralisators $C(p) := C_{\mathbb{Z}D_p}(b)$ — in Abänderung der Notation — der Involution b von D_p in $\mathbb{Z}D_p$ berechnet werden.

Da $\mathbb{Q}D_p = \mathbb{Q}C_2 \oplus (\mathbb{Q}[\eta(p)])_{2\times 2}$ mit $\eta(p) = \zeta(p) + \zeta(p)^{-1}$ sowie $\sum_{i=0}^{p-1} \zeta(p)^i = 0$, somit ist $\zeta(p)$ eine primitive p-te Einheitswurzel. Dann ist $C(p)$ durch das folgende Pullbackdiagramm bestimmt:

$$\begin{array}{ccc} C_{\mathbb{Z}D_p}(b) & \longrightarrow & \mathbb{Z} < b > \\ \downarrow & & \downarrow \\ \mathbb{Z}[\eta(p)] < b > & \longrightarrow & \mathbb{F}_p < b > \end{array}$$

Da $\mathbb{Z}[\eta(p)] = \mathbb{Z}[\eta(2p)]$, sind sowohl die zyklotomischen Einheiten

$$u_k(p) := 1 + \eta_1(p) + \eta_2(p) + .. + \eta_k(p);\ k = 1, .., \frac{p-3}{2}$$

als auch die Elemente

$$v_k(p) := 1 - \eta_1(p) + \eta_2(p) \pm .. \pm \eta_k(p);\ k = 1, .., \frac{p-3}{2}$$

mit $\eta_i(p) = \zeta(p)^i + \zeta(p)^{-i}$ Einheiten.

Da wir eine Primzahl p fixieren, lassen wir die Bezeichnung '(p)' künftig fort.

Man rechnet

$$\frac{1+b}{2}u_k + \frac{1-b}{2}v_k = \begin{cases} (1 + \eta_2 + \eta_4 + .. + \eta_k) + (\eta_1 + \eta_3 + .. + \eta_{k-1})b & \text{für } k \text{ gerade} \\ (1 + \eta_2 + \eta_4 + .. + \eta_{k-1}) + (\eta_1 + \eta_3 + .. + \eta_k)b & \text{für } k \text{ ungerade} \end{cases}$$

Dies bildet in $\mathbb{F}_p < b >$ auf

$$\begin{cases} (k+1) + k \cdot b & \text{für } k \text{ ungerade} \\ k + (k+1) \cdot b & \text{für } k \text{ gerade} \end{cases}$$

ab. In den Wedderburn Komponenten von $\mathbb{F}_pC_2$ sind diese Elemente gleich

$$\begin{array}{ll} (2k+1, 1) & k \text{ gerade} \\ (2k+1, -1) & k \text{ ungerade.} \end{array}$$

Da aber $b = (1, -1)$ Bild einer globalen Einheit ist, ist $(2k + 1, 1)$ Bild einer globalen Einheit. Da $-b = (-1, 1)$ Bild einer globalen Einheit ist, ist $(\mathbb{F}_p, 1)$ Bild globaler Einheiten, denn falls $x = 2k+1 \Rightarrow -x = 2k'$. Analog ist $(1, \mathbb{F}_p)$ Bild globaler Einheiten und somit ganz $U(\mathbb{F}_p C_2)$.

Somit ist

$$Cl(C_{\mathbb{Z}D_p}(b)) = Cl(\mathbb{Z}[\eta(p)]C_2) \oplus Cl(\mathbb{Z}C_2).$$

Nun ist aber der zweite Summand trivial, und für den ersten Summanden berechnet man den Pullback

$$\begin{array}{ccc} \mathbb{Z}[\eta(p)]C_2 & \longrightarrow & \mathbb{Z}[\eta(p)] \\ \downarrow & & \downarrow \\ \mathbb{Z}[\eta(p)] & \longrightarrow & \mathbb{F}_2 \otimes_{\mathbb{Z}} \mathbb{Z}[\eta(p)] \end{array} .$$

Bemerkung 10 Falls p eine Primzahl ist, für die $2^{\frac{p-1}{2}} - 1$ Mersennesche Primzahl ist und falls $2 \cdot \mathbb{Z}[\eta(p)]$ ein Primideal in $\mathbb{Z}[\eta(p)]$ ist, ist $Cl(\mathbb{Z}[\eta(p)]C_2) = Cl(\mathbb{Z}[\eta(p)])^2$. Denn dann hat die Einheitengruppe von $\mathbb{Z}[\eta(p)]/2\mathbb{Z}[\eta(p)]$ Primzahlordnung und wird damit von allen Elementen außer der 1 erzeugt.

Die Klassengruppe des Zentrums von $\mathbb{Z}D_p$ wurde in [Fr-73, FRU-74] berechnet. Die Argumente werden nun wiederholt:

$$Z(\mathbb{Z}D_p) =< 1, a^i + a^{-i}, (1 + a + a^2 + ... + a^{p-1}) \cdot b | i = 1, .., p - 1 >_{\mathbb{Z}}$$

und daher ist ein Pullbackdiagramm gegeben:

$$\begin{array}{ccc} Z(\mathbb{Z}D_p) & \longrightarrow & \mathbb{Z} + p\mathbb{Z}b \\ \downarrow & & \downarrow \\ \mathbb{Z}[\eta(p)] & \longrightarrow & \mathbb{Z}/(p\mathbb{Z}) \end{array}$$

Es ist somit $Cl(Z(\mathbb{Z}D_p)) \simeq Cl(\mathbb{Z}[\eta(p)]) \oplus Cl(\mathbb{Z} + p\mathbb{Z}b)$. Dies führt auf die Untersuchung des Pullbackdiagramms

$$\begin{array}{ccc} \mathbb{Z} + p\mathbb{Z}b & \longrightarrow & \mathbb{Z} \\ \downarrow & & \downarrow \\ \mathbb{Z} & \longrightarrow & \mathbb{Z}/(2p\mathbb{Z}) \end{array}$$

und zur Mayer-Vietoris-Sequenz

$$1 \longrightarrow C_{\frac{p-1}{2}} \longrightarrow Cl(\mathbb{Z} + p\mathbb{Z}b) \longrightarrow 1.$$

Daher ist

$$Cl(Z(\mathbb{Z}D_p)) \simeq Cl(\mathbb{Z}[\eta(p)]) \oplus C_{\frac{p-1}{2}}.$$

Daß $Picent(\hat{\mathbb{Z}}_q D_p) = 1$ für alle Primzahlen q ist, wird in [FRU-74] bewiesen. Für alle Primzahlen q außer $q = 2$ folgt dies aus [RS-87b] und [RS-87a, (1.2.12)].

Nach [Lee-64, Theorem 4.2] ist

$$Cl(\mathbb{Z}D_p) \simeq Cl(\mathbb{Z}[\eta(p)]).$$

Wir bekommen ein kommutatives Diagramm mit exakten Zeilen und Spalten:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \uparrow & & \uparrow & & & & \\
0 & \longrightarrow & \kappa'_p & \longrightarrow & \kappa'_p & & \longrightarrow & & 0 \\
 & & \uparrow & & \uparrow & & & & \\
0 & \longrightarrow & Cl(C_{\mathbb{Z}D_p}(b)) & \longrightarrow & Cl(\mathbb{Z}[\eta(p)]C_2) \oplus Cl(\mathbb{Z}C_2) & & \longrightarrow & & 0 \\
 & & \uparrow & & \uparrow \lambda & & & & \\
0 & \longrightarrow & Cl(Z(\mathbb{Z}D_p)) & \longrightarrow & Cl(\mathbb{Z}[\eta(p)]) \oplus Cl(\mathbb{Z} + p\mathbb{Z}b) & & \longrightarrow & & 0 \\
 & & \uparrow & & \uparrow & & & & \\
0 & \longrightarrow & \gamma_p & \longrightarrow & \gamma_p & & \longrightarrow & & 0 \\
 & & \uparrow & & \uparrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

Da $\lambda = \lambda e \oplus \lambda(1-e)$ mit $1-e$ die Projektion modulo a und λe sicherlich injektiv ist, ist $\gamma_p \simeq C_{\frac{p-1}{2}}$ und

$$|\kappa'_p| = \frac{|Cl(\mathbb{Z}[\eta(p)])C_2|}{|Cl(\mathbb{Z}[\eta(p)])|}.$$

Es existiert ein kommutatives Diagramm mit exakten Zeilen:

$$\begin{array}{ccccccc}
0 & \longrightarrow & Cl_{\mathbb{Z}D_p}(C_{\mathbb{Z}D_p}(b)) & \longrightarrow & Cl(C_{\mathbb{Z}D_p}(b)) & \xrightarrow{\phi} & Cl(\mathbb{Z}D_p) \\
 & & \uparrow & & \uparrow & & \| \\
0 & \longrightarrow & Cl_{\mathbb{Z}D_p}(Z(\mathbb{Z}D_p)) & \longrightarrow & Cl(Z(\mathbb{Z}D_p)) & \xrightarrow{\phi'} & Cl(\mathbb{Z}D_p)
\end{array}$$

Damit ist

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \kappa_p & \longrightarrow & \kappa_p' & \longrightarrow & \kappa_p'' & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & Cl_{\mathbb{Z}D_p}(C_{\mathbb{Z}D_p}(b)) & \longrightarrow & Cl(C_{\mathbb{Z}D_p}(b)) & \xrightarrow{\lambda} & Cl(\mathbb{Z}[\eta(p)]) & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & Cl_{\mathbb{Z}D_p}(Z(\mathbb{Z}D_p)) & \longrightarrow & Cl(Z(\mathbb{Z}D_p)) & \longrightarrow & Cl(\mathbb{Z}[\eta(p)])^{[2]} & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \gamma_p & \longrightarrow & \gamma_p & \longrightarrow & 0 & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

ein kommutatives Diagramm mit exakten Zeilen und Spalten, wie man aus dem Schlangenlemma unter Verwendung von [FRU-74, (4.3)] sieht. (Zur Bezeichnung siehe Seite 44.) Daher ist

$$ker[Cl_{\mathbb{Z}D_p}(Z(\mathbb{Z}D_p)) \longrightarrow Cl_{\mathbb{Z}D_p}(C_{\mathbb{Z}D_p}(b))] \simeq C_{\frac{p-1}{2}}.$$

Sei ein lokal freies Ideal $\mathcal{A}$ von $\mathbb{Z}[\eta(p)]$ gegeben. Dann induziert das Paar $(\mathcal{A}, \mathbb{Z}[\eta(p)])$ ein Ideal von $C_{\mathbb{Z}D_p}(b)$. Falls $\mathcal{A}$ zu einem Idèle $(\alpha) = \prod_{\wp \in Spec(\mathbb{Z}[\eta(p)])} \alpha_\wp$ gehört, gehört das Idèle

$$\beta := \prod_{\wp} [(1+b)\cdot 1 + (1-b)\cdot \alpha_\wp]$$

zu einem Urbild von $(\mathcal{A}, \mathbb{Z}[\eta(p)])$ in $Cl(C_{\mathbb{Z}D_p}(b))$.

Eine Darstellung von D_p erhält man analog zur Darstellung in [Ro-83] durch:

$$b \longrightarrow \begin{pmatrix} -1 & 0 \\ -\eta(p) & 1 \end{pmatrix},\ a \longrightarrow \begin{pmatrix} 0 & 1 \\ -1 & \eta(p) \end{pmatrix}.$$

Konjugiert man die Darstellung mit $\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$, erhält man die Darstellung

$$b \longrightarrow \begin{pmatrix} -1 & 0 \\ 2-\eta(p) & 1 \end{pmatrix},\ a \longrightarrow \begin{pmatrix} 1 & 1 \\ \eta(p)-2 & \eta(p)-1 \end{pmatrix}.$$

Somit ist

$$(\beta) = \prod_{\wp} \begin{pmatrix} 2\alpha_\wp & 0 \\ (2-\eta(p))\cdot(1-\alpha_\wp) & 2 \end{pmatrix}.$$

Da aber

$$\begin{pmatrix} 1 & 0 \\ (2-\eta(p)) & 2 \end{pmatrix}$$

eine Einheit in $(\mathbb{Q}[\eta(p)])_{2\times 2}$ ist, ist (β) aufgefaßt als Idèle von $(\mathbb{Q}[\eta(p)])_{2\times 2}$ äquivalent zum Idèle

$$\begin{pmatrix} 1 & 0 \\ (2-\eta(p)) & 2 \end{pmatrix} \cdot (\beta) = \prod_{\wp} \begin{pmatrix} 2\alpha_\wp & 0 \\ 2(2-\eta(p)) & 4 \end{pmatrix} =: (\gamma).$$

Falls $R := \mathbb{Z}[\eta(p)]$ abgekürzt wird, ist das zu (γ) gehörige Ideal $\mathcal{C}$ gleich

$$\bigcap_{\wp} \begin{pmatrix} 2\alpha_\wp & 0 \\ 2(2-\eta(p)) & 4 \end{pmatrix} \cdot \begin{pmatrix} R_\wp & R_\wp \\ R_\wp & R_\wp \end{pmatrix}.$$

Dies ist aber gleich

$$\bigcap_{\wp} \begin{pmatrix} 2\alpha_\wp R_\wp & 2\alpha_\wp R_\wp \\ 2(2-\eta(p))R_\wp + 4R_\wp & 2(2-\eta(p))R_\wp + 4R_\wp \end{pmatrix}.$$

Da aber $p \in (2-\eta(p))R$, ist dies gleich

$$\bigcap_{\wp} \begin{pmatrix} 2\alpha_\wp R_\wp & 2\alpha_\wp R_\wp \\ 2R_\wp & 2R_\wp \end{pmatrix} = \begin{pmatrix} 2\mathcal{A} & 2\mathcal{A} \\ 2R_\wp & 2R_\wp \end{pmatrix}.$$

Dessen reduzierte Norm ist dann aber gleich $4 \cdot \mathcal{A} \simeq \mathcal{A}$.

Dadurch ist λ surjektiv und

$$0 \longrightarrow \kappa_p \longrightarrow \kappa_p' \longrightarrow \kappa_p'' \longrightarrow 0$$

ist exakt. Man sieht daher, daß

$$\kappa_p'' \simeq Cl(\mathbb{Z}D_p)/Cl(\mathbb{Z}D_p)^{[2]},\ |\kappa_p'| = \frac{|Cl(\mathbb{Z}[\eta(p)])C_2|}{|Cl(\mathbb{Z}[\eta(p)])|}$$

und

$$|\kappa_p| = \frac{|Cl(\mathbb{Z}[\eta(p)])C_2| \cdot |Cl(\mathbb{Z}[\eta(p)])^{[2]}}{|Cl(\mathbb{Z}[\eta(p)])|^2}$$

und somit

$$|coker[Cl_{\mathbb{Z}D_p}(Z(\mathbb{Z}D_p)) \longrightarrow Cl_{\mathbb{Z}D_p}(C_{\mathbb{Z}D_p}(b))]| =$$
$$= \frac{|Cl(\mathbb{Z}[\eta(p)]C_2)|}{|Cl(\mathbb{Z}[\eta(p)])|^2} \cdot |Cl(\mathbb{Z}[\eta(p)])^{[2]}|.$$

Bemerkung 11 N. C. Ankeney, S. Chowla und H. Hasse beweisen in [ACH-65], daß für Primzahlen p von der Form $p = (2qn)^2 + 1$ mit einer Primzahl q und einer ganzen Zahl $n > 1$ die Klassenzahl $H(p) := |Cl(\mathbb{Z}[\sqrt{p}])|$ die Klassenzahl $h^+(p)$ teilt. Zum Anderen ist aber $H(p)$ ungerade und größer als 1 für diese Primzahlen p. Beispiele sind die Primzahlen

$$p \in \{257, 401, 577, 1297, 1601, 2917, 3137, 4357, 7057, 8101\}.$$

Es ist aber $(Cl(\mathbb{Z}[\eta(p)]))_{[2]} = Cl(\mathbb{Z}[\eta(p)])$ genau dann, wenn $Cl(\mathbb{Z}[\eta(p)])$ eine elementarabelsche 2-Gruppe ist. In jedem Fall ist aber

$$|Cl(\mathbb{Z}[\eta(p)])C_2|/|Cl(\mathbb{Z}[\eta(p)])| \geq |Cl(\mathbb{Z}[\eta(p)])|.$$

Zur Erinnerung sei noch einmal eines der Ergebnisse von A. Fröhlich, I. Reiner und S. Ullom angegeben.

Lemma 15 *([FRU-74]) $\mathbb{Z}D_p$ besitzt genau*

$$\frac{p-1}{2} \cdot \frac{|Cl(\mathbb{Z}[\eta(p)])|}{|Cl(\mathbb{Z}[\eta(p)])^{[2]}|}$$

Konjugationsklassen von Gruppenbasen.

Wir haben also bewiesen:

Satz 4 *1. Es existieren in $\mathbb{Z}D_p$ genau*

$$\frac{|Cl(\mathbb{Z}[\eta(p)]C_2)|}{|Cl(\mathbb{Z}[\eta(p)])|}$$

Konjugationsklassen von Involutionen, die lokal und rational zu b konjugiert sind.

2. *Eine Involution $b \in D_p$ ist in genau $\frac{p-1}{2}$ Repräsentanten von Konjugationsklassen von Gruppenbasen enthalten.*

3. *Von den Konjugationsklassen lokal und rational zu b konjugierter Involutionen in $\mathbb{Z}D_p$ bestehen dann genau*

$$\frac{|Cl(\mathbb{Z}[\eta(p)])|}{|Cl(\mathbb{Z}[\eta(p)])^{[2]}|}$$

Konjugationsklssen aus Involutionen, die in einer Gruppenbasis liegen und

$$\frac{|Cl(\mathbb{Z}[\eta(p)]C_2)|}{|Cl(\mathbb{Z}[\eta(p)])|} - \frac{|Cl(\mathbb{Z}[\eta(p)])|}{|Cl(\mathbb{Z}[\eta(p)])^{[2]}|}$$

bestehen aus nicht in Gruppenbasen liegenden Involutionen.

4. *Falls* $p \in \{(2nq)^2 + 1 | n \in \mathbb{Z}, n \geq 2, q\mathbb{Z} \in Spec(\mathbb{Z})\}$ *Primzahl ist, existiert eine Konjugationsklasse von Involutionen, deren Elemente in* $V(\hat{\mathbb{Z}}_r D_p)$ *für alle Primzahlen* r *konjugiert zu* b *sind, die aber in keiner Gruppenbasis von* $\mathbb{Z}D_p$ *liegen.*

Bemerkung 12 I. S. Luthar und A. K. Bhandari zeigten in [LB-83] schon 1983, daß rational jede Involution in $\mathbb{Z}D_p$ zu b konjugiert ist.

3.10 Anhang

Mit dem 'maple V' Programm konnten für einige Primzahlen p der Wert $|Cl(\mathbb{Z}[\eta(p)]C_2)|$ berechnet werden. Für $p \in \{3, 5, 7, 11, 179, 19379, 43403\}$ ist

$$Cl(\mathbb{Z}[\eta(p)]C_2) = Cl(\mathbb{Z}[\eta(p)])^2,$$

da dafür $2^{\frac{p-1}{2}} - 1$ Mersennesche Primzahl ist. Insbesondere konnte, falls 2 ein Primideal in $\mathbb{Z}[\eta(p)]$ erzeugt, geprüft werden, wie groß der Index der von den cyclotomischen Einheiten $U_C(p)$ von $\mathbb{Z}[\eta(p)]$ in $\mathbb{Z}[\eta(p)]/2\mathbb{Z}[\eta(p)]$ erzeugten Untergruppe ist.

Dabei ergibt sich für die Primzahlen p in $\{3, 5, 7, 11, 13, 19, 23, 29, 47, 53, 59, 61, 67, 71, 79, 83, 103, 107, 131, 139, 149, 163, 167, 173, 179, 181, 191, 211, 227, 239, 263, 271, 293, 311, 317, 347, 359, 367, 379\}$ die Beziehung

$$Cl(\mathbb{Z}[\eta(p)]C_2) \simeq Cl(\mathbb{Z}[\eta(p)])^2.$$

Für die Primzahlen p in $\{37, 101, 197, 199, 269, 349, 373\}$ kann die Beziehung nur dann richtig sein, wenn $|Cl(\mathbb{Z}[\eta(p)])| > 1$ ist.

Bezüglich den Primzahlen p in $\{17, 31, 41, 43, 73, 89, 97, 109, 113, 127, 137, 151, 157, 193, 223, 229, 233, 241, 251, 257, 277, 281, 283, 307, 313, 331, 337, 353\}$ konnte keine Entscheidung getroffen werden, da dann 2 kein Primideal in $\mathbb{Z}[\eta(p)]$ erzeugt.

Es ist von van der Linden ([vdL-82]) gezeigt, daß $h^+_{163} = 4$ und $h^+_p = 1$ für alle Primzahlen $p < 163$ gilt, falls die verallgemeinerte Riemann Vermutung richtig ist. Für Primzahlen $p \leq 67$ ist die verallgemeinerte Riemann Vermutung nicht nötig. Viele Fälle konnte schon früher J. M. Masley in [Ma-78] behandeln.

Korollar 4 *Wir setzen voraus, daß das 'maple V' Progamm fehlerlos ist. Aussagen über Primzahlen größer als 67 setzen die vrallgemeinerte Riemann Vermutung voraus.*

1. *Falls* $p \in \{3, 5, 7, 11, 13, 19, 23, 29, 47, 53, 59, 61, 67, 71, 79, 83, 103, 107, 131, 139, 149\}$*, liegt jede Involution in* $\mathbb{Z}D_p$*, die lokal zu b konjugiert ist, auch ganzzahlig in einer Gruppenbasis.*

2. *Falls* $p \in \{37, 101\}$ *existieren in* $\mathbb{Z}D_p$ *genau zwei Konjugationsklassen von Involutionen, die rational und lokal zu b konjugiert sind, ganzzahlig jedoch nicht in einer Gruppenbasis liegen. Genau die Konjugationsklasse von b besteht aus Involutionen, die in Gruppenbasen liegen.*

3. *Falls* $Cl(\mathbb{Z}[\eta(163)])$ *zyklisch ist, existieren in* $\mathbb{Z}D_{163}$ *genau 2 Konjugationsklassen von Involutionen, die rational und lokal zu b konjugiert sind, ganzzahlig jedoch in keiner Gruppenbasis liegen, und 2 Konjugationsklassen von Involutionen, die rational und lokal zu b konjugiert sind und in einer Gruppenbasis liegen. Sonst liegen alle Involutionen, die lokal und rational zu b konjugiert sind, in* $\mathbb{Z}D_{163}$ *in einer Gruppenbasis.*

In der folgenden Tabelle sei $U_C(p)$ die Gruppe der zyklotomischen Einheiten in $\mathbb{Z}[\eta(p)]$ und $U_C(p)$ mod 2 bezeichnet deren Bild in $\mathbb{Z}[\eta(p)]/2\mathbb{Z}[\eta(p)]$. Bekanntlich haben die zyklotomischen Einheiten in der gesamten Einheitengruppe den Index h^+_p.

Primzahl	$< 2 >$ prim in $\mathbb{Z}[\eta(p)]$	$\frac{\lvert U(\mathbb{Z}[\eta(p)]/2\mathbb{Z}[\eta(p)])\rvert}{\lvert U_C(p) \bmod 2\rvert}$
3	ja	1
5	ja	1
7	ja	1
11	ja	1
13	ja	1
17	nein	
19	ja	1
23	ja	1
29	ja	1
31	nein	
37	ja	3
41	nein	
43	nein	
47	ja	1
53	ja	1
59	ja	1
61	ja	1
67	ja	1
71	ja	1
73	nein	
79	ja	1
83	ja	1
89	nein	
97	nein	
101	ja	3
103	ja	1
107	ja	1
109	nein	
113	nein	
127	nein	
131	ja	1
137	nein	
139	ja	1
149	ja	1
151	nein	

Primzahl	$< 2 >$ prim in $\mathbb{Z}[\eta(p)]$	$\frac{\lvert U(\mathbb{Z}[\eta(p)]/2\mathbb{Z}[\eta(p)])\rvert}{\lvert U_C(p) \bmod 2\rvert}$
157	nein	
163	ja	1
167	ja	1
173	ja	1
179	ja	1
181	ja	1
191	ja	1
193	nein	
197	ja	3
199	ja	7
211	ja	1
223	nein	
227	ja	1
229	nein	
233	nein	
239	ja	1
241	nein	
251	nein	
257	nein	
263	ja	1
269	ja	3
271	ja	1
277	nein	
281	nein	
283	nein	
293	ja	1
307	nein	
311	ja	1
313	nein	
317	ja	1
331	nein	

Primzahl	$< 2 >$ prim in $\mathbb{Z}[\eta(p)]$	$\frac{\lvert U(\mathbb{Z}[\eta(p)]/2\mathbb{Z}[\eta(p)])\rvert}{\lvert U_C(p) \bmod 2\rvert}$
337	nein	
347	ja	1
349	ja	3
353	nein	
359	ja	1
367	ja	1
373	ja	3
379	ja	1

Die Programme hierzu sind nachfolgend aufgelistet. Vor der Anwendung muß das Programmpaket GF mit 'readlib(lattice);readlib(GF);' gestartet werden.

```
fangean:=proc(p)
local i,j;
q := 1/2*p-1/2;
a := array(0 .. q+1,0 .. q+1);
for i from 0 to q+1 do for j from 0 to q+1 do a[i,j] := 0 od od;
a[0,0] := 1;
a[1,1] := 1;
for i from 2 to q do
if a[i-1,0] = 0 then
a[i,0] := 2*a[i-1,1];
for j from 2 by 2 to q do a[i,j] := a[i-1,j-1]+a[i-1,j+1]
od
else for j by 2 to q do a[i,j] := a[i-1,j-1]+a[i-1,j+1] od
fi
od
end

test:= proc(p)
local n,ord,i;
n:=1; ord:=0;
for i to p do n:=(2*n) mod p;
if (n=1) or (n=p-1) then ord:=i; i:=p fi
od;
ord:=ord
```

```
end;

zweiprim:=proc(p)
local L;
L:=GF(p,1);
zwei:=L[‘+‘](L[1],L[1]);
Laenge:=member(L[order](zwei),p-1);
if not Laenge then
if test(p)=1/2 * p - 1/2 then Laenge:=true
else Laenge:=false
fi
fi
end;

diesmipol:=proc(p)
local i;
berminpoly(p); mu := 0; for i from 0 to q do mu := c[i]*Z^i+mu od
end

berminpoly:=proc(p)
local i,b,j,k;
fangean(p);
c := array(0 .. q);
b := array(0 .. q);
for i from 0 to q do c[i] := 0; b[i] := -a[q,i]+1 od;
c[q] := 1;
for i from 0 to q-1 do
j := q-i-1;
c[j] := b[j];
for k from 0 to q do b[k] := b[k]-a[j,k]*c[j] od
od
end

verbessertsys:=proc(p)
local gegete,G,pol,ar,potenz,i,j,agfield,ordnung,quotientenord;
zweiprim(p);
gegete := 1;
if Laenge then
```

```
pol := diesmipol(p);
G := GF(2,1/2*p-1/2,pol);
al := G[ConvertIn](Z);
ar := array(1 .. 1/2*p-3/2);
agfield := array(0 .. 1/2*p-1/2,0 .. 1/2*p-1/2);
potenz := array(0 .. 1/2*p-3/2);
for i from 0 to 1/2*p-1/2 do
for j from 0 to 1/2*p-1/2 do agfield[i,j] := G[ConvertIn](a[i,j] mod 2) od
od;
potenz := array(0 .. 1/2*p-3/2);
potenz[0] := G[1];
for i to 1/2*p-3/2 do potenz[i] := G[‘*‘](potenz[i-1],al); ar[i] := potenz[i] od;
for i from 2 to 1/2*p-3/2 do
for j to i-1 do ar[i] := G[‘+‘](ar[i],G[‘*‘](agfield[i,j],ar[j])) od
od;
ar[1] := G[‘+‘](G[1],ar[1]);
for i from 2 to 1/2*p-3/2 do ar[i] := G[‘+‘](ar[i],ar[i-1]) od;
quotientenord := 2^(1/2*p-1/2)-1;
for i to 1/2*p-3/2 do
ordnung := G[order](ar[i]);
gegete := ilcm(ordnung,gegete);
if ordnung = quotientenord then print(‘Einheit Nr‘,i,‘ erzeugt‘); i := 1/2*p-
3/2
else
if gegete = quotientenord then print(‘cyclotomische Einheiten erzeugen‘); i
:= 1/2*p-3/2
fi
fi
od;
if gegete <> quotientenord then
print(‘cyclotomische Einheiten werden von ‘,gegete,‘ annuliert‘,
‘erzeugen Untergruppe vom Index‘,quotientenord/gegete)
fi
else print(‘< 2 > ist nicht primes Ideal‘)
fi
end
```

Literatur

[ACH-65] N.C. Ankeney, S. Chowla, H. Hasse: On the class number of the maximal real subfield of a cyclotomic field; J. reine angew. Math. 217 (1965), 217–220.

[CR-82-87] C.W. Curtis, I. Reiner: Methods of Representation Theory; Vol. 1, 2; Wiley 1982 & 1987.

[Co-60] H. Cohn: A numerical study of Weber's real class number calculation; Numerische Mathematik 2 (1960), 347–362.

[CW-82] G. Cornell, L. C. Washington: Class Numbers of Cyclotomic Fields; J. Number Theory 21 (1985), 260–274.

[CN-76] P. Cassou-Nouguès: Groupe des Classes de l'Algèbre d'un Groupe Métacyclique; J. Algebra 41 (1976), 116–136.

[EMS-82] S. Endo, T. Miyata, K. Sekiguchi: Picard Groups and Automorphism Groups of Metacyclic Groups, J. Algebra 77 (1982), 286–310.

[Fr-73] A. Fröhlich: The Picard group of noncommutative rings, in particular of orders; Transactions of the Amer. Math. Soc. 180 (1973), 1–45.

[FKW-74] A. Fröhlich, M.E. Keating, S.M.J. Wilson: The Class Group of Quaternion and Dihedral 2–Groups; Mathematika 21 (1974), 64–71.

[FRU-74] A. Fröhlich, I. Reiner, S. Ullom: Class groups and Picard groups of orders; Proc. London Math. Soc. (3) 29 (1974), 405–434.

[GRU-72] S. Galovich, I. Reiner, S. Ullom: Class groups for integral representations of metacyclic groups; Mathematika 19 (1972), 105–111.

[GVS-91] A. Giambruno, A. Valenti, S.K. Sehgal: Automorphisms of the integral group rings of some wreath products; Comm. in Alg. 19 (2) (1991), 519–534.

[GR-87a] W. Gustafson, K.W. Roggenkamp: A Mayer Vietoris sequence for Picard groups, with applications to integral group rings of dihedral and quaternion groups, Reiner memorial volume of Ill. J. of Math. (1987).

[GR-87b] W. Gustafson, K.W. Roggenkamp: Automorphisms and Picard groups for Hereditary Orders; Visiting Scholar's Lectures (1988), Texas Tech Univ.

[Ha-49] H. Hasse: Zahlentheorie; Akademie Verlag Berlin 1949.

[Ha-65] H. Hasse: Über mehrklassige, aber eingeschlechtige reell-quadratische Zahlkörper; Elem. Math. 20 (1965), 49–72.

[Hi-39] G. Higman: The Units in Group Rings; Dr. phil. thesis, Oxford University (1939).

[HP-72] I. Hughes, K. E. Pearson: The group of units in the group ring $\mathbb{Z}\mathbb{Z}S_3$; Can. Math. Bull. 15 (1972), 529–534.

[Hu-67] B. Huppert: Endliche Gruppen 1; Springer 1967.

[Ja-69] D. A. Jackson: The group of units in the integral group ring of finite metabelian and finite nilpotent groups; Quart. J. Math. Oxford (2) 20 (1969), 313–319.

[Ke-74] M. E. Keating: Class groups of metacyclic groups of order $p^r q$, p a regular prime; Mathematika 21 (1974), 90–95.

[Ki-92a] W. Kimmerle: More on the Class sum correspondence; section VI in [RT-92], ed. K.W. Roggenkamp und M.J. Taylor.

[Ki-92b] W. Kimmerle: Variations of the Zassenhaus conjecture; section X in [RT-92], ed. K.W. Roggenkamp und M.J. Taylor.

[Lee-64] M. P. Lee: Integral representations of dihedral groups of order $2p$; Transactions of the Amer. Math. Soc. 110 (1964), 213–231.

[LB-83] I. S. Luthar, A. K. Bhandari: Torsion Units of Integral Group Rings of Metacyclic Groups; J. Number Theory 17 (1983), 270–283.

[LT-90] I.S. Luthar, P. Trama: Zassenhaus-conjecture for certain integral group rings; J. Indian Math. Soc. 55 (1990) no. 1–4, 199–212.

[LP-92] I.S. Luthar, I.B.S. Passi: Torsion Units in Matrix Group Rings; Comm. Alg. 20 (4) (1992), 1223–1228.

[MRSW-87] Z. Marciniak, J. Ritter, S.K. Sehgal, A. Weiss: Torsion Units in Integral Group Rings of Some Metabelian Groups, II; J. Number Theory 25 (1987), 340–352.

[Ma-78] J. M. Masley: Class numbers of real cyclic number fields with small conductor; Compositio Math. 37 Fasc. 3 (1978), 297–319.

[Mil-71] J. Milnor: Introduction to algebraic K-Theory; Ann. Math. Studies 72, Princeton Univ. Press 1971.

[Miy-80] T. Miyata: On the units of the integral group ring of a dihedral group; J. Math. Soc. Japan 32 No. 4 (1980), 703–708.

[Pa-65] D.S. Passman: Isomorphic Groups and Group Rings, Pac. J. Math. (2) 35 (1965), 561–583.

[PM-74] C. Polcino Milies: The Group of Units of the Integral Group Ring $\mathbb{Z}D_4$; Bol. Soc. Brasil. Math. 4 (1974), 85–92.

[RU-74] I. Reiner, S. Ullom: A Mayer-Vietoris Sequence for Class Groups; J. Algebra 31 (1974), 305–342.

[Ro-80] K.W. Roggenkamp: Metabelian group rings and extension categories; Can. J. Math. 32 No. 2 (1980), 449–459.

[Ro-83] K.W. Roggenkamp: Automorphisms and isomorphisms of integral group rings of finite groups; in Groups – Korea 1983, Springer LNM 1098, 118–135, 1984.

[Ro-89] K.W. Roggenkamp: The isomorphism problem and related topics; Bayreuther Mathematische Schriften 33 (1989), 173–196.

[Ro-92] K. W. Roggenkamp: Subgroup Rigidity of p-adic group rings; erscheint in J. London Math. Soc. (1992).

[RS-86] K.W. Roggenkamp, L.L. Scott: The isomorphism theorem for integral group rings of finite nilpotent on abelian groups; preprint, 1986.

[RS-87a] K.W. Roggenkamp, L.L. Scott: Isomorphisms of p-adic group rings; Annals of Mathematics 126 (1987), 593–647.

[RS-87b] K.W. Roggenkamp, L.L. Scott: A strong answer to the isomorphism problem for finite p–solvable groups with a normal p–subgroup containing its centralizer; Manuskript, 1987.

[RS-87c] K.W. Roggenkamp, L.L. Scott: On a conjecture of Zassenhaus for finite group rings; Manuskript, 1987.

[RT-92] K.W. Roggenkamp, M.J. Taylor: Group Rings and Class Groups; Basel, 1992.

[RZ-91] K.W. Roggenkamp, A. Zimmermann: On the Isomorphism Problem for Integral Group Rings of Finite Groups; (1991), erscheint in Arch. d. Math.

[Sch-28] K. Schaffenstein: Tafel der Klassenzahlen der reellen quadratischen Zahlkörper mit Primzahldiskriminante unter 12000 und zwischen 100000–101000 und 1000000–1001000; Math. Ann. 98 (1928), 745–748.

[Sc-85] L.L. Scott: Brief an K.W. Roggenkamp; 13. Juni 1985.

[Sc-87] L.L. Scott: Recent progress on the isomorphism problem; Proc. in Symposia in Pure Mathematics 47 (1987), 259 – 273.

[Sc-90] L.L. Scott: Defect groups and the isomorphism problem; Représentations linéaires des groupes finis. Proc. Colloq. Luminy, Fr. 1988, Asterisque (1990), 181 – 182.

[SWW-83] E. Seah, L. C. Washington, H. Williams: The Calculation of a Large Cubic Class Number With an Application to Real Cyclotomic Fields; Math. Comp. 41 (1983), 303–305.

[Se-83] S.K. Sehgal: Torsion units in integral group rings; Proc. Nato Institute on Methods in Ring Theory, Antwerp, D. Riedel, Dordrecht (1983), 497–504.

[SSZ-84] S. K. Sehgal, S. K. Sehgal, H. J. Zassenhaus: Isomorphism of Integral Group Rings of Abelian by Nilpotent Class Two Groups; Comm. in Alg. 12 (19), 2401–2407.

[Sw-60] R.G. Swan: Induced representations and projective modules; Annals of Mathematics 71 (1960), 552–578.

[Sw-62] R.G. Swan: Projective modules over group rings and maximal orders; Annals of Mathematics (2) 76 (1962), 55-61.

[Sw-63] R.G. Swan: Grothendieck ring of a finite group; Topology 2 (1963), 85–110.

[Ta-84] M. J. Taylor: Classgroups of Group Rings; Cambridge 1984.

[Th-89] G. Thompson: On the conjugacy of group bases; Ph. D. thesis, Univ. of Virginia 1989.

[Va-92] A. Valenti: On the automorphism group of the integral group ring of S_k wr S_n; J. Pure and Appl. Alg. 78 (1992), 203–211.

[vdL-82] F. J. van der Linden: Class Number Computations of Real Abelian Number Fields; Math. Comp. 39 no.160 (1982), 693–707.

[Wa-82] L. C. Washington: Introduction to Cyclotomic Fields; Springer New York Heidelberg Berlin 1982.

[Web-1886] H. Weber: Theorie der abelschen Zahlkörper; Acta Math. 8 (1886), 193–263.

[Wei-88] A. Weiss: Rigidity of p-adic p-torsion; Annals of Mathematics 127 (1988), 317–332.

[Wei-91] A. Weiss: Torsion units in integral group rings; J. reine angew. Math. 415 (1991), 175–187.

[Wh-68] Whitcomb: The group ring problem; Ph. D. thesis, University of Chicago 1968.

[Zi-90] A. Zimmermann: Das Isomorphieproblem ganzzahliger Gruppenringe für Gruppen mit abelschem Normalteiler und Quotienten, der eine Vermutung von Hans Zassenhaus erfüllt; Diplomarbeit, Universität Stuttgart (1990).

Lebenslauf

Name: Alexander Zimmermann,
geboren am 4. Januar 1964 in Stuttgart.
Eltern: Alfred Zimmermann und Marianne Zimmermann geborene Raber.
Eichbergschule in Musberg vom September 1970 bis 1974.
Philipp Matthäus Hahn Gymnasium in Echterdingen vom September 1974 bis September 1975.
Immanuel Kant Gymnasium in Leinfelden vom September 1975 bis Juni 1983.
Reifeprüfung: ebenda Juni 1983.
Wehrdienst vom 1. Juli 1983 bis 30. September 1984.
Beginn des Studiums der Mathematik an der Universität Stuttgart im Wintersemester 1984/85.
Vordiplom im Sommersemester 1986 in Stuttgart.
Diplom am 22. Mai 1990 an der Universität Stuttgart.
Wissenschaftlicher Mitarbeiter des Mathematischen Instituts B der Universität Stuttgart seit Juni 1990.
Preis bei der Studentenkonferenz Mathematik '91 an der Humboldt Universität zu Berlin im März 1991.