Contributions to the integral representation theory of groups

Martin Hertweck

Habilitationsschrift, approved by
the Faculty of Mathematics and Physics
University of Stuttgart, 2004

Je sais bien que le lecteur n'a pas grand besoin de savoir tout cela, mais j'ai besoin, moi, de le lui dire.

Jean-Jacques Rousseau
Les Confessions – Livre I, 1782

2000 *Mathematics Subject Classification.*
20C05 Group rings of finite groups and their modules
20C07 Group rings of infinite groups and their modules
20C10 Integral representations of finite groups
16S34 Group rings
16U60 Units, groups of units
16U70 Center, normalizer (invariant elements)

Keywords and Phrases.
group, automorphism, unit group, integral representation theory, isomorphism problem, normalizer problem, Zassenhaus conjecture

This thesis is available as an online publication at

`http://elib.uni-stuttgart.de/opus`

Contents

Notation v

Zusammenfassung (German summary) vii

Summary 1

I. On the isomorphism problem for integral group rings 16
1. Local–global considerations . . . 16
2. Mazur's construction adapted to finite groups . . . 20
3. Semilocal analysis of the counterexample . . . 25
4. A group-theoretical problem related to the isomorphism problem . . . 33
5. Automorphisms of group rings of abelian by nilpotent groups . . . 38

II. On the Zassenhaus conjecture 42
6. Some general observations . . . 42
7. A pullback diagram for integral group rings . . . 48
8. Semilocal counterexamples . . . 59
9. Group- and character table automorphisms of $(\mathbb{Z}/r\mathbb{Z}) \wr S_n$ . . . 64

III. Automorphisms of integral group rings: local–global considerations 74
10. General considerations and the groups of Blanchard . . . 74
11. Two groups lead to global counterexamples . . . 78
12. . . . but not the third one . . . 80
13. Bicyclic units and torsion . . . 99

IV. Some results on specific automorphism groups 102
14. Class-preserving automorphisms . . . 102
15. Coleman automorphisms . . . 105
16. Subdirect products of finite groups . . . 112

V. On the normalizer problem for infinite groups 126
17. Normalizers of group bases: general coefficients . . . 126
18. Normalizers of group bases: G-adapted coefficients . . . 134

19. Groups satisfying the normalizer property 136
20. Trivial central units 142

VI. Hypercentral units in integral group rings **145**
21. Hypercentral units and Q*-groups 145
22. Groups with nontrivial intersection of their non-normal subgroups 147
23. The hypercenter and unipotent elements 150
24. Subgroups of a group basis which are normal in the unit group 154
25. Non-central elements of the hypercenter 157

VII. Finite conjugacy for orders in division rings **160**
26. The finite conjugacy center and the second center 160
27. On the finite conjugacy center 163
28. Division rings of dimension greater than 4 over the center 165
29. Division rings of dimension 2 over the center 168

VIII. Central units in p-blocks **173**
30. On Robinson's unit 173

Bibliography **181**

Notation

Abbreviations

Aut	automorphism group
Inn	inner automorphism group
conj	conjugation
det	determinant
dim	dimension
End	endomorphism ring
id	identity
Irr	irreducible
ker	kernel
Out	outer automorphism group
supp	support
Tr	trace

Set Theory

$\|A\|$	number of elements in set A
$f\|_A$	restriction of function f to set A

Miscellaneous

$\mathbb{N}$	natural numbers
$\mathbb{Z}$	rational integers
$\mathbb{Z}_{(p)}$	localization $\{a/b \mid a, b \in \mathbb{Z}, p \nmid b\}$
$\mathbb{Z}_p$	p-adic integers
$\mathbb{Z}_\pi$	semilocalization $\bigcap_{p\in\pi} \mathbb{Z}_{(p)}$
$\mathbb{Q}$	rational field
$\mathbb{C}$	complex field
$\mathbb{F}_q$	finite field with q elements

Linear Algebra

$\mathrm{Mat}_n(R)$	ring of $n \times n$ matrices over ring R
$\mathrm{GL}_n(R)$	group of invertible $n \times n$ matrices over R
$\mathrm{SL}_n(R)$	$\{X \in \mathrm{GL}_n(R) \mid \det(X) = 1\}$
char.pol(M)	characteristic polynomial of matrix M
$\mathrm{diag}(a_1, \dots)$	diagonal matrix with diagonal entries $a_1, \dots$

Group Theory

$H \leq G$	subgroup inclusion
$H < G$	proper subgroup inclusion
$H \trianglelefteq G$	H is normal subgroup of G
$H \lhd G$	H is proper normal subgroup of G
$\|G : H\|$	index of H in G
$\langle x \rangle$	cyclic group generated by x
C_n	a cyclic group of order n
$\langle x, y, \dots \rangle$	group generated by the elements $x, y, \dots$
$G_1 \times G_2$	direct product of groups
$N \rtimes K$	semidirect product of normal subgroup N with subgroup K

G/N	factor group of G by normal subgroup N
$\mathrm{C}_G(H)$	centralizer of H in G
$\mathrm{N}_G(H)$	normalizer of H in G
$\pi(G)$	set of prime divisors of $\lvert G\rvert$
x^y	conjugation $y^{-1}xy$
$[x,y]$	commutator $x^{-1}y^{-1}xy$
$\mathrm{Z}(G)$	center of G
$\mathrm{O}_p(G)$	largest normal p-subgroup of G
$\mathrm{O}_{p'}(G)$	largest normal p'-subgroup of G
$\bar{G}, \tilde{G}, \ldots$	homomorphic images of G ("bar convention")
$\mathrm{F}(G)$	Fitting subgroup of G
$\mathrm{F}^*(G)$	generalized Fitting subgroup of G
$\Delta(G)$	FC-center of G
$\Delta^+(G)$	set of torsion elements of $\Delta(G)$
$\mathrm{Z}_n(G)$	n-th term of upper central series of G
$\mathrm{Z}_\infty(G)$	hypercenter $\bigcup_i \mathrm{Z}_i(G)$
$\mathrm{R}(G)$	intersection of the non-normal subgroups of G
proj lim	projective limit
$\mathrm{Aut}_\mathrm{c}(G)$	group of class-preserving automorphisms of G
$\mathrm{Aut}_\mathrm{Col}(G)$	group of Coleman automorphisms of G
$\mathrm{Aut}_R(G)$	group of automorphisms inducing inner automorphisms of RG
$\mathrm{PAut}(G)$	group of power automorphisms of G
$\mathrm{AutCT}(G)$	automorphism group of character table of G

Ring Theory

$\Lambda^\times$	group of units of ring Λ
RG	group ring of group G over commutative ring R
$R[G]$	R-span of G
$\mathrm{U}(RG)$	group of units of RG
$\mathrm{V}(RG)$	group of units of RG of augmentation 1
$\mathrm{I}_R(G)$	augmentation ideal of RG
$\mathrm{I}_R(N)G$	kernel of natural map $RG \to RG/N$
$\hat{M}$	sum of elements of set M in group ring
ϵ_N	idempotent $\frac{1}{\lvert N\rvert}\sum_{n\in N} n$
η_N	idempotent $1-\epsilon_N$
$\mathrm{Aut}_\mathrm{n}(RG)$	group of augmentation-preserving automorphisms of RG
$\mathrm{Autcent}(\Lambda)$	group of central automorphisms of Λ
$\mathrm{Cl}(\Lambda)$	locally free class group of Λ
$\mathrm{Picent}(\Lambda)$	Picard group of Λ relative to the center

Zusammenfassung (German summary)

Longum iter est per praecepta, breve et efficax per exempla.

Lucius Annaeus Seneca
Epistulae Morales ad Lucilium – Liber VI, 62–65

"Darstellungstheorie" ist, grob gesprochen, "Modultheorie". Eine der Hauptaufgaben der *ganzzahligen* Darstellungstheorie sollte die Konstruktion von unzerlegbaren Gittern über Ordnungen sein. Ein prominentes Beispiel einer $\mathbb{Z}$-Ordnung ist der ganzzahlige Gruppenring $\mathbb{Z}G$ einer endlichen Gruppe G. Ein grundlegendes Problem (mit dem wir es hier jedoch *nicht* zu tun haben werden) ist, einen vollständigen Satz von Invarianten (unter Isomorphie) eines $\mathbb{Z}G$-Gitters M zu finden welcher die Isomorphieklasse von M eindeutig bestimmt.

Man kann sich $\mathbb{Z}G$, oder allgemeiner die ganzzahlige Darstellungstheorie, als ein Bindeglied zwischen gewöhnlicher und modularer Darstellungstheorie vorstellen. (Diese "Allgemeinheit" läßt bereits erkennen, dass die Klärung der Struktur von $\mathbb{Z}G$ im allgemeinen eine delikate Aufgabe ist.) Einen Schritt weitergehend können wir uns ganzzahlige Darstellungstheorie, im Sinne von Curtis und Reiner [28, 27], als einen zentralen Kern vorstellen, welcher verschiedene Themen in gewöhnlicher und modularer Darstellungstheorie, algebraischer Zahlentheorie, und algebraischer K-Theorie verbindet. Dieser Standpunkt wird in Kapitel III veranschaulicht, wo wir anhand eines Beispiels lokal–global Aspekte in Bezug auf Automorphismen von ganzzahligen Gruppenringen erörtern werden.

In der Darstellungstheorie ist es üblich über $\mathbb{Z}G$-Moduln zu sprechen und dabei die ausgezeichnete Gruppenbasis G ausdrücklich im Auge zu haben. (Andernfalls, was sollte es bedeuten dass M ein Permutationsmodul ist?) Wir können jedoch die verschiedenen Möglichkeiten wie G, als Gruppenbasis, in $\mathbb{Z}G$ eingebettet werden kann in Betracht ziehen: Dies führt zu Fragen über Ringautomorphismen von $\mathbb{Z}G$, von denen die sogenannte "Zassenhaus-Vermutung" die beachtenswerteste ist. Wir können auch fragen welche Eigenschaften einer endlichen Gruppe G durch ihre ganzzahligen Darstellungen bestimmt sind. Ob die Gruppe G bis auf Isomorphie durch ihren ganzzahligen Gruppenring bestimmt ist, ist das sogenannte "Isomorphieproblem für ganzzahlige Gruppenringe". Diese Fragestellungen sind sicherlich im Sinne einiger wohlbekannter Probleme die Richard

Brauer [18] zur Diskussion stellte, und sie waren Ende des vergangenen Jahrhunderts der Gegenstand vieler Forschung. Wir werden die "semilokale Version" des Isomorphieproblems und der Zassenhaus-Vermutung in den ersten beiden Kapiteln eingehend besprechen. Dabei wird der Koeffizientenring der ganzen Zahlen $\mathbb{Z}$ ersetzt durch eine geeignete Semilokalisation $\mathbb{Z}_\pi$ von $\mathbb{Z}$ (die gleich eingeführt wird), so dass Fragen über lokal freie Klassengruppen vermieden werden.

Kenntnis der p-adischen Gruppenringe $\mathbb{Z}_pG$ gibt Einblick wie G auf abelschen Gruppen operieren kann. Da die interessantesten arithmetischen Eigenschaften beim Übergang von $\mathbb{Z}G$ zu einer maximalen Überordnung in $\mathbb{Q}G$ verloren gehen, sind wir versucht, die Semilokalisation

$$\mathbb{Z}_\pi := \bigcap_{p||G|} \mathbb{Z}_{(p)}$$

als angemessenen "ganzzahligen Koeffizientenring mit Bezug auf G" anzusehen. Dieser Ring ist "komfortabler" als $\mathbb{Z}$ da er nur endlich viele maximale Ideale besitzt, und dasselbe gilt für den Gruppenring $\mathbb{Z}_\pi G$. Dennoch hat $\mathbb{Z}_\pi G$ alle interessanten Quotienten: Zu einer die Ordnung von G teilenden Primzahl p, und einer natürlichen Zahl n, haben wir kanonische Ringhomomorphismen $\mathbb{Z}G \hookrightarrow \mathbb{Z}_\pi G \twoheadrightarrow (\mathbb{Z}/p^n\mathbb{Z})G$.

Vorausgesetzt man interessiert sich für die Eigenschaften von G welche durch die Modulkategorie $\mathbb{Z}G\,\mathrm{Mod}$ bestimmt sind, ist dies sogar der bessere Rahmen, denn die folgenden Aussagen sind äquivalent: Es gibt eine Äquivalenz $\mathbb{Z}G\,\mathrm{Mod} \simeq \mathbb{Z}H\,\mathrm{Mod}$ von Modulkategorien; es gibt einen Isomorphismus $\mathbb{Z}_\pi G \cong \mathbb{Z}_\pi H$ von Ringen; es gibt eine Äquivalenz $\mathbb{Z}_\pi G\,\mathrm{Mod} \simeq \mathbb{Z}_\pi H\,\mathrm{Mod}$.

In Kapitel III zeigen wir für eine Gruppe G der Ordnung 96, dass der semilokale Gruppenring $\mathbb{Z}_\pi G$ einen Automorphismus besitzt, welcher mit keinem Automorphismus von $\mathbb{Z}G$ bis auf einen inneren Automorphismus von $\mathbb{Q}G$ übereinstimmt.

Gewisse *Gruppen*automorphismen treten in natürlicher Weise bei Untersuchungen zur Zassenhaus-Vermutung und des Isomorphieproblems auf. Klassenerhaltende Automorphismen zu studieren wurde neu motiviert durch Arbeiten von Roggenkamp und Kimmerle, die diese Automorphismen in Beziehung zur Zassenhaus-Vermutung setzten (Untersuchungen in diese Richtung begannen in [117]), und eine Beobachtung von Mazur verknüpft das Isomorphieproblem für ganzzahlige Gruppenringe mit der Existenz bestimmter nicht innerer klassenerhaltender Automorphismen, nämlich jenen welche innere Automorphismen des Gruppenrings induzieren. Darüberhinaus sollte, nach Scotts Auffassung, im Fall auflösbarer Gruppen ein Automorphismus eines semilokalen Gruppenrings betrachtet werden können als eine Kollektion von "rational zueinander passender" Gruppenisomorphismen von Trägheitsgruppen, und eine ähnliche Beschreibung sollte es auch für Gruppenringisomorphismen geben. Ein großer Teil der ersten beiden Kapitel, sowie das ganze Kapitel IV, ist dem Studium derjenigen Gruppenautomorphismen gewidmet, welche in diesem Zusammenhang auftreten.

Die Kapitel V–VII bilden einen weiteren Teil dieser Arbeit. Im Gegensatz zu dem ersten Teil befassen wir uns dort mit Einheiten in ganzzahligen Gruppenringen von *unendlichen* Gruppen. Die Ergebnisse werden selbstverständlich auch für Gruppenringe endlicher Gruppen gelten, aber die Grundhaltung wird sein, dass der Schwerpunkt auf die Reduktion auf den Fall endlicher Gruppen gelegt wird, welcher entweder bekannt ist oder als handhabbar eingeschätzt wird. Wir können die Einheitengruppe $\mathrm{U}(\mathbb{Z}G)$ einer beliebigen Gruppe G in unsere Überlegungen mit einbeziehen, aber in den meisten Fällen sind die Ergebnisse nur vollständig falls G eine periodische Gruppe ist. Dies hängt mit dem Umstand zusammen, dass wir bislang wenig über die multiplikative Gruppe des ganzzahligen Gruppenrings einer torsionsfreien Gruppe wissen. Anstelle von $\mathbb{Z}G$ werden wir allgemeiner RG betrachten, wobei R ein G-angepasster Ring ist, dass heißt, ein Integritätsbereich der Charakteristik 0 in welchem eine Primzahl p nicht invertierbar ist wann immer G ein Element der Ordnung p besitzt. Wir werden näher eingehen auf den Normalisator von G in der Einheitengruppe $\mathrm{U}(RG)$, auf die aufsteigende Zentralreihe von $\mathrm{U}(RG)$, und auf das endliche Konjugiertheit-Zentrum[1] von $\mathrm{U}(\mathbb{Z}G)$.

Wir werden sagen dass eine Gruppe G die *Normalisator-Eigenschaft* besitzt falls für jeden G-angepassten Ring R der Normalisator $\mathrm{N}_{\mathrm{U}(RG)}(G)$ von G in $\mathrm{U}(RG)$ nur aus den auf der Hand liegenden Einheiten besteht, das heißt falls $\mathrm{N}_{\mathrm{U}(RG)}(G) = \mathcal{Z}G$ gilt, wobei $\mathcal{Z}$ das Zentrum von $\mathrm{U}(RG)$ bezeichnet. Die Frage, ob eine Gruppe die Normalisator-Eigenschaft besitzt oder nicht, soll als das Normalisator-Problem bezeichnet werden. Es hat sich herausgestellt, dass Gruppen die die Normalisator-Eigenschaft *nicht* besitzen, als Bausteine für Gegenbeispiele zum Isomorphieproblem fungieren können.

In Kapitel V studieren wir, motiviert durch von Mazur [93] erzielten Ergebnissen, das Normalisator-Problem für unendliche Gruppen. Vermutlich hat Mazur als erster auf diesem Gebiet gearbeitet. Wir werden die in [93] aufgeworfenen Fragen beantworten, und wir werden Klassen von Gruppen geben die die Normalisator-Eigenschaft besitzen, damit jene Klassen vergrößernd die von Jespers, Juriaans, de Miranda und Rogerio [72] gegeben wurden.

In Kapitel VI untersuchen wir die aufsteigende Zentralreihe $1 \trianglelefteq \mathrm{Z}_1(\mathcal{U}) = \mathrm{Z}(\mathcal{U}) \trianglelefteq \mathrm{Z}_2(\mathcal{U}) \trianglelefteq \ldots$ der Einheitengruppe $\mathcal{U} = \mathrm{U}(RG)$ eines ganzzahligen Gruppenrings RG einer periodischen Gruppe G. Unsere Motivation beziehen wir aus dem Umstand dass $\mathrm{Z}_2(\mathcal{U}) \leq \mathrm{N}_{\mathcal{U}}(G)$ gilt. Diese Beobachtung ist der Startpunkt von Lis Schrift [86], in der gezeigt wird dass $\mathrm{Z}_2(\mathcal{U}) = \mathrm{Z}_3(\mathcal{U})$ im Fall $R = \mathbb{Z}$ gilt. Kürzlich wurde eine vollständige Beschreibung von $\mathrm{Z}_2(\mathcal{U})$ im Fall $R = \mathbb{Z}$ von Li und Parmenter [87] gegeben. Unter Verwendung anderer Methoden haben wir davon unabhängig die entsprechende Beschreibung in dem allgemeinen Fall erhalten: $\mathrm{Z}_3(\mathcal{U}) = \mathrm{Z}_2(\mathcal{U}) \leq \mathrm{Z}(\mathcal{U})\mathrm{Z}_2(G)$; und falls $\mathrm{Z}_2(\mathcal{U}) \neq \mathrm{Z}(\mathcal{U})$, ist G eine sogenannte Q^*-Gruppe.

In Kapitel VII zeigen wir, dass für eine periodische Gruppe G das zweite Zentrum $\mathrm{Z}_2(\mathrm{U}(\mathbb{Z}G))$ mit dem endlichen Konjugiertheit-Zentrum von $\mathrm{U}(\mathbb{Z}G)$ übereinstimmt, also

[1] finite conjugacy center

mit der Menge der Elemente von $\mathrm{U}(\mathbb{Z}G)$ welche nur endlich viele Konjugierte unter der Operation von $\mathrm{U}(\mathbb{Z}G)$ besitzen.

Mit dem letzten Kapitel beabsichtigen wir Hoffnungen zu wecken, dass eines Tages die ganzzahlige Darstellungstheorie signifikante Beiträge zur Theorie der endlichen Gruppen liefern wird. Es ist ein bedeutendes offenes Problem, einen direkten und "darstellungstheoretischen" Beweis eines ungeraden Analogons zu Glaubermans Z^*-Theorem zu finden. Robinson [114] studierte die Charaktertheorie eines minimalen Gegenbeispiels, K, zu dem Z_p^*-Theorem für ungerades p. In [115] zeigte Robinson, dass seine Ergebnisse benützt werden können um das Problem in einen ganz anderen Zusammenhang zu stellen, dem der Einheiten in Gruppenringen: Er zeigte die Existenz einer nichttrivialen zentralen Einheit der Ordnung p in dem p-Hauptblock von K, vorausgesetzt dass $p \geq 5$, oder dass $p = 3$ und K nicht einfach ist.

Vorausgesetzt dass $p = 3$, und x ein Element der Ordnung 3 in K ist welches mit keinem seiner anderen Konjugierten vertauscht, zeigen wir, dass für jeden irreduziblen Charakter χ von K der Charakterwert $\chi(x)$ ein ganzzahliges Vielfaches einer Potenz einer primitiven dritten Einheitswurzel ζ ist. Eine Konsequenz ist, dass die Existenz der nichttrivialen zentralen Einheit in dem p-Hauptblock in jedem Fall garantiert ist. Die Beweisidee ist in der Tat ziemlich einfach, sie stützt sich auf die Klassifikation der unzerlegbaren $\mathbb{Z}[\zeta]C_3$-Gitter. Hiermit schließt sich der Kreis dieses kleinen Überblicks über die vorliegende Schrift!

Jedes Kapitel ist in sich abgeschlossen und kann unabhängig von den anderen gelesen werden. Der Inhalt eines jeden Kapitels wird weiter unten ausführlicher beschrieben.

Der Leser wird feststellen, dass in dieser Schrift viele Beispiele gegeben werden. Wir meinen, dass dies heutzutage keiner Rechtfertigung bedarf und sind überzeugt: "Lang ist der Weg durch Vorschriften, kurz und wirkungsvoll durch praktische Beispiele."

Gleichwohl möchten wir den Leser darauf hinweisen, dass in der in Englisch geschriebenen Zusammenfassung an dieser Stelle zu dem Thema "Beispiele" einige Betrachtungen von Ringel wiedergegeben sind.

Kapitel I

Wir gehen davon aus, dass der Leser mit den Begriffen "ganzzahliger Gruppenring" und "Isomorphieproblem für ganzzahlige Gruppenringe" vertraut ist. In den ersten vier Kapiteln dieser Arbeit werden wir uns nur mit *endlichen* Gruppen G beschäftigen. Schreiben wir dann $\mathbb{Z}_\pi G$, so ist $\mathbb{Z}_\pi$ als Durchschnitt von Lokalisationen $\mathbb{Z}_{(p)}$ zu verstehen, wobei p eine endliche Menge von Primzahlen durchläuft, welche die Primteiler der Ordnung von G enthält. Man beachte dass $\mathbb{Z}_\pi G$ ein semilokaler Ring ist.

Graham Higman bezeichnete $\mathcal{O}G$ als ganzzahligen Gruppenring wann immer $\mathcal{O}$ ein Ring algebraisch ganzer Zahlen ist. Wir werden $\mathbb{Z}_\pi G$ ebenfalls als ganzzahligen Gruppenring bezeichnen. Mit Bezug auf dass Isomorphieproblem für ganzzahlige Gruppen-

ringe ist dies durch (1.1) gerechtfertigt: Nach Jacobinskis grundlegender Arbeit über Geschlechter von Gittern folgt aus $\mathbb{Z}_\pi G \cong \mathbb{Z}_\pi H$, dass $\mathcal{O}G \cong \mathcal{O}H$ für einen geeigneten Ring $\mathcal{O}$ von algebraisch ganzen Zahlen gilt. Weitere lokal–global Aspekte werden in Abschnitt 1 besprochen, einschließlich Scotts Verfahrensweise zur Konstruktion von Gruppenringautomorphismen und Isomorphismen in dem semilokalen Fall, welche jegliche Verwendung der Theorie der Ordnungen vermeidet (siehe (1.4) und (1.6)). Wir werden solche Konstruktionen in den Abschnitten 3 und 8 anwenden, und (1.4) wird für das Verständnis von einem Teil von Kapitel 3 hilfreich sein.

In Abschnitt 2 besprechen wir Möglichkeiten, wie Gegenbeispiele zum Isomorphieproblem für ganzzahlige Gruppenringe konstruiert werden können in dem Fall, dass semilokale Gruppenringe vorliegen. In (2.3) zeigen wir, wie eine Konstruktion von Mazur auf den Fall endlicher Gruppen übertragen werden kann, wobei multiplikative 1-Kozykeln ins Spiel kommen. Wir weisen auch auf den lokal–global Aspekt (2.10) dieser Konstruktion hin, wozu wir den Begriff eines lokalen Systems von 1-Kozykeln einführen, worunter wir eine Kollektion von lokalen 1-Kozykeln verstehen wollen, welche sich rational durch 1-Koränder unterscheiden.

Es gibt nicht isomorphe Gruppen X und Y, beide von der Ordnung $2^{21} \cdot 97^{28}$, mit isomorphen ganzzahligen Gruppenringen, $\mathbb{Z}X = \mathbb{Z}Y$. Diese Gruppen zur Hand habend, verfolgen wir in Abschnitt 3 den durch (1.6) vorgeschriebenen Weg, um zu zeigen dass die Gruppenringe semilokal isomorph sind. Dies führt zu neuer Einsicht in die Struktur dieser Gruppen. Tatsächlich werden wir eine kleine Abänderung vornehmen: Die 97-Sylowgruppe wird durch eine 17-Sylowgruppe ersetzt werden, ohne dabei die Struktur der Gruppen zu verändern. Offen bleiben wird die Frage, ob dies zu einem weiteren globalen Gegenbeispiel führt.

Motiviert durch die semilokale Untersuchung dieses Gegenbeispiels, präsentieren wir in Abschnitt 4 eine p-Gruppe (für eine beliebige Primzahl p), die ebenfalls jene Eigenschaften der 2-Sylowgruppe von X besitzt, welche sich als kritisch für die semilokale Konstruktion herausgestellt haben. Dies suggeriert stark, dass es semilokale Gegenbeispiele zum Isomorphieproblem geben sollte deren zugrundeliegenden Gruppen ungerade Ordnung haben.

Kenntnis über die Automorphismen von ganzzahligen Gruppenringen kann hilfreich sein um das Isomorphieproblem für gewisse Klassen von Gruppen zu klären, unter Verwendung von (Variationen von) Kimmerles $G \times G$-Tricks. Dies wird in Abschnitt 5 verdeutlicht, wo wir einen weiteren Beweis eines auf Scott zurückgehenden Satzes geben werden. Aus Wissen über Automorphismen (5.5) werden wir (5.7) ableiten: Endliche nilpotent auf abelsche Gruppen sind durch ihren ganzzahligen Gruppenring bestimmt.

Kapitel II

Dieses Kapitel enthält verschiedene Ergebnisse in Zusammenhang mit der Zassenhaus-Vermutung (betreffend Automorphismen von ganzzahligen Gruppenringen $\mathbb{Z}G$, wobei G eine endliche Gruppe ist).

In Abschnitt 6 ergreifen wir die Gelegenheit, um in einem Omnibus-Lemma (6.1) einige mehr oder weniger wohlbekannte Eigenschaften von Antiinvolutionen auf Gruppenringen zusammenzufassen, die mit der Zassenhaus-Vermutung zusammenhängen. Falls beispielsweise $\alpha \in \mathrm{Aut}_{\mathrm{n}}(\mathbb{Z}G)$, und $*$ die zu G assozierte Antiinvolution bezeichnet, dann gilt $[*, \alpha] = \mathrm{conj}(u^*u)$ für ein $u \in \mathrm{N}_{\mathrm{U}(\mathbb{Q}G)}(\mathbb{Z}G)$ genau dann, wenn α eine Zassenhaus-Zerlegung bezüglich G besitzt, d.h., falls es $\rho \in \mathrm{Aut}(G)$ gibt mit $\alpha\rho \in \mathrm{Inn}(\mathbb{Q}G)$. Wir möchten auch auf ein Konjugiertheitskriterium (6.4) hinweisen, welches allerdings bislang noch keine Anwendungen gefunden hat.

Roggenkamp und Scott zeigten, im Falle dass G Normalteiler $N_1, \ldots, N_r$ von paarweise teilerfremder Ordnung besitzt, ein ganzzahliger Gruppenring RG durch ein Pullback-Diagramm (7.1) beschrieben werden kann, welches sich als besonders nützlich herausgestellt hat um Gegenbeispiele zur Zassenhaus-Vermutung zu konstruieren. Wir werden einen ausführlichen Beweis dieses Resultats in Abschnitt 7 geben, wobei wir auf eine interessante Beschreibung (7.2) des Ideals $\sum_{i=1}^{r}(RG) \cdot \hat{N}_i$ hinweisen werden.

Dieses Ergebnis von Roggenkamp und Scott kann auch zur Berechnung der Einheitengruppen gewisser ganzzahliger Gruppenringe verwendet werden. Dies wird in (7.3) veranschaulicht, wo wir die Einheitengruppe von $\mathbb{Z}C_{10}$ und deren Index in einer maximalen Überordnung berechnen.

Lam und Leung (7.4) haben folgendes zahlentheoretisches Problem gelöst: Gegeben eine natürliche Zahl m, für welche Zahlen n gibt es $m$te Einheitswurzeln $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ mit $\alpha_1 + \cdots + \alpha_n = 0$? Wir werden deren Ergebnisse in einen allgemeineren Zusammenhang setzen, und die Ergebnisse werden dann vollständig in der Sprache der Gruppenringe formuliert sein, da wir (7.2) benutzen werden, um einige lineare Disjunktheits-Argumente überflüssig zu machen. Der Ausgangspunkt wird (7.7) sein: Für Normalteiler A und B von G mit $A \cap B = 1$ gilt $\mathbb{N}_0G \cap (\mathbb{Z}G \cdot \hat{A} + \mathbb{Z}G \cdot \hat{B}) = \mathbb{N}_0G \cdot \hat{A} + \mathbb{N}_0G \cdot \hat{B}$ (hier ist $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$). Dann werden wir in enger Anlehnung an die von Lam und Leung gegebene Darstellung die Verallgemeinerung von (7.4) in (7.11) geben: Die Augmentation eines jeden Elements aus $\mathbb{N}_0G \cap \sum_{i=1}^{r} \mathbb{Z}G \cdot \hat{N}_i$ ist in $\sum_{i=1}^{r} \mathbb{N}_0 \, |N_i|$ enthalten.

In Abschnitt 8 wenden wir uns der Konstruktion von Gegenbeispielen zur Zassenhaus-Vermutung im semilokalen Fall zu. (Solche Beispiele wurden oft "Gegenbeispiele" genannt, ihr Auftreten wurde mit Überraschung aufgenommen. Nunmehr erscheint es richtig, solches Verhalten als ganz gewöhnlich einzuschätzen.) Nach einiger Vorarbeit werden wir bereit sein um mit relativ geringem Aufwand solche Beispiele zu geben, unter denen eine metabelsche Gruppe mit abelschen Sylowgruppen, eine überauflösbare Gruppe, und eine Frobeniusgruppe sein werden.

In Abschnitt 9 berechnen wir die Gruppen- und die Charaktertafelautomorphismen der Kranzprodukte $G_{n,r} = (\mathbb{Z}/r\mathbb{Z}) \wr S_n$ (welche eine der zwei unendlichen Serien von irreduziblen endlichen komplexen Reflektionsgruppen bilden): In (9.1) geben wir eine explizite Beschreibung von $\mathrm{Out}(G_{n,r})$, und für $G_{n,r} \neq G_{2,2}$ zeigen wir in (9.2), dass die Sequenz $1 \to \mathrm{Inn}(G_{n,r}) \to \mathrm{Aut}(G_{n,r}) \to \mathrm{AutCT}(G_{n,r}) \to 1$ exakt ist. Insbesondere erhalten wir, dass die Zassenhaus-Vermutung für diese Gruppen gilt (was jedoch bereits bekannt ist, siehe [129, Section 44]).

Kapitel III

Das Hauptergebnis dieses Kapitels ist, dass der semilokale Gruppenring $\mathbb{Z}_\pi G$ einer endlichen Gruppe G einen Automorphismus α besitzen kann, welcher von keinem globalen Automorphismus repräsentiert wird, d.h., es gibt keinen Automorphismus von $\mathbb{Z}G$ der sich auf $\mathbb{Q}G$ von α nur um einen inneren Automorphismus unterscheidet.

Wir werden ein Beispiel ausarbeiten welches eine von Blanchards Gruppen G der Ordnung 96 von [13] verwendet. Diese Gruppe ist von der Form $G = (\langle q : q^3\rangle \times \langle c : c^2\rangle \times \langle b : b^4\rangle) \rtimes \langle a : a^4\rangle$. Blanchard zeigt, dass es ein $\alpha \in \mathrm{Aut}_{\mathrm{n}}(\mathbb{Z}_\pi G)$ gibt, welches nur die beiden treuen irreduziblen Charaktere von G vertauscht, und welches nicht als Produkt eines Gruppenautomorphismus (auf $\mathbb{Z}_\pi G$ fortgesetzt) und eines zentralen Automorphismus geschrieben werden kann. Wir werden zeigen, dass ein solches α von keinem globalen Automorphismus repräsentiert wird.

Wir beschreiben kurz unsere Vorgehensweise. Verbunden mit den Normalteilern $Q = \langle q\rangle$ und $M = \mathrm{Z}(G) = \langle b^2\rangle$ von G, haben wir ein Pullback-Diagramm (7.1)

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \Gamma \\ \downarrow & & \downarrow \\ \Lambda & \longrightarrow & \Lambda_2 \oplus \Lambda_3 \end{array} .$$

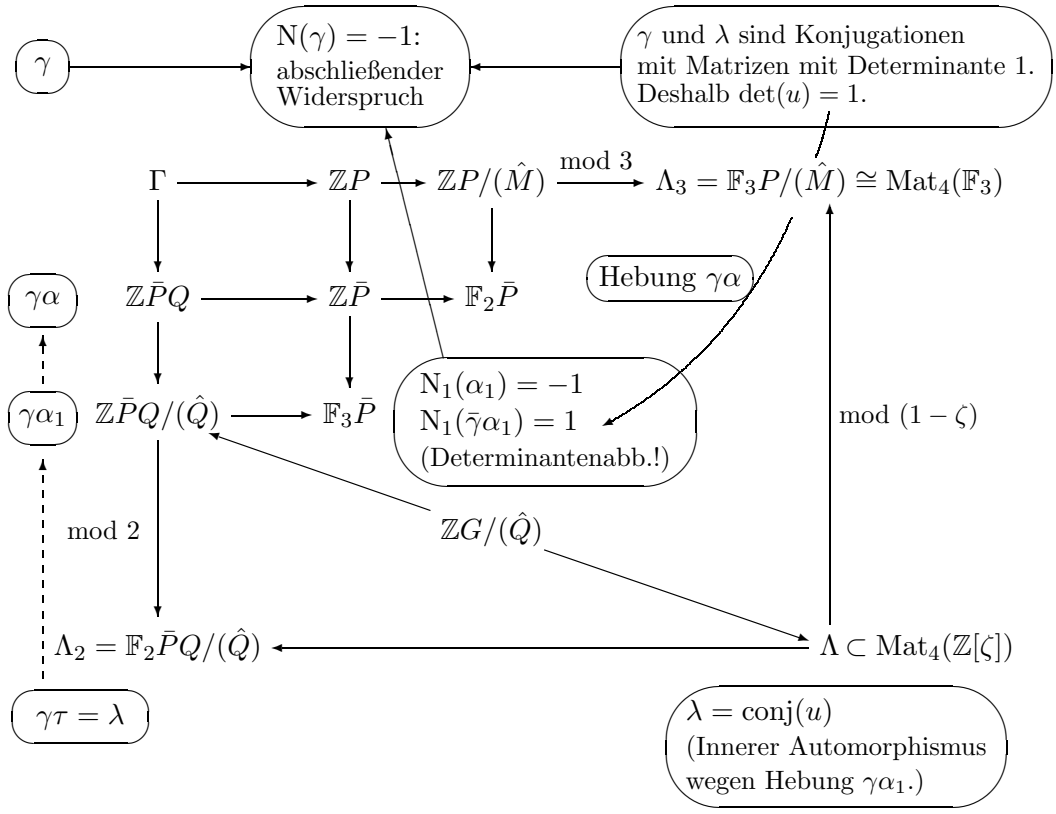
Wir können $\Lambda \subset \mathrm{Mat}_4(\mathbb{Z}[\zeta])$ annehmen, wobei ζ eine primitive dritte Einheitswurzel ist, da genau die beiden treuen irreduziblen Charaktere von G, welche algebraisch konjugiert sind, zu $\mathbb{C}\Lambda$ gehören.

Es gibt ein $\tau \in \mathrm{Aut}(G)$ welches die beiden treuen irreduziblen Charaktere vertauscht und einen inneren Automorphismus auf $\Lambda_2 \oplus \Lambda_3$ induziert. Die ganze Diskussion läuft auf die Frage hinaus, ob es $\gamma \in \mathrm{Autcent}(\Gamma)$ und $\lambda \in \mathrm{Autcent}(\Lambda)$ geben kann, welche sich auf dem gemeinsamen Quotienten $\Lambda_2 \oplus \Lambda_3$ um den von τ induzierten inneren Automorphismus unterscheiden. Aus der Annahme, dass es solche Automorphismen gibt, werden wir letztendlich einen Widerspruch herleiten.

Es sei $P = \langle a, b, c\rangle$, eine 2-Sylowgruppe von G. Querstriche sollen Reduktion modulo M bedeuten, so dass $\bar{P} = P/M$ ist. Dann ist Γ das Bild der natürlichen Abbildung $\mathbb{Z}G \to \mathbb{Z}\bar{P}Q \oplus \mathbb{Z}P$. Der Automorphismus γ induziert zentrale Automorphismen von $\mathbb{Z}\bar{P}Q$ und $\mathbb{Z}P$, welche ebenfalls mit γ bezeichnet werden sollen.

Für jedes $\beta \in \mathrm{Autcent}(\mathbb{Z}P)$ können wir wiefolgt eine Norm $\mathrm{N}(\beta) \in \{\pm 1\}$ definieren: β induziert auf den Summanden von $\mathbb{Q}P$ die echte Matrixringe sind innere Automorphismen, gegeben durch Konjugation mit Matrizen mit Determinante ± 1, und $\mathrm{N}(\beta)$ ist das Produkt der Determinanten solcher Matrizen. Unter Verwendung von Fröhlichs Lokalisations-Sequenz, und Mayer–Vietoris Sequenzen zur Berechnung von lokal freien Klassengruppen, können wir zeigen dass stets $\mathrm{N}(\beta) = 1$ gilt.

Man betrachte nun folgendes Diagramm, in welchem jedes "Quadrat" ein Pullback-Diagramm ist. (Die Bedeutung der ausgefüllten Ovale wird nachträglich erklärt werden.)



Wir können gleichermaßen eine Norm N_1 für zentrale Automorphismen von $\mathbb{F}_3\bar{P}$ definieren. Jedes $\beta \in \mathrm{Autcent}(\mathbb{Z}P)$ induziert einen inneren Automorphismus $\bar{\beta}$ von $\mathbb{F}_3\bar{P}$ und einen inneren Automorphismus $\mathrm{conj}(T)$ von $\Lambda_3 \cong \mathrm{Mat}_4(\mathbb{F}_3)$, und wir haben $\mathrm{N}(\beta) = \mathrm{N}_1(\bar{\beta}) \cdot \det(T)$.

Es ist einfach zu sehen, dass ohne Einschränkung der Allgemeinheit angenommen werden darf, dass sowohl γ als auch λ auf Λ_3 eine Konjugation mit einer Matrix mit Determinante 1 ist.

Wir werden einen inneren Automorphismus α_1 von $\mathbb{Z}\bar{P}Q/(\hat{Q})$ konstruieren, welcher den von τ auf Λ_2 induzierten inneren Automorphismus hebt, und wir werden zeigen, dass α_1 weiter zu einem zentralen Automorphismus α von $\mathbb{Z}\bar{P}Q$ hebbar ist.

Insbesondere wird λ von einem zentralen Automorphismus von $\mathbb{Z}G/(\hat{Q})$ induziert, was zur Folge hat dass λ einen inneren Automorphismus von $\mathbb{Z}_2\Lambda$ induziert. Daraus schließen wir, unter erneuter Verwendung von Fröhlichs Lokalisations-Sequenz, dass λ ein innerer Automorphismus ist, sagen wir, conj(u). Man beachte, dass $\det(u) = 1$ gilt da die Reduktion von u modulo $(1-\zeta)$ Determinante 1 hat.

Der Automorphismus γ induziert einen zentralen Automorphismus $\bar{\gamma}$ von $\mathbb{F}_3\bar{P}$, und wir interessieren uns für $\mathrm{N}_1(\bar{\gamma})$. Jeder zentrale Automorphismus von $\mathbb{Z}\bar{P}Q/(\hat{Q})$ induziert einen zentralen Automorphismus von $\mathbb{F}_3\bar{P}$. Wir wissen dass $\mathrm{N}_1(\alpha_1) = -1$ gilt, und da $\gamma\alpha_1$ eine Hebung des von λ auf Λ_2 induzierten Automorphismus ist, versuchen wir also $\mathrm{N}_1(\bar{\gamma}\alpha_1)$ zu berechnen.

Die Untergruppe $U \leq \Lambda^\times$ bestehe aus jenen Einheiten v, für die es einen zentralen Automorphismus β_v von $\mathbb{Z}\bar{P}Q/(\hat{Q})$ gibt, welcher auf Λ_2 mit dem durch Konjugation mit dem Bild von v gegebenen inneren Automorphismus übereinstimmt. Dann liefert die Zuordnung $v \mapsto \mathrm{N}_1(\bar{\beta}_v)$ einen wohldefinierten Homomorphismus $d : U \to \{\pm 1\}$. Der Autor würde sehr gerne wissen, ob nun ein allgemeines Argument zeigt dass dieser Homomorphismus von der Determinantenabbildung herrührt.

Was wir zeigen werden ist, dass falls sich für ein $v \in \Lambda^\times$ der durch Konjugation mit dem Bild von v gegebene innere Automorphismus von Λ_2 zu einem zentralen Automorphismus ν von $\mathbb{Z}\bar{P}Q$ heben läßt, $\det(v) = \pm 1$ gilt, mit $\det(v) = 1$ genau dann wenn $d(v) = 1$. Dazu werden wir v und ν, unter Verwendung von geeigneten "Modifikationen" von bizyklischen Einheiten, sorgfältig modifizieren bis die Behauptung offensichtlich ist.

Also ist $\mathrm{N}_1(\bar{\gamma}\alpha_1) = \det(u) = 1$, und folglich $\mathrm{N}(\gamma) = -1$, der gewünschte Widerspruch.

Kapitel IV

Dieses Kapitel enthält eine lose Reihe von Ergebnissen in Bezug auf spezielle Automorphismengruppen, die bei Betrachtung der Zassenhaus-Vermutung und des Isomorphieproblems auftreten.

In Abschnitt 14 kommen wir kurz in Berührung mit klassenerhaltenden Automorphismen von endlichen Gruppen und zeigen (14.4): Klassenerhaltende Automorphismen von zyklisch auf abelschen Gruppen sind innere Automorphismen.

Ein Coleman-Automorphismus einer endlichen Gruppe G ist ein Automorphismus von G, dessen Einschränkung auf jede Sylowgruppe von G mit der Einschränkung eines inneren Automorphismus von G übereinstimmt. In Abschnitt 15 führen wir in [61] begonnene Untersuchungen fort und studieren die Struktur einer endlichen Gruppe G mit einem nicht inneren Coleman-Automorphismus von p-Potenzordnung unter der Voraussetzung, dass $G/\mathrm{F}^*(G)$ keinen Hauptfaktor der Ordnung p hat. Tatsächlich wissen wir nicht, ob es eine solche Gruppe gibt; wir studieren die Struktur eines mini-

malen Gegenbeispiels. Anhand eines Beispiels (15.4) zeigen wir, dass dies auf interessante Fragen (15.6) über zentrale Erweiterungen, hauptsächlich von einfachen Gruppen, führt, welche jedoch unbeantwortet bleiben werden. Kurz betrachten wir auch Coleman-Automorphismen von zentralen Erweiterungen.

In Abschnitt 16 beschäftigen wir uns mit subdirekten Produkten von endlichen Gruppen. Spezieller besprechen wir das Konzept von getwisteten projektiven Limiten, welches natürlicherweise bei der Diskussion des ganzzahligen Isomorphieproblems für auflösbare Gruppen auftritt, siehe (16.5). Wir geben ein Beispiel (16.17), in dem Twisten mit einem inneren Automorphismus zu einer nicht isomorphen Gruppe derselben Ordnung führt.

Falls G ein projektiver Limes ist, bemerken wir dass $\mathrm{Aut}(G)$, unter milden Voraussetzungen, auf natürliche Weise ebenfalls ein projektiver Limes ist. Dies beschafft uns einen praktischen Weg, die Gruppe der Coleman-Automorphismen $\mathrm{Aut}_{\mathrm{Col}}(G)$ einer auflösbaren Gruppe G zu berechnen, und wir werden einen kurzen Beweis eines Resultats von Dade (16.13) geben: $\mathrm{Out}_{\mathrm{Col}}(G)$ ist abelsch.

Eine auflösbare Gruppe G ist der projektive Limes seiner Faktorgruppen $G/\mathrm{O}_{p'}(G)$. Wir können den projektiven Limes Γ der Gruppenringe $\mathbb{Z}G/\mathrm{O}_{p'}(G)$ bilden und uns fragen, wieviel Information Γ über $\mathbb{Z}G$ enthält. Wir zeigen die Existenz einer exakten Sequenz, welche zu einem gewissen Ausmaß mißt, wie weit Γ davon entfernt ist die "simultane p-Version" der Zassenhaus-Vermutung zu erfüllen.

Kapitel V

Es sei G eine Gruppe, und R ein kommutativer Ring. Die Automorphismen von G, die einen inneren Automorphismus des Gruppenrings RG induzieren, bilden eine Gruppe $\mathrm{Aut}_R(G)$. Wir setzen $\mathrm{Out}_R(G) = \mathrm{Aut}_R(G)/\mathrm{Inn}(G)$. Man beachte, dass $\mathrm{Aut}_R(G) \cong \mathrm{N}_{\mathcal{U}}(G)/\mathrm{Z}(\mathcal{U})$ gilt, wobei $\mathcal{U} = \mathrm{U}(RG)$ gesetzt ist.

Der grundlegendste Fakt über Elemente aus $\mathrm{N}_{\mathcal{U}}(G)$ bezieht die Standard-Antiinvolution $*_G$ von RG mit ein: $u \in \mathrm{N}_{\mathcal{U}}(G)$ impliziert $uu^{*_G} \in \mathrm{Z}(\mathcal{U})$, und dies impliziert wiederum $(uu^{-*_G})^{*_G}(uu^{-*_G}) = 1$.

Die Umkehrung gilt im allgemeinen nicht: Selbst wenn R G-adaptiert ist, muß $uu^{*_G} \in \mathrm{Z}(\mathcal{U})$ nicht notwendigerweise $u \in \mathrm{N}_{\mathcal{U}}(G)$ implizieren. Dies gilt jedoch falls $R = \mathbb{Z}$ ist. Weiterhin, falls $R = \mathbb{Z}$, gibt ein klassisches Result, welches auf Higman und Berman zurückgeht, dass $uu^{-*_G} \in \pm G$ für jedes $u \in \mathrm{N}_{\mathcal{U}}(G)$ gilt, woraus unmittelbar folgt, dass $\mathrm{Out}_{\mathbb{Z}}(G)$ vom Exponent 2 ist. Dies unterstreicht die Sonderstellung, die der Koeffizientenring $\mathbb{Z}$ einnimmt, und die Stärke solcher "Stern-Argumente". Wir möchten jedoch darauf hinweisen, dass wir in den Kapiteln V und VI keinerlei Gebrauch von "Stern-Argumenten" machen werden. Dies hat zur Konsequenz, dass unsere Resultate für beliebige G-adaptierte Koeffizientenringe R gültig sein werden. Einige unserer Resultate sind in dem Fall $R = \mathbb{Z}$ bereits bekannt. Jedoch schließen die bekannten Beweise oft "Stern-Argumente" mit ein, so dass wir andersgeartete Beweise finden mußten, siehe z.B. (19.1) und (19.3).

In Abschnitt 17 geht es um die Frage, was ohne weitere Voraussetzungen an den Koeffizientenring R (neben der Kommutativität) über $\mathrm{Out}_R(G)$ ausgesagt werden kann. Unser erstes Resultat (17.3) ist, dass $\mathrm{Aut}_R(G) \leq \mathrm{Aut}_c(G)$ gilt.

Für die Untersuchung von $\mathrm{N}_{\mathcal{U}}(G)$ ist die erste grundlegende Beobachtung, dass man mit dem Gruppenring des endlichen Konjugiertheit-Zentrums $\Delta(G)$ von G arbeiten kann, denn für $u \in \mathrm{N}_{\mathcal{U}}(G)$ mit $1 \in \mathrm{supp}(u)$ gilt $D := \{g^{-1}g^u \mid g \in G\} \subseteq \mathrm{supp}(u) \subseteq \Delta(G)$. In (17.2) zeigen wir, dass $\langle D\rangle$ und $\langle \mathrm{supp}(u)\rangle$ normale Untergruppen von G sind. Ist desweiteren $u = u^{*_G}$, dann gilt $T := \{g^{-1}g^v \mid g \in G, v \in \langle u\rangle\} \subseteq \mathrm{supp}(u)$. Dies ist insofern ein interessantes Resultat, als es uns zeigt dass T eine endliche Menge ist, und wir nun einen (gruppentheoretischen!) Satz von Baer (17.4) mit einbeziehen können um zu folgern, dass $N = \langle T\rangle$ eine *endliche* normale Untergruppe von G ist. Man beachte, dass Konjugation mit u auf G/N die Identität induziert.

Unter Verwendung von Ideen von Mazur [93], und, wiederum, des Satzes von Baer, werden wir schließlich in (17.8) zeigen, dass jedes Element von $\mathrm{Aut}_R(G)$ einen inneren Automorphismus von G/N für eine endliche normale Untergruppe N von G induziert. Als Korollar erhalten wir (17.9): Die Gruppe $\mathrm{Out}_R(G)$ ist periodisch. Vorausgesetzt dass $\Delta(G)$ endlich erzeugt ist, zeigen wir in (17.7), dass $\mathrm{Out}_R(G)$ eine endliche Gruppe ist.

Wir beenden den Abschnitt mit einigen Beispielen, welche negative Antworten zu einigen Fragen aus [93] liefern. Insbesondere zeigen wir, dass es zu $u \in \mathrm{N}_{\mathcal{U}}(G)$ nicht notwendigerweise ein Gruppenelement $g \in G$ geben muß so dass $\langle \mathrm{supp}(ug)\rangle$ eine endliche Gruppe ist (vgl. mit (18.5)). Weiterhin, falls eine Primzahl p die Ordnung eines Elements von $\mathrm{Out}_R(G)$ teilt, muß G nicht notwendigerweise ein Element der Ordnung p haben.

In Abschnitt 18 werden wir kurze und vereinheitlichte Beweise einiger "Darstellungs-Sätze" geben welche in [74,72,70] erscheinen. Die grundlegende Idee (18.1) hinter diesen Sätzen ist, das klassische Result, dass der rationale Gruppenring $\mathbb{Q}H$ einer geordneten Gruppe H nur triviale Einheiten besitzt, zu verallgemeinern. Es sei $\Delta^+(G)$ die Menge der Torsionselemente in $\Delta(G)$ (dies ist eine charakteristische Untergruppe von G), und es sei R ein $\Delta^+(G)$-adaptierter Ring. Dann haben wir den "Darstellungs-Satz" (18.5): Für jedes $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ mit $1 \in \mathrm{supp}(u)$ ist die Trägergruppe $\langle \mathrm{supp}(u)\rangle$ eine endliche normale Untergruppe von G. Als Korollar erhalten wir (18.6): Ist $u \in \mathrm{N}_{\mathrm{V}(RG)}(G)$ mit $u^n \in G$ für ein $n \in \mathbb{N}$, dann gilt $u \in G$. Ein weiteres Korollar (18.7) besagt, dass $\Delta^+(G)$ ein Element von Primzahlordnung p enthält, falls die Primzahl p die Ordnung eines Elements der periodischen Gruppe $\mathrm{Out}_R(G)$ teilt.

Ab jetzt bezeichne R stets einen $\Delta^+(G)$-adaptierten Ring.

In Abschnitt 19 werden wir (18.5) benutzen, um in (19.1) und (19.3) die Struktur von $\mathrm{N}_{\mathrm{V}(RG)}(G)/G$ (dies ist eine torsionsfreie abelsche Gruppe) und $\mathrm{N}_{\mathrm{V}(RG)}(G)/\mathrm{Z}(\mathrm{V}(RG))G$ zu untersuchen.

Wir werden sagen dass G die *Normalisator-Eigenschaft* besitzt falls $\mathrm{Out}_R(G) = 1$,

oder, gleichwertig, $\mathrm{N}_{\mathrm{U}(RG)}(G) = \mathrm{Z}(\mathrm{U}(RG))G$ für jeden G-adaptierten Ring R gilt. Wir werden (18.5) auch benutzen, um für einige Klassen von Gruppen die Normalisator-Eigenschaft nachzuweisen. Wir möchten erwähnen, dass unsere Resultate nahezu vollständig waren, als wir einen Vorabdruck einer Arbeit von Jespers, Juriaans, de Miranda and Rogerio [72] erhielten. Wir vergleichen deren Hauptergebnisse mit den entsprechenden Ergebnissen, die wir erzielen konnten:

Eine Gruppe G hat die Normalisator-Eigenschaft, vorausgesetzt dass G zu einer der Klassen gehört, die gegeben ist

in [72]:	in Abschnitt 19:
• Gruppen mit $\Delta^+(G)$ ohne nichttrivialer 2-Torsion; Torsionsgruppen mit normaler 2-Sylowgruppe;	(19.11) Gruppen, deren endliche normale Untergruppen eine normale 2-Sylowgruppe haben;
• lokal nilpotente Gruppen;	(19.12) Gruppen, deren endliche normale Untergruppen nilpotent sind;
• EK-Gruppen[a] G, so dass $[G, G]$ eine p-Gruppe ist.	(19.6) Gruppen G, so dass endliche Faktorgruppen von $[G, G]$ p-Gruppen sind.

[a] Sämtliche Konjugiertenklassen haben endliche Länge.

(Strenggenommen wird in [72] nur $\mathrm{Out}_{\mathbb{Z}}(G) = 1$ nachgeprüft.)

Einer der Gründe, warum wir größere Klassen erhalten, ist dass wir die für unendliche Gruppen zweckmäßige Version des Ward–Coleman Lemmas (siehe Seite 138) verwenden: Ist G endlich, betrachtet man gewöhnlich die Operation eines $u \in \mathrm{N}_{\mathcal{U}}(G)$ auf einer p-Sylowgruppe von G, wohingegen im Fall G unendlich, man die Operation auf Untergruppen von endlichem p'-Index in G zu betrachten hat (siehe (19.4)). Als eine Anwendung erhalten wir sofort (19.6), ohne den "Darstellungs-Satz" überhaupt anwenden zu müssen!

Wir geben auch ein technisches Lemma (19.5), welches uns erlaubt, ausgiebigen Gebrauch von dem "Darstellungs-Satz" (18.5) zu machen. Auf diese Weise überträgt sich die wohlbekannte Tatsache (19.14), dass eine endliche Gruppe G die Normalisator-Eigenschaft besitzt sofern sie nur eine ihren eigenen Zentralisator enthaltende normale p-Untergruppe hat, auf den Fall unendlicher Gruppen (19.15).

An [72] anschließend, besprechen wir in Abschnitt 20 kurz die Frage, wann RG "nur triviale zentrale Einheiten" hat. Wir zeigen in (20.3) dass, falls R ein Integritätsbereich der Charakteristik Null ist in dem keine rationale Primzahl invertierbar ist, die Redewendung "RG besitzt nur triviale zentrale Einheiten" gerechtfertigt ist, da sie unabhängig von der zugrundeliegenden Gruppenbasis ist. Der Beweis verwendet einen Satz von Burn, welcher besagt, dass die Trägergruppe eines zentralen Idempotents in RG eine endliche normale Untergruppe von G ist.

Burns Satz wird auch verwendet werden um eine positive Antwort (20.6) auf eine Frage von Mazur [92, p. 438] zu geben: Ist G eine EK-Gruppe, und R ein G-adaptierter Ring, dann ist jede Gruppenbasis von RG ebenfalls eine EK-Gruppe.

Kapitel VI

Es sei $\mathcal{U}$ die Gruppe der Einheiten eines Gruppenrings RG, wobei G eine periodische Gruppe und R ein G-adaptierter Ring ist, und es sei $1 \trianglelefteq \mathrm{Z}_1(\mathcal{U}) = \mathrm{Z}(\mathcal{U}) \trianglelefteq \mathrm{Z}_2(\mathcal{U}) \trianglelefteq \ldots$ die aufsteigende Zentralreihe von $\mathcal{U}$. Unser Hauptergebnis (21.2) besagt, dass $\mathrm{Z}_3(\mathcal{U}) = \mathrm{Z}_2(\mathcal{U}) \leq \mathrm{Z}(\mathcal{U})\mathrm{Z}_2(G)$ gilt; und falls $\mathrm{Z}_2(\mathcal{U}) \neq \mathrm{Z}(\mathcal{U})$, ist G eine sogenannte Q^*-Gruppe (wie in (21.1) definiert).

Q^*-Gruppen erscheinen, möglicherweise zum ersten Mal, in der Schrift [16] von Bovdi, der zeigte, dass G eine Q^*-Gruppe ist, falls G eine nicht zentrale Untergruppe besitzt welche normal in $\mathrm{U}(\mathbb{Z}G)$ ist.

Wir möchten anmerken, dass unsere Präsentation den Umstand hervorhebt, dass hier eine starke Verbindung zu dem Normalisator-Problem besteht.

Zuallererst ist einfach zu sehen, dass $\mathrm{Z}_2(\mathcal{U}) \leq \mathrm{N}_{\mathcal{U}}(G)$ gilt. Für einen Moment sei angenommen, dass G die Normalisator-Eigenschaft besitzt, d.h., dass die Beziehung $\mathrm{N}_{\mathcal{U}}(G) = \mathrm{Z}(\mathcal{U})G$ besteht. Dann gilt $\mathrm{Z}_2(\mathcal{U}) = \mathrm{Z}(\mathcal{U})(G \cap \mathrm{Z}_2(\mathcal{U}))$. Für beliebige $g \in G \cap \mathrm{Z}_2(\mathcal{U})$ und $u \in \mathcal{U}$ ist $g^u \in \mathrm{Z}_2(\mathcal{U}) \leq \mathrm{N}_{\mathcal{U}}(G)$, und da g^u endliche Ordnung hat, folgt $g^u \in G$ (siehe (23.2.4) oder (18.6)). Folglich ist $G \cap \mathrm{Z}_2(\mathcal{U})$ eine normale Untergruppe von $\mathcal{U}$, und unser Hauptergebnis (21.2) folgt aus Bovdis Ergebnissen (siehe (24.4) und (25.3)).

Setze $\mathrm{Z}_\infty(\mathcal{U}) = \bigcup_{n=1}^{\infty} \mathrm{Z}_n(\mathcal{U})$. Wesentlich für unsere Vorgehensweise wird (23.3) sein, wo wir $\mathrm{Z}_\infty(\mathcal{U}) \leq \mathrm{N}_{\mathcal{U}}(G)$ zeigen, und dass Elemente von $\mathrm{Z}_\infty(\mathcal{U})$ mit allen unipotenten Elementen von $\mathcal{U}$ vertauschen. Anschließend werden wir in (23.5) unter der Annahme, dass ein $u \in \mathrm{N}_{\mathcal{U}}(G)$ mit allen unipotenten Elementen von $\mathbb{Z}G$ vertauscht, zeigen, dass $\mathrm{conj}(u)$ einen Potenzautomorphismus von G induziert, und falls weiter G keine Dedekindgruppe ist, ist dann $[G, u] \leq \mathrm{R}(G)$, wobei $\mathrm{R}(G)$ den Durchschnitt aller nicht normalen Untergruppen von G bezeichnet. Dies erlaubt uns, zwei gruppentheoretische Ergebnisse ins Spiel zu bringen. Das erste ist Blackburns Klassifikation (22.2) der endlichen Gruppen G mit $\mathrm{R}(G) \neq 1$. Diese Klassifikation wird benutzt werden, um (23.8) zu beweisen: Falls G keine Dedekindgruppe ist, und ein $u \in \mathrm{N}_{\mathcal{U}}(G)$ mit allen unipotenten Elementen von $\mathbb{Z}G$ vertauscht, dann gilt $u \in \mathrm{Z}(\mathcal{U})G$. Das andere Ergebnis, welches Cooper zu verdanken ist, besagt, dass ein Potenzautomorphismus einer beliebigen Gruppe ein zentraler Automorphismus ist, d.h. ein Automorphismus, welcher auf der zentralen Faktorgruppe die Identität induziert. Dies wird in (23.6) benutzt werden, um $\mathrm{Z}_\infty(\mathcal{U}) = \mathrm{Z}_2(\mathcal{U})$ zu zeigen. Insgesamt erhalten wir in (23.9), dass $\mathrm{Z}_\infty(\mathcal{U}) \leq \mathrm{Z}(\mathcal{U})\mathrm{Z}_2(G)$ gilt.

Als nächstes beschreiben wir kurz, was in den einzelnen Abschnitten ausgeführt wird.

In Abschnitt 21 geben wir das Hauptergebnis und stellen die Geschichte dieses Klassifikationstheorems dar. Insbesondere sei bemerkt, dass wir unsere Ergebnisse unabhängig

von einer Arbeit von Li und Parmenter erzielt haben, in welcher diese unter Verwendung anderer Methoden das Ergebnis für den Fall $R = \mathbb{Z}$ erhalten haben.

In Abschnitt 22 benützen wir Blackburns Klassifikation für eine Fall zu Fall Untersuchung, und zeigen in (22.4): Ist eine endliche Gruppe G keine Dedekindgruppe, und ist der Durchschnitt $\mathrm{R}(G)$ ihrer nicht normalen Untergruppen nicht trivial, dann gilt $\mathrm{R}(G) \leq \mathrm{Z}(G)$ und $\mathrm{Out}_{\mathrm{c}}(G) = 1$.

Die Ergebnisse aus Abschnitt 23, in dem die zentrale Proposition (23.3) bewiesen wird, sind bereits oben beschrieben worden.

Um die Darstellung in sich geschlossen zu halten, geben wir in Abschnitt 24 einen kurzen Beweis des oben erwähnten Resultats von Bovdi.

In Abschnitt 25 zeigen wir, wie Bovdis Result benutzt werden kann um $\mathrm{Z}_\infty(\mathcal{U}) \leq \mathrm{Z}(\mathcal{U})\mathrm{Z}_2(G)$ zu etablieren, wobei wir eng vorangegangener Arbeit von Arora, Hales und Passi folgen werden. Und es wird nun natürlich mit Bovdis Result folgen, dass G eine Q^*-Gruppe ist falls $\mathrm{Z}_2(\mathcal{U}) \neq \mathrm{Z}(\mathcal{U})$ gilt. Wir geben eine vollständige Beschreibung (25.3) von $\mathrm{Z}_\infty(\mathcal{U})$ falls R ein Ring algebraischer Zahlen in einem total reellen Zahlkörper ist. Ist andererseits R in einem gewissen Sinn "groß genug", darf man $\mathrm{Z}_2(\mathcal{U}) = \mathrm{Z}(\mathcal{U})$ erwarten, wie in (25.4) gezeigt wird.

Kapitel VII

Für eine periodische Gruppe G werden wir zeigen, dass das zweite Zentrum $\mathrm{Z}_2(\mathrm{U}(\mathbb{Z}G))$ der Gruppe der Einheiten in $\mathbb{Z}G$ mit dem endlichen Konjugiertheit-Zentrum $\Delta(\mathrm{U}(\mathbb{Z}G))$ von $\mathrm{U}(\mathbb{Z}G)$ übereinstimmt, d.h. mit der Menge der Elemente von $\mathrm{U}(\mathbb{Z}G)$ die nur endlich viele Konjugierte unter der Operation von $\mathrm{U}(\mathbb{Z}G)$ haben.

Um dieses Ziel zu erreichen, werden wir einen Satz von Sehgal und Zassenhaus (26.1) benutzen. Angenommen, G ist eine endliche Gruppe. Ist D ein Block von $\mathbb{Q}G$ welcher eine total definite Quaternionenalgebra ist, stimmt die von G induzierte Involution $*$ mit der "klassischen" Involution auf D überein (27.3), so dass mit dem Sehgal–Zassenhaus Result folgt, dass uu^* zentral in $\mathbb{Z}G$ ist für jedes Element u aus $\mathbb{Z}G$ welches nur endlich viele Konjugierte unter der Operation von $\mathrm{U}(\mathbb{Z}G)$ hat.[2] Ist also u weiterhin eine Einheit in $\mathbb{Z}G$, so zeigt das übliche "Stern-Argument", dass $u \in \mathrm{N}_{\mathrm{U}(\mathbb{Z}G)}(G)$. Nun zeigt ein Standardargument, dass dieses Ergebnis auch für eine periodische Gruppe G bestehen bleibt.[3]

Man beachte, dass ein Element u von $\mathbb{Z}G$, welches nur endlich viele Konjugierte unter der Operation von $\mathrm{U}(\mathbb{Z}G)$ hat, mit allen unipotenten Elementen von $\mathbb{Z}G$ vertauscht (23.1).

[2] Aus der endgültigen Version [71] von [70] ist kaum ersichtlich, dass in diesem Zusammenhang wir diese (einfache) Beobachtung zuerst verwendeten.

[3] Folglich läßt sich der zu [70, Theorem 2.3] gegebene Beweis unschwer zu einem Beweis von [70, Corollary 4.3] umschreiben.

Dies ist bereits genügend Information, um die Gleichheit $\Delta(\mathrm{U}(\mathbb{Z}G)) = \mathrm{Z}_2(\mathrm{U}(\mathbb{Z}G))$ aus bekannten Resultaten abzuleiten, was in Abschnitt 27 geschehen wird.[4]

Wiederum sei G endlich, und ein Schiefkörper D sei ein Block von $\mathbb{Q}G$. Es sei $\mathbb{Z}[G]$ das Bild von $\mathbb{Z}G$ in D. Unter Verwendung von Amitsurs Klassifikation der endlichen Gruppen, die sich in die multiplikative Gruppe eines Schiefkörpers einbetten lassen, führen wir in den Abschnitten 28 und 29 folgendes aus. Es sei $x \in \mathbb{Z}[G]$. Ist D keine total definite Quaternionenalgebra, so ist x entweder zentral in $\mathbb{Z}[G]$ oder hat unendlich viele Konjugierte unter der Operation von $\mathrm{U}(\mathbb{Z}G)$, und in letzterem Fall konstruieren wir Einheiten in $\mathrm{U}(\mathbb{Z}G)$, welche benützt werden können um unendlich viele Konjugierte zu produzieren. Ist D eine total definite Quaternionenalgebra, geben wir die Gruppe der Einheiten in $\mathbb{Z}[G]$ explizit an (welche von endlicher Ordnung über dem Zentrum ist).

Kapitel VIII

Das ungerade Analogon zu dem berühmten Z^*-Theorem von Glauberman kann wie folgt formuliert werden: *Falls x ein Element von Primzahlordnung p in einer endlichen Gruppe G ist, welches mit keinem seiner anderen Konjugierten vertauscht, dann gilt* $[x, G] \leq \mathrm{O}_{p'}(G)$. Es ist wohlbekannt, dass dieses Theorem für ungerades p leicht mit Hilfe der Klassifikation der endlichen einfachen Gruppen zu beweisen ist, aber einen direkten Beweis zu finden wäre sicherlich nützlich und aufschlußreich.

Man beachte, dass unsere Voraussetzung an das Gruppenelement x gerade besagt, dass seine Klassensumme C_x in $x + \mathrm{Tr}_1^{\langle x\rangle}(\mathbb{Z}G)$ enthalten ist, wobei $\mathrm{Tr}_1^{\langle x\rangle}$ die gewöhnliche relative Spurabbildung bezeichnet.

Es sei χ ein irreduzibler Charakter von G, es bezeichne ω_χ den zu χ gehörigen zentralen Charakter, und es sei $\rho : G \to \mathrm{Mat}_n(\mathcal{O})$ eine Darstellung von G welche uns χ liefert, wobei $\mathcal{O}$ der Ring der ganzen Zahlen in einer endlichen Erweiterung des p-adischen Körpers $\mathbb{Q}_p$ ist, welche eine primitive $p$te Einheitswurzel ζ enthält. Dann gilt $\rho(x) + \mathrm{Tr}_1^{\langle\rho(x)\rangle}(M) = \omega_\chi(C_x)\cdot\mathrm{Id}_n$ für ein $M \in \mathrm{Mat}_n(\mathcal{O})$. Man beachte, dass $\omega_\chi(C_x) \in R = \mathbb{Z}_p[\zeta]$ gilt.

Nun sei $p = 3$, und C_3 eine zyklische Gruppe der Ordnung 3. Dieterich hat gezeigt, dass RC_3 endlichen Darstellungstyp hat, und dass es 9 Isomorphieklassen von unzerlegbaren RC_3-Gittern gibt. Damit leiten wir leicht (30.5) her: *Falls $X \in \mathrm{GL}_n(R)$ die Ordnung 3 besitzt, und falls $X + \mathrm{Tr}_1^{\langle X\rangle}(M) \equiv \omega\cdot\mathrm{Id}_n \pmod{3R}$ für gewisse $M \in \mathrm{Mat}_n(R)$ und $\omega \in R$ gilt, dann ist die Spur von X ein ganzzahliges Vielfaches einer Potenz von ζ.*

Wir können nicht erwarten dass $\mathcal{O} = R$ ist, aber $\mathcal{O}$ ist ein freier R-Modul von endlichem Rang m. Damit haben wir eine R-lineare Einbettung $\mathrm{Mat}_n(\mathcal{O}) \hookrightarrow \mathrm{Mat}_{nm}(R)$, und wir erhalten (in dem Fall $p = 3$), dass $\chi(x)$ *ein ganzzahliges Vielfaches einer Potenz*

[4] Aus den Bemerkungen in [71, S. 95] könnte man unzutreffenderweise schließen, dass wir zu diesem Beweis durch eine sorgfältige Untersuchung von [70] gekommen sind.

von ζ ist.

Es sei e_0 das zu dem Hauptblock B_0 von $\mathbb{Z}_{(3)}G$ gehörige zentrale Idempotent. Es ist wohlbekannt, dass e_0C_x eine Einheit in B_0 ist. Robinson bemerkte, dass unter der Voraussetzung, dass die zu B_0 gehörigen irreduziblen Charaktere die obige Bedingung erfüllen, $u_x = e_0C_x(e_0C_{x^{-1}})^{-1}$ eine zentrale Einheit der Ordnung 3 in B_0 ist, und dass $[x, G] \leq \mathrm{O}_{3'}(G)$ gilt, falls u_x eine triviale Einheit ist, d.h. falls $u_x = e_0g$ für ein $g \in G$ gilt.

Die letzte Beobachtung verbindet die Frage, ob $[x, G] \leq \mathrm{O}_{3'}(G)$ gilt oder nicht gilt, mit der "Defektgruppen-Frage" für den Hauptblock (siehe [128, p. 267]): Selbst bescheidener Fortschritt in Richtung auf eine positive Antwort zu dieser Frage würde zur Konsequenz haben, dass u_x eine triviale Einheit ist (siehe [115]).

Danksagungen

An dieser Stelle möchte ich Prof. Kimmerle für die Gewährung wertvollen Freiraumes zur selbstständigen Arbeit meinen herzlichsten Dank aussprechen.
Ich möchte noch anfügen, daß diese Arbeit durch die Deutsche Forschungsgemeinschaft (DFG) gefördert wurde.
Die Computerprogramme GAP und Maple haben mir bei einem Teil meiner Untersuchungen wertvolle Hilfe geleistet. Für die Erstellung dieser Arbeit wurde LaTeX mit dem Paket KOMA-Script benutzt.

Summary

Longum iter est per praecepta, breve et efficax per exempla.

Lucius Annaeus Seneca
Epistulae Morales ad Lucilium – Liber VI, 62–65

Loosely speaking, "representation theory" is "module theory". One of the main objects of *integral* representation theory should be the construction of indecomposable lattices over orders. A prominent example of a $\mathbb{Z}$-order is the integral group ring $\mathbb{Z}G$ of a finite group G. A fundamental problem (with which we shall *not* be concerned with) is to find a full set of isomorphism invariants of a $\mathbb{Z}G$-lattice M which determines the isomorphism class of M uniquely.

One can envisage $\mathbb{Z}G$, or more general integral representation theory, as a link between ordinary and modular representation theory. (This "universality" already indicates that clarifying the structure of $\mathbb{Z}G$ in general is a delicate issue.) Going further on in this direction, we may regard integral representation theory, in the sense of Curtis and Reiner [28,27], as a central core which connects various topics in ordinary and modular representation theory, algebraic number theory, and algebraic K-theory. This point of view will be illustrated in Chapter III, where we discuss, by means of an example, local–global aspects concerning automorphisms of integral group rings.

It is common usage in representation theory to speak about $\mathbb{Z}G$-modules M having the distinguished group basis G explicitly in mind. (Otherwise, what should be the meaning of M being a permutation module?) However, we may take into account the various ways G can be embedded, as a group basis, into $\mathbb{Z}G$: This leads to questions about ring automorphisms of $\mathbb{Z}G$, the so called "Zassenhaus conjecture" being the most notable one. We may also ask which properties of the finite group G are determined by its integral representations. Asking whether the isomorphism class of G is determined by its integral group ring is the so called "isomorphism problem for integral group rings". These questions are certainly in the sense of well known problems posed by Richard Brauer [18], and they constituted the subject of much research at the end of the past century. We shall discuss the "semilocal version" of the isomorphism problem and the Zassenhaus conjecture in Chapters I and II in some detail. Thereby, the coefficient ring of rational integers $\mathbb{Z}$ is replaced by a suitable semilocalization $\mathbb{Z}_\pi$ of $\mathbb{Z}$ (which we shall

introduce next), thus avoiding questions about locally free class groups.

The knowledge of the p-adic group rings $\mathbb{Z}_pG$ yields insight into the possible actions of G on abelian groups. Since the most interesting arithmetical properties are lost when one passes from $\mathbb{Z}G$ to a maximal over order in $\mathbb{Q}G$, we are tempted to consider as an appropriate "integral coefficient ring with respect to G" the semilocalization

$$\mathbb{Z}_\pi := \bigcap_{p||G|} \mathbb{Z}_{(p)}.$$

This ring is more "comfortable" than $\mathbb{Z}$ itself, since it has only finitely many maximal ideals, and the same is true for the group ring $\mathbb{Z}_\pi G$. Nevertheless, $\mathbb{Z}_\pi G$ has all interesting quotients: For a prime p dividing the order of G, and a natural number n, we have canonical ring homomorphisms $\mathbb{Z}G \hookrightarrow \mathbb{Z}_\pi G \twoheadrightarrow (\mathbb{Z}/p^n\mathbb{Z})G$.

Suppose one is interested in the properties of G which are determined by the module category $\mathbb{Z}G\,\mathrm{Mod}$, this is even the better setting since the following statements are equivalent: there is an equivalence $\mathbb{Z}G\,\mathrm{Mod} \simeq \mathbb{Z}H\,\mathrm{Mod}$ of module categories; there is an isomorphism $\mathbb{Z}_\pi G \cong \mathbb{Z}_\pi H$ of rings; there is an equivalence $\mathbb{Z}_\pi G\,\mathrm{Mod} \simeq \mathbb{Z}_\pi H\,\mathrm{Mod}$.

In Chapter III we show that there is a group G of order 96 such that the semilocal group ring $\mathbb{Z}_\pi G$ has an automorphism which does not agree, up to an inner automorphism of $\mathbb{Q}G$, with some automorphism of $\mathbb{Z}G$.

Certain *group* automorphisms naturally appeared in the analysis of the Zassenhaus conjecture and the isomorphism problem. New motivation to study class-preserving automorphisms of finite groups came from work of Roggenkamp and Kimmerle, which related them to the Zassenhaus conjecture (research in this direction began in [117]). An observation of Mazur linked the isomorphism problem for integral group rings with the existence of certain non-inner class-preserving automorphisms, namely those which induce inner automorphisms of the group ring. Moreover, in Scott's opinion, the picture in the solvable group case of a semilocal group ring automorphism should be a collection of group isomorphisms on inertial groups that fit together rationally, and their should be a similar description for group ring isomorphisms. A large part of the first two chapters, and the whole Chapter IV, is devoted to the study of group automorphisms which show up in this context.

Chapters V–VII constitute another part of this work. In contrast with the first part, we then deal with units of integral group rings of *infinite* groups. The results will be, of course, also valid for group rings of finite groups, but the tenor will be that emphasis is put on the reduction to the finite group case, which is either known or assumed to be manageable. We can consider the unit group $\mathrm{U}(\mathbb{Z}G)$ for an arbitrary group G, but in most cases the results are complete only for the case that G is a periodic group. This is related to the fact that so far we know little about the multiplicative group of the integral group ring of a torsion-free group. Instead of $\mathbb{Z}G$ we shall consider more general RG, where R is a G-adapted ring, that is, an integral domain of characteristic 0 in which

a prime p is not invertible whenever G has an element of order p. We shall elaborate on the normalizer of G in the unit group $\mathrm{U}(RG)$, the upper central series of $\mathrm{U}(RG)$ and the finite conjugacy center of $\mathrm{U}(\mathbb{Z}G)$.

We shall say that a group G has the *normalizer property* if for any G-adapted ring R, the normalizer $\mathrm{N}_{\mathrm{U}(RG)}(G)$ of G in $\mathrm{U}(RG)$ consists of the obvious units only, i.e., if $\mathrm{N}_{\mathrm{U}(RG)}(G) = \mathcal{Z}G$, where $\mathcal{Z}$ denotes the center of $\mathrm{U}(RG)$. Asking whether a group has the normalizer property or not will be termed the normalizer problem. It has been shown that groups which do *not* have the normalizer property may serve as building blocks for counterexamples to the isomorphism problem.

In Chapter V we study the normalizer problem for infinite groups, motivated by results of Mazur [93], who was probably the first one to work on this problem. We will answer the questions raised in [93], and we will give classes of groups having the normalizer property, enlarging those given by Jespers, Juriaans, de Miranda and Rogerio [72].

In Chapter VI we examine the upper central series $1 \trianglelefteq \mathrm{Z}_1(\mathcal{U}) = \mathrm{Z}(\mathcal{U}) \trianglelefteq \mathrm{Z}_2(\mathcal{U}) \trianglelefteq \dots$ of the unit group $\mathcal{U} = \mathrm{U}(RG)$ of an integral group ring RG of a periodic group G. Our motivation comes from the fact that $\mathrm{Z}_2(\mathcal{U}) \leq \mathrm{N}_{\mathcal{U}}(G)$. This observation is the starting point of Li's paper [86], where it is shown that $\mathrm{Z}_2(\mathcal{U}) = \mathrm{Z}_3(\mathcal{U})$ in the $R = \mathbb{Z}$ case. Recently, a complete description of $\mathrm{Z}_2(\mathcal{U})$ in the $R = \mathbb{Z}$ case was given by Li and Parmenter [87]. Using different methods, we obtained independently the corresponding description in the general case: $\mathrm{Z}_3(\mathcal{U}) = \mathrm{Z}_2(\mathcal{U}) \leq \mathrm{Z}(\mathcal{U})\mathrm{Z}_2(G)$; and if $\mathrm{Z}_2(\mathcal{U}) \neq \mathrm{Z}(\mathcal{U})$, then G is a so called Q^*-group.

In Chapter VII we show that for a periodic group G, the second center $\mathrm{Z}_2(\mathrm{U}(\mathbb{Z}G))$ conincides with the finite conjugacy center of $\mathrm{U}(\mathbb{Z}G)$, i.e., with the set of elements of $\mathrm{U}(\mathbb{Z}G)$ having only finitely many conjugates under the action of $\mathrm{U}(\mathbb{Z}G)$.

The last chapter is intended to raise hopes that significant applications of integral representation theory to finite group theory will be found some day. It is an important open problem to find a direct and "representation-theoretic" proof of some odd analogue to Glauberman's Z^*-theorem. Robinson [114] studied the character theory of a minimal counterexample, K, to the Z_p^*-theorem for odd p. In [115], Robinson showed that his results can be used to place the problem in quite another context, that of units in group rings: he demonstrated the existence of a nontrivial central unit of order p in the principal p-block of K, provided that $p \geq 5$, or that $p = 3$ and K is not simple.

We show that if $p = 3$, and x is an element of order 3 in K which commutes with none of its other conjugates, then for each irreducible character χ of K, the character value $\chi(x)$ is an integral multiple of a power of a primitive third root of unity ζ. As a consequence, the existence of the nontrivial central unit in the principal p-block is guaranteed in any case. The idea of the proof is actually quite simple, and is based on the classification of the indecomposable $\mathbb{Z}[\zeta]C_3$-lattices. We've come full circle of this short overview of the present paper!

Each chapter is self-contained, and its content is described in detail below.

The reader will notice that this paper contains many examples. We think that nowadays this needs no justification; we are confident that "The way is made long through rules, but short and effective through examples."

Nevertheless, we would like to render some considerations of Ringel on this theme. The reader only interested in the results of this paper can safely skip the following remark.

Looking at examples. We would like to quote three pointed remarks from Ringel's paper [112]:

1. There is a book on the foundations of module and ring theory [147] (with the subtitle "A handbook for study and research"), which, as Ringel puts it, *"manages to avoid any nontrivial examples whatsoever"*, and that *"It should not be surprising that it claims to present a proof that all indecomposable artinian modules have local endomorphism rings, an assertion which would imply the validity of Krull-Remak-Schmidt for artinian rings."* (See 31.14 of the book; the "proof" essentially carries over Guérindon's error [45].) Fortunately, we can quote from the introduction of the 1991 English edition: "Besides several minor changes and improvements this English edition contains a number of new results." There are remarkably simple examples of indecomposable artinian modules whose endomorphism rings are not local, for example modules over the ring $\left[\begin{smallmatrix}\mathbb{Q} & 0\\ \mathbb{Q} & \mathbb{Z}\end{smallmatrix}\right]$ (see [111]).
2. *"Apparently, until 1998 no one had studied artinian modules over a ring such as* $\left[\begin{smallmatrix}\mathbb{Q} & 0\\ \mathbb{Q} & \mathbb{Z}\end{smallmatrix}\right]$. *To get inspiration from examples should be one of the most important endeavour of mathematicians. But in contrast, to look at examples was considered quite obsolete by many algebraists until very recent times."*
3. From the "maybe provocative postulates" concerning the prospects of algebra in this century, given at the end of the paper, we quote: *"Many new phanomena should be discovered when studying non-commutative structures in greater detail. (The preoccupation with the development of "theories" has neglected up to now the careful study of examples.)"*

We briefly outline some background; Ringel's papers [111,112] are the source where we copied from.

To begin with, we remark that the presentation stresses the fact that categorical equivalences show that a given category may be realized in different ways.

The theorem of Krull-Remak-Schmidt is one of the basic results in representation theory. In 1932, Krull asked whether direct decompositions of a general artinian module into indecomposables are unique up to isomorphisms. Only in 1995, this question was answered in the negative in a joint paper of Facchini, Herbera, Levy and Vámos.

Following the Pimenov-Yakovlev approach [104], consider the "innocent" ring $R = \left[\begin{smallmatrix}\mathbb{Q} & 0\\ \mathbb{Q} & \mathbb{Z}\end{smallmatrix}\right]$. (This ring is really innocent, though after Small's example [135] from 1965, certainly many students (including the author) were forced to have a look at this ring. Furthermore, it should be remarked that today, it is known that triangular matrix rings arising from bimodules act as a good source for constructing "counterexamples", see for example [52, 41, 139, 104].)

What are the left R-modules? Given a left R-module M, set $B = e_1M$ and $A = e_2M$, where $e_1 = \left[\begin{smallmatrix}1 & 0\\ 0 & 0\end{smallmatrix}\right]$ and $e_2 = \left[\begin{smallmatrix}0 & 0\\ 0 & 1\end{smallmatrix}\right]$. Clearly $M = B \oplus A$ as additive groups. Note that A is a submodule of M, annihilated by Re_1R, and that $R/Re_1R = \mathbb{Z}$, so A is really a $\mathbb{Z}$-module. The quotient M/A is just the $\mathbb{Q}$-module B. Multiplication with $\left[\begin{smallmatrix}0 & 0\\ 1 & 0\end{smallmatrix}\right]$ on M yields a $\mathbb{Z}$-linear map $\gamma : B \to A$. Conversely, such a triple (B, A, γ) determines a column module $M = \left[\begin{smallmatrix}B\\ A\end{smallmatrix}\right]_\gamma$, with the obvious "matrix multiplication" $\left[\begin{smallmatrix}x & 0\\ z & y\end{smallmatrix}\right] \cdot \left[\begin{smallmatrix}b\\ a\end{smallmatrix}\right] = \left[\begin{smallmatrix}xb\\ (zb)\gamma + ya\end{smallmatrix}\right]$.

Let $\mathcal{A}'$ be the category of all $\mathbb{Z}$-linear maps $\gamma : B \to A$, where A, B are abelian groups with B torsion-free divisible, together with the obvious morphisms. (Note that the torsion-free divisible abelian groups are just the $\mathbb{Q}$-vector spaces.) Then we have essentially shown that there is an isomorphism of categories $\eta : \mathcal{A}' \to R\,\mathrm{Mod}$ so that $\eta(B, A, \gamma) = \left[\begin{smallmatrix} B \\ A \end{smallmatrix}\right]_\gamma$.

What are the artinian left R-modules? An R-module $\left[\begin{smallmatrix} B \\ A \end{smallmatrix}\right]_\gamma$ is artinian if and only if A is an artinian abelian group and B is a finite dimensional vector space over $\mathbb{Q}$. Thus if we assume that γ is surjective (so that A is divisible too), then $\left[\begin{smallmatrix} B \\ A \end{smallmatrix}\right]_\gamma$ is artinian if and only if B is of finite rank and A is the direct sum of finitely many Prüfer groups.

Now let $\mathcal{A}$ be the full subcategory of $\mathcal{A}'$ consisting of all surjective $\mathbb{Z}$-linear maps $\gamma : B \to A$, where B is torsion-free of finite rank and A is an artinian $\mathbb{Z}$-module. Also, let $\mathcal{F}$ be the category of torsion-free abelian groups F of finite rank such that $pF = F$ for almost all prime numbers p. The members of $\mathcal{F}$ are precisely the groups F that occur as the kernel of a map γ as above, and an exact sequence $0 \to F \to \mathbb{Q}^n \to A \to 0$, where A is artinian, is a minimal injective resolution of F. This shows that we have a categorical equivalence $\mathcal{F} \simeq \mathcal{A}$.

Nothing strange has happened, but that $\mathcal{A}$ may be interpreted as a category of artinian modules over the ring R is what had been neglected before. For it has been established a long time ago that the category $\mathcal{F}$ does not satisfy the theorem of Krull-Remak-Schmidt: The first example was given by Jónsson in 1945, later ones were given by Butler, Corner, Fuchs and others. In some sense, Krull's problem has been solved 50 years before it was answered in the negative in 1995!

Chapter I

We assume that the reader is familiar with the notions integral group ring and isomorphism problem for integral group rings. In the first four chapters, we shall only deal with finite groups G. When we write $\mathbb{Z}_\pi G$ it is understood that $\mathbb{Z}_\pi$ is the intersection of localizations $\mathbb{Z}_{(p)}$ with p ranging over a finite set π of primes which contains the prime divisors of the order of G. Note that $\mathbb{Z}_\pi G$ is a semilocal ring.

Graham Higman termed $\mathcal{O}G$ an integral group ring whenever $\mathcal{O}$ is a ring of algebraic integers. We shall call $\mathbb{Z}_\pi G$ an integral group ring as well. With respect to the isomorphism problem for integral group rings, this is justified by (1.1): It follows from Jacobinski's fundamental work on genera of lattices that $\mathbb{Z}_\pi G \cong \mathbb{Z}_\pi H$ implies that $\mathcal{O}G \cong \mathcal{O}H$ for some ring $\mathcal{O}$ of algebraic integers. Another local–global aspects are discussed in Section 1, including Scott's approach to the construction of group ring automorphisms and isomorphisms in the semilocal case that avoids any explicit use of the theory of orders (see (1.4) and (1.6)). We shall apply such constructions in Sections 3 and 8, and (1.4) will also be helpful for the understanding of part of Chapter 3.

In Section 2 we talk about possibilities how to construct counterexamples to the isomorphism problem for integral group rings in the semilocal group ring case. In (2.3) we show how an observation of Mazur can be adapted to the finite group case, which involves the use of multiplicative 1-cocyles. We also point out the local–global aspect (2.10) of this construction, introducing the notion of local system of 1-cocycles, which

shall be a collection of local 1-cocycles which differ rationally by 1-coboundaries.

There are two non-isomorphic groups X and Y, both of order $2^{21} \cdot 97^{28}$, which have isomorphic integral group rings, $\mathbb{Z}X = \mathbb{Z}Y$. Having these groups at hand, we pursue in Section 3 the way prescribed by (1.6) to show that the group rings are semilocally isomorphic. This leads to new insight into the structure of these groups. Actually, this allows us to make a small modification: We will replace the Sylow 97-subgroup by a Sylow 17-subgroup, without changing the structure of the groups. The question remains open whether this yields another global counterexample.

Motivated by the semilocal analysis of the counterexample, we present in Section 4 a p-group (for any prime p) which likewise has those properties of the Sylow 2-subgroup of X which turned out to be crucial to the semilocal construction. This strongly suggests that there should be semilocal counterexamples to the isomorphism problem with the underlying groups having odd order.

Knowledge about automorphisms of integral group rings may help to settle the isomorphism problem for certain classes of groups, via (variations of) Kimmerle's $G \times G$-trick. This will be demonstrated in Section 5, where we give another proof of a theorem due to Scott. From knowledge about automorphisms (5.5) we deduce (5.7): Finite abelian by nilpotent groups are determined by their integral group rings.

Chapter II

This chapter contains various results related to the Zassenhaus conjecture (concerning automorphisms of integral group rings $\mathbb{Z}G$, where G is a finite group).

In Section 6, we take the opportunity to collect in an omnibus lemma (6.1) some more or less well known properties of antiinvolutions of group rings associated to group bases which are related to the Zassenhaus conjecture. For example, if $\alpha \in \mathrm{Aut}_{\mathrm{n}}(\mathbb{Z}G)$, and $*$ denotes the antiinvolution associated to G, then $[*, \alpha] = \mathrm{conj}(u^*u)$ for some $u \in \mathrm{N}_{\mathrm{U}(\mathbb{Q}G)}(\mathbb{Z}G)$ if and only if α admits a Zassenhaus decomposition with respect to G, that is, if there is $\rho \in \mathrm{Aut}(G)$ such that $\alpha\rho \in \mathrm{Inn}(\mathbb{Q}G)$. We also wish to point out a conjugacy criterion (6.4), which, however, has not yet found applications.

Roggenkamp and Scott showed that in the presence of normal subgroups $N_1, \ldots, N_r$ of G of pairwise coprime order, an integral group ring RG can be described by a pullback diagram (7.1) which proved to be very useful to construct counterexamples to the Zassenhaus conjecture. We shall give a detailed proof of this result in Section 7, thereby pointing out in (7.2) an interesting description of the ideal $\sum_{i=1}^{r}(RG) \cdot \hat{N}_i$.

The Roggenkamp–Scott result can also be used to compute unit groups of integral group rings. This is illustrated in (7.3) where we compute the unit group of $\mathbb{Z}C_{10}$ and its index in the unit group of a maximal over order.

Lam and Leung (7.4) solved the following problem in number theory: Given a natural number m, what are the possible integers n for which there exist mth roots of unity

$\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ such that $\alpha_1 + \cdots + \alpha_n = 0$? We will put their crucial results into a more general context, the results then being stated entirely in the language of group rings, since we can use (7.2) to dispense with some linear disjointness arguments. The starting point will be (7.7): For normal subgroups A and B of G with $A \cap B = 1$, we have $\mathbb{N}_0 G \cap (\mathbb{Z}G \cdot \hat{A} + \mathbb{Z}G \cdot \hat{B}) = \mathbb{N}_0 G \cdot \hat{A} + \mathbb{N}_0 G \cdot \hat{B}$ (here $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$). Then, we will follow closely the presentation given by Lam and Leung to give a generalization of (7.4) in (7.11): The augmentation of each element of $\mathbb{N}_0 G \cap \sum_{i=1}^{r} \mathbb{Z}G \cdot \hat{N}_i$ is contained in $\sum_{i=1}^{r} \mathbb{N}_0 |N_i|$.

In Section 8, we turn to the construction of semilocal counterexamples to the Zassenhaus conjecture. (Such examples often have been called "counterexamples", they were considered as very surprising. But it seems now that such a behavior should be rated as quite usual.) After some preparatory work, we are ready to produce such examples with relatively minor effort, which will include a metabelian group with abelian Sylow subgroups, a supersolvable group, and a Frobenius group.

In Section 9, we calculate the group- and character table automorphisms for the wreath products $G_{n,r} = (\mathbb{Z}/r\mathbb{Z}) \wr S_n$, which form one of the two infinite series of irreducible finite complex reflection groups. In particular, we will see that the Zassenhaus conjecture holds for these groups (which, however, is already known [129, Section 44]). More precisely, we show for $G_{n,r} \neq G_{2,2}$ that the sequence $1 \to \mathrm{Inn}(G_{n,r}) \to \mathrm{Aut}(G_{n,r}) \to \mathrm{AutCT}(G_{n,r}) \to 1$ is exact (9.2), which generalizes [14, Proposition 4.3], and we describe $\mathrm{Out}(G_{n,r})$ explicitly (9.1).

Chapter III

The main result of this chapter is that the semilocal group ring $\mathbb{Z}_\pi G$ of a finite group G may have an automorphism α which is not represented by a global one, that is, there is no automorphism of $\mathbb{Z}G$ which differs on $\mathbb{Q}G$ from α only by an inner automorphism.

We will work out an example, using one of Blanchard's groups G of order 96 from [13]. This group is of the form $G = (\langle q : q^3 \rangle \times \langle c : c^2 \rangle \times \langle b : b^4 \rangle) \rtimes \langle a : a^4 \rangle$. Blanchard showed that there is an $\alpha \in \mathrm{Aut}_{\mathrm{n}}(\mathbb{Z}_\pi G)$ which permutes only the two faithful irreducible characters of G, and which cannot be written as the product of a group automorphism (extended to $\mathbb{Z}_\pi G$) and a central automorphism. We will show that such an α is not represented by a global automorphism.

We briefly describe our strategy. Associated with the normal subgroups $Q = \langle q \rangle$ and $M = \mathrm{Z}(G) = \langle b^2 \rangle$ of G, we have the pullback diagram (7.1)

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \Gamma \\ \downarrow & & \downarrow \\ \Lambda & \longrightarrow & \Lambda_2 \oplus \Lambda_3 \end{array} .$$

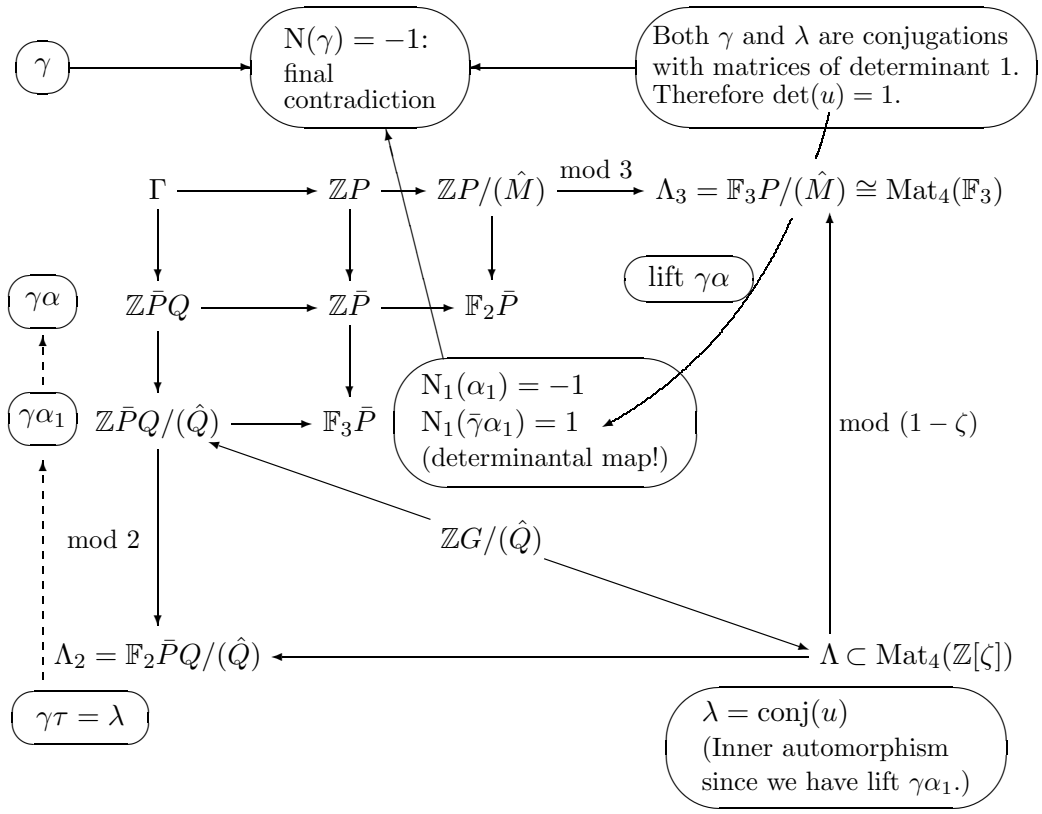
We may assume that $\Lambda \subset \mathrm{Mat}_4(\mathbb{Z}[\zeta])$, where ζ denotes a primitive third root of unity, since precisely the two faithful irreducible characters of G, which are algebraically conjugate, belong to $\mathbb{C}\Lambda$.

There is $\tau \in \mathrm{Aut}(G)$ which permutes the two faithful irreducible characters, and induces an inner automorphism on $\Lambda_2 \oplus \Lambda_3$. The whole discussion boils down to the question whether there are $\gamma \in \mathrm{Autcent}(\Gamma)$ and $\lambda \in \mathrm{Autcent}(\Lambda)$ which differ on the common quotient $\Lambda_2 \oplus \Lambda_3$ by the inner automorphism induced by τ. Assuming that such automorphisms exist, we will finally reach a contradiction.

Let $P = \langle a, b, c \rangle$, a Sylow 2-subgroup of G, and let bars denote reduction modulo M, so that $\bar{P} = P/M$. Then Γ is the image of the natural map $\mathbb{Z}G \to \mathbb{Z}\bar{P}Q \oplus \mathbb{Z}P$. The automorphism γ induces central automorphisms of $\mathbb{Z}\bar{P}Q$ and $\mathbb{Z}P$ which shall also be denoted by γ.

For each $\beta \in \mathrm{Autcent}(\mathbb{Z}P)$, we can define a norm $\mathrm{N}(\beta) \in \{\pm 1\}$ as follows: β induces on the proper matrix ring summands of $\mathbb{Q}P$ inner automorphisms given by conjugation with matrices of determinant ± 1, and $\mathrm{N}(\beta)$ is the product of the determinants of such matrices. Using Fröhlich's localization sequence, and Mayer–Vietoris sequences to calculate locally free class groups, we are able to show that always $\mathrm{N}(\beta) = 1$.

Consider now the following diagram, in which each "square" is a pullback diagram.



(The meaning of the filled in ovals will be explained subsquently.)

We can similarly define a norm N_1 for central automorphisms of $\mathbb{F}_3\bar{P}$. Any $\beta \in \mathrm{Autcent}(\mathbb{Z}P)$ induces an inner automorphism $\bar{\beta}$ of $\mathbb{F}_3\bar{P}$ and an inner automorphism $\mathrm{conj}(T)$ of $\Lambda_3 \cong \mathrm{Mat}_4(\mathbb{F}_3)$, and we have $\mathrm{N}(\beta) = \mathrm{N}_1(\bar{\beta}) \cdot \det(T)$.

It is easy to see that we can assume without lost of generality that on Λ_3, both γ and λ are conjugations with matrices of determinant 1.

We will construct an inner automorphism α_1 of $\mathbb{Z}\bar{P}Q/(\hat{Q})$ which lifts the inner automorphism τ induces on Λ_2, and we will show that α_1 lifts further to a central automorphism α of $\mathbb{Z}\bar{P}Q$.

In particular, λ is induced from a central automorphism of $\mathbb{Z}G/(\hat{Q})$, which implies that λ induces an inner automorphism of $\mathbb{Z}_2\Lambda$. Using again Fröhlich's localization sequence, we then see that λ is an inner automorphism, $\mathrm{conj}(u)$ (say). Note that $\det(u) = 1$ since the reduction of u modulo $(1-\zeta)$ has determinant 1.

The automorphism γ induces a central automorphism $\bar{\gamma}$ of $\mathbb{F}_3\bar{P}$, and we are interested in $\mathrm{N}_1(\bar{\gamma})$. Each central automorphism of $\mathbb{Z}\bar{P}Q/(\hat{Q})$ induces a central automorphism of $\mathbb{F}_3\bar{P}$. We know that $\mathrm{N}_1(\alpha_1) = -1$, so we try to calculate $\mathrm{N}_1(\bar{\gamma}\alpha_1)$ since $\gamma\alpha_1$ is a lift of the automorphism λ induces on Λ_2.

Let $U \leq \Lambda^\times$ consist of those units v such that there is a central automorphism β_v of $\mathbb{Z}\bar{P}Q/(\hat{Q})$ which induces on Λ_2 the inner automorphism given by conjugation with the image of v. Then, the assignment $v \mapsto \mathrm{N}_1(\bar{\beta}_v)$ yields a well defined homomorphism $d : U \to \{\pm 1\}$. The author would very much like to know whether there is a general argument showing that this homomorphism arises from the determinantal map.

What we will show is that if for some $v \in \Lambda^\times$, the inner automorphism of Λ_2 given by conjugation with the image of v can be lifted to a central automorphism ν of $\mathbb{Z}\bar{P}Q$, then $\det(v) = \pm 1$, and $\det(v) = 1$ if and only if $d(v) = 1$. This will be done by carefully modifying v and ν, using suitable "modifications" of bicyclic units, until the claim will be obvious.

So $\mathrm{N}_1(\bar{\gamma}\alpha_1) = \det(u) = 1$, and consequently $\mathrm{N}(\gamma) = -1$, the final contradiction.

Chapter IV

This chapter contains a loose variety of results concerning specific automorphism groups which showed up in connection with the Zassenhaus conjecture and the isomorphism problem.

In Section 14, we only briefly touch upon class-preserving automorphisms of finite groups when showing (14.4) that class-preserving automorphisms of abelian by cyclic groups are inner automorphisms.

A Coleman automorphism of a finite group G is an automorphism of G whose restriction to any Sylow subgroup of G equals the restriction of some inner automorphism of G. In Section 15, we continue research began in [61] and study the structure of a finite

group G which has a non-inner Coleman automorphism of p-power order under the assumption that no chief factor of $G/\mathrm{F}^*(G)$ is isomorphic to C_p. Actually, we do not know whether such a group exists, but we study the structure of a minimal counterexample. By means of an example (15.4) we show that this leads to interesting questions (15.6) about central extensions, mainly of simple groups, which, however, will remain open. We also briefly consider Coleman automorphisms of central extensions.

In Section 16, we shall deal with subdirect products of finite groups. More specifically, we discuss the concept of twisted projective limits, which appears naturally in the discussion of the integral isomorphism problem for solvable groups, see (16.5). We give an example (16.17) where twisting with an inner automorphism leads to a non-isomorphic group of the same order.

We note that if G is a projective limit, then $\mathrm{Aut}(G)$ is, under some mild conditions, also a projective limit in a natural way. This provides a convenient way to compute the group of Coleman automorphisms $\mathrm{Aut}_{\mathrm{Col}}(G)$ of a solvable group G, and we will give a short proof of a result of Dade (16.13): $\mathrm{Out}_{\mathrm{Col}}(G)$ is abelian.

A solvable group G is the projective limit of the factor groups $G/\mathrm{O}_{p'}(G)$. We can form the projective limit Γ of the group rings $\mathbb{Z}G/\mathrm{O}_{p'}(G)$ and may ask how much information Γ contains about $\mathbb{Z}G$. We show that there is an exact sequence which measures to some extent how far Γ is away from satisfying a "simultaneous p-version" of the Zassenhaus conjecture.

Chapter V

Let G be a group, and R a commutative ring. The automorphisms of G inducing an inner automorphism of the group ring RG form a group $\mathrm{Aut}_R(G)$. We set $\mathrm{Out}_R(G) = \mathrm{Aut}_R(G)/\mathrm{Inn}(G)$. Note that $\mathrm{Aut}_R(G) \cong \mathrm{N}_{\mathcal{U}}(G)/\mathrm{Z}(\mathcal{U})$, where $\mathcal{U} = \mathrm{U}(RG)$.

The most basic fact about elements of $\mathrm{N}_{\mathcal{U}}(G)$ involves the standard anti-involution $*_G$ of RG: $u \in \mathrm{N}_{\mathcal{U}}(G)$ implies that $uu^{*_G} \in \mathrm{Z}(\mathcal{U})$, which in turn implies $(uu^{-*_G})^{*_G}(uu^{-*_G}) = 1$. The converse is not true in general: Even if R is G-adapted, $uu^{*_G} \in \mathrm{Z}(\mathcal{U})$ does not necessarily imply that $u \in \mathrm{N}_{\mathcal{U}}(G)$. This is, however, true in the $R = \mathbb{Z}$ case. Moreover, if $R = \mathbb{Z}$, then by a classical result due to Higman and Berman, $uu^{-*_G} \in \pm G$ for any $u \in \mathrm{N}_{\mathcal{U}}(G)$, which immediately implies that $\mathrm{Out}_{\mathbb{Z}}(G)$ is of exponent 2. This underlines the special role the coefficient ring $\mathbb{Z}$ plays, and the strength of such "star-arguments". However, we would like to point out that in Chapters V and VI we will not make any use of star-arguments. As a consequence, our results will be valid for arbitrary G-adapted coefficient rings R. Some of our results are already known in the $R = \mathbb{Z}$ case. Then, however, the known proofs often involve star-arguments, and we had to find different proofs, see e.g. (19.1) and (19.3).

In Section 17, the point is what can be said about $\mathrm{Out}_R(G)$ without making any further assumption on the coefficient ring R. Our first result (17.3) is that $\mathrm{Aut}_R(G) \leq \mathrm{Aut}_{\mathrm{c}}(G)$.

When studying $\mathrm{N}_{\mathcal{U}}(G)$, the first basic observation is that we can work in the group ring of the FC-center $\Delta(G)$ of G, since for $u \in \mathrm{N}_{\mathcal{U}}(G)$ with $1 \in \mathrm{supp}(u)$, we have $D := \{g^{-1}g^u \mid g \in G\} \subseteq \mathrm{supp}(u) \subseteq \Delta(G)$. In (17.2), we show that $\langle D\rangle$ and $\langle \mathrm{supp}(u)\rangle$ are normal subgroups of G. If furthermore $u = u^{*G}$, then $T := \{g^{-1}g^v \mid g \in G, v \in \langle u\rangle\} \subseteq \mathrm{supp}(u)$. This is an interesting result inasmuch as it tells us that T is a finite set, and we can involve a (group-theoretical!) theorem of Baer (17.4) to conclude that $N = \langle T\rangle$ is a *finite* normal subgroup of G. Note that conjugation with u induces the identity on G/N.

Using ideas of Mazur [93], and again Baer's theorem, we will eventually show in (17.8) that any element of $\mathrm{Aut}_R(G)$ induces an inner automorphism of G/N for some finite normal subgroup N of G. As a corollary, we obtain (17.9): The group $\mathrm{Out}_R(G)$ is periodic. Provided that $\Delta(G)$ is finitely generated, we show in (17.7) that $\mathrm{Out}_R(G)$ is a finite group.

We finish the section with some examples which provide negative answers to some questions from [93]. In particular, we show that for $u \in \mathrm{N}_{\mathcal{U}}(G)$, there need not be a group element $g \in G$ such that $\langle \mathrm{supp}(ug)\rangle$ is a finite group (cf. with (18.5)). Furthermore, if a prime p divides the order of an element of $\mathrm{Out}_R(G)$, then G need not have an element of order p.

In Section 18, we shall give short and unified proofs of some "representation theorems" appearing in [74, 72, 70]. The basic idea (18.1) behind these theorems is to generalize the classical result that the group ring $\mathbb{Q}H$ of an ordered group H has only trivial units. Let $\Delta^+(G)$ be the set of torsion elements in $\Delta(G)$ (a characteristic subgroup of G), and let R be a $\Delta^+(G)$-adapted ring. Then we have the "representation theorem" (18.5): For any $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ with $1 \in \mathrm{supp}(u)$, the support group $\langle \mathrm{supp}(u)\rangle$ is a finite normal subgroup of G. As a corollary, we obtain (18.6): If $u \in \mathrm{N}_{\mathrm{V}(RG)}(G)$ is such that $u^n \in G$ for some $n \in \mathbb{N}$, then $u \in G$. Another corollary (18.7) is that if a prime p divides the order of an element of the periodic group $\mathrm{Out}_R(G)$, then $\Delta^+(G)$ has an element of order p.

From now on, R always denotes a $\Delta^+(G)$-adapted ring.

In Section 19, we shall use (18.5) to analyze in (19.1) and (19.3) the structure of $\mathrm{N}_{\mathrm{V}(RG)}(G)/G$ (this is a torsion-free abelian group) and $\mathrm{N}_{\mathrm{V}(RG)}(G)/\mathrm{Z}(\mathrm{V}(RG))G$.

We shall say that G has the *normalizer property* if for any G-adapted ring R, we have $\mathrm{Out}_R(G) = 1$, or, equivalently, $\mathrm{N}_{\mathrm{U}(RG)}(G) = \mathrm{Z}(\mathrm{U}(RG))G$. We will use (18.5) also to verify the normalizer property for certain classes of groups. We would like to mention that we almost completed our results when we obtained a preprint of work done by Jespers, Juriaans, de Miranda and Rogerio [72]. We compare their main results with the corresponding results we could obtain:

A group G has the normalizer property provided G belongs to one of the classes given

in [72]:	in Section 19:
• groups such that $\Delta^+(G)$ is without non-trivial 2-torsion; torsion groups with normal Sylow 2-subgroup;	(19.11) groups whose finite normal subgroups have a normal Sylow 2-subgroup;
• locally nilpotent groups;	(19.12) groups whose finite normal subgroups are nilpotent;
• FC-groups with $[G, G]$ a p-group.	(19.6) groups such that finite factor groups of $[G, G]$ are p-groups.

(Strictly speaking, only $\mathrm{Out}_{\mathbb{Z}}(G) = 1$ was verified in [72].)

One of the reasons why we obtain larger classes is that we use for infinite groups the proper version of the Ward–Coleman Lemma (see page 138): If G is finite, one usually considers the action of some $u \in \mathrm{N}_{\mathcal{U}}(G)$ on a Sylow p-subgroup of G, whereas if G is infinite, one has to consider the action on subgroups which are of finite p'-index in G (see (19.4)). As an application, we obtain at once (19.6), without making any use of the "representation theorem"!

We also give a technical lemma (19.5) which allows us to make full use of the "representation theorem" (18.5). That way, the well known fact (19.14) that a finite group G has the normalizer property provided G has a normal p-subgroup containing its own centralizer in G, carries over to the infinite group case (19.15).

In Section 20 we briefly discuss, following [72], the question for when RG has "only trivial central units". We show (20.3) that if R is an integral domain of characteristic zero in which no rational prime is invertible, then the phrase "RG possesses only trivial central units" is justified, as it is independent from the underlying group basis. The proof makes use of a result of Burn, saying that the support group of a central idempotent in RG is a finite normal subgroup of G.

Burn's result will also be used to give a positive answer (20.6) to a question of Mazur [92, p. 438]: If G is a FC-group, and R is G-adapted, then any group basis of RG is also a FC-group.

Chapter VI

Let $\mathcal{U}$ be the group of units of a group ring RG, where G is a periodic group, and R a G-adapted ring, and let $1 \trianglelefteq \mathrm{Z}_1(\mathcal{U}) = \mathrm{Z}(\mathcal{U}) \trianglelefteq \mathrm{Z}_2(\mathcal{U}) \trianglelefteq \ldots$ be the upper central series of $\mathcal{U}$. Our main result (21.2) is that $\mathrm{Z}_3(\mathcal{U}) = \mathrm{Z}_2(\mathcal{U}) \leq \mathrm{Z}(\mathcal{U})\mathrm{Z}_2(G)$; and if $\mathrm{Z}_2(\mathcal{U}) \neq \mathrm{Z}(\mathcal{U})$, then G is a so called Q^*-group (as defined in (21.1)).

Q^*-groups appear, possibly for the first time, in the paper [16] of Bovdi, who proved that if G has a non-central subgroup which is normal in $\mathrm{U}(\mathbb{Z}G)$, then G is a Q^*-group.

We would like to remark that our presentation stresses the fact that there is a strong connection with the normalizer problem.

First of all, it is easy to see that $\mathrm{Z}_2(\mathcal{U}) \leq \mathrm{N}_{\mathcal{U}}(G)$. Assume for a moment that G has the normalizer property, that is, we have $\mathrm{N}_{\mathcal{U}}(G) = \mathrm{Z}(\mathcal{U})G$. Then $\mathrm{Z}_2(\mathcal{U}) = \mathrm{Z}(\mathcal{U})(G \cap \mathrm{Z}_2(\mathcal{U}))$. Take any $g \in G \cap \mathrm{Z}_2(\mathcal{U})$ and $u \in \mathcal{U}$. Then $g^u \in \mathrm{Z}_2(\mathcal{U}) \leq \mathrm{N}_{\mathcal{U}}(G)$, and since g^u has finite order, it follows that $g^u \in G$ (see (23.2.4) or (18.6)). Thus $G \cap \mathrm{Z}_2(\mathcal{U})$ is a normal subgroup of $\mathcal{U}$, and our main result (21.2) follows from Bovdi's results (see (24.4) and (25.3)).

Set $\mathrm{Z}_\infty(\mathcal{U}) = \bigcup_{n=1}^{\infty} \mathrm{Z}_n(\mathcal{U})$. Vitally for our strategy will be (23.3), where we establish that $\mathrm{Z}_\infty(\mathcal{U}) \leq \mathrm{N}_{\mathcal{U}}(G)$ and that elements of $\mathrm{Z}_\infty(\mathcal{U})$ commute with all unipotent elements of $\mathcal{U}$. Then, we will show in (23.5) that if some $u \in \mathrm{N}_{\mathcal{U}}(G)$ commutes with all unipotent elements of $\mathbb{Z}G$, then $\mathrm{conj}(u)$ induces a power automorphism of G, and if G is not a Dedekind group, then $[G, u] \leq \mathrm{R}(G)$, where $\mathrm{R}(G)$ denotes the intersection of all non-normal subgroups of G. This allows us to involve two group-theoretical results. The first one is Blackburn's classification (22.2) of the finite groups G with $\mathrm{R}(G) \neq 1$. This classification will be used to prove (23.8): If G is not a Dedekind group, and if some $u \in \mathrm{N}_{\mathcal{U}}(G)$ commutes with all unipotent elements of $\mathbb{Z}G$, then $u \in \mathrm{Z}(\mathcal{U})G$. The other result, due to Cooper, is that a power automorphism of an arbitrary group is a central automorphism, i.e., induces the identity on the central factor group. This will be used in (23.6) to show that $\mathrm{Z}_\infty(\mathcal{U}) = \mathrm{Z}_2(\mathcal{U})$. Altogether, we obtain in (23.9) that $\mathrm{Z}_\infty(\mathcal{U}) \leq \mathrm{Z}(\mathcal{U})\mathrm{Z}_2(G)$.

Next, we briefly describe what is done in the individual sections.

In Section 21, we describe the main result and tell the story of this classification theorem. In particular, we notice that we obtained our results independently from work of Li and Parmenter, who obtained, using different methods, the result in the $R = \mathbb{Z}$ case.

In Section 22, we use Blackburn's classification to show in case by case analysis (22.4): If a finite group G is not a Dedekind group and if the intersection $\mathrm{R}(G)$ of its non-normal subgroups is nontrivial, then $\mathrm{R}(G) \leq \mathrm{Z}(G)$ and $\mathrm{Out}_{\mathrm{c}}(G) = 1$.

The results from Section 23, where the central proposition (23.3) is established, are already described above.

In order to keep the exposition self-contained, we give in Section 24 a short proof of the above mentioned result of Bovdi.

In Section 25 we show how Bovdi's result can be used to establish that $\mathrm{Z}_\infty(\mathcal{U}) \leq \mathrm{Z}(\mathcal{U})\mathrm{Z}_2(G)$, following closely previous work of Arora, Hales and Passi. And, of course, it now follows from Bovdi's result that G is a Q^*-group provided that $\mathrm{Z}_2(\mathcal{U}) \neq \mathrm{Z}(\mathcal{U})$. We give a complete description (25.3) of $\mathrm{Z}_\infty(\mathcal{U})$ in the case that R is a ring of algebraic integers in a totally real number field. On the other hand, if R is in a certain sense "large enough", then one should expect that $\mathrm{Z}_2(\mathcal{U}) = \mathrm{Z}(\mathcal{U})$, as is shown in (25.4).

Chapter VII

We will show that for a periodic group G, the second center $\mathrm{Z}_2(\mathrm{U}(\mathbb{Z}G))$ of the group of units of $\mathbb{Z}G$ coincides with the finite conjugacy center $\Delta(\mathrm{U}(\mathbb{Z}G))$ of $\mathrm{U}(\mathbb{Z}G)$, i.e., with the set of elements of $\mathrm{U}(\mathbb{Z}G)$ having only finitely many conjugates under the action of $\mathrm{U}(\mathbb{Z}G)$.

To achieve this aim, we will use a theorem of Sehgal and Zassenhaus (26.1). Assume that G is a finite group. If D is a block of $\mathbb{Q}G$ which is a totally definite quaternion algebra then the involution $*$ induced by G coincides with the "classical" involution on D (27.3), so the Sehgal–Zassenhaus result implies that uu^* is central in $\mathbb{Z}G$ for each element u of $\mathbb{Z}G$ having only finitely many conjugates under the action of $\mathrm{U}(\mathbb{Z}G)$.[5] Thus if u is a unit in $\mathbb{Z}G$, then the usual "star-argument" shows that $u \in \mathrm{N}_{\mathrm{U}(\mathbb{Z}G)}(G)$. A standard argument now shows that this result is also valid for a periodic group G.[6]

Note that an element u of $\mathbb{Z}G$ which has only finitely many conjugates under the action of $\mathrm{U}(\mathbb{Z}G)$ commutes with all unipotent elements of $\mathbb{Z}G$ (23.1).

This is already sufficient information to deduce the equality $\Delta(\mathrm{U}(\mathbb{Z}G)) = \mathrm{Z}_2(\mathrm{U}(\mathbb{Z}G))$ from known results; this is done in Section 27.[7]

Again, let G be finite, and let D be a block of $\mathbb{Q}G$ which is a division ring. Let $\mathbb{Z}[G]$ be the image of $\mathbb{Z}G$ in D. Using Amitsur's classification of the finite groups that are embeddable in the multiplicative group of a division ring, we do in Sections 28 and 29 the following. Let $x \in \mathbb{Z}[G]$. If D is not a totally definite quaternion algebra, then x is either central in $\mathbb{Z}[G]$ or has infinitely many conjugates under the action of $\mathrm{U}(\mathbb{Z}G)$, and in the latter case, we construct units in $\mathrm{U}(\mathbb{Z}G)$ that can be used to produce infinitely many different conjugates. If D is a totally definite quaternion algebra, we give explicitly the group of units in $\mathbb{Z}[G]$ (which is of finite order over the center).

Chapter VIII

The odd analogue to Glauberman's famous Z^*-theorem can be formulated as follows: *If x is an element of prime order p in a finite group G which commutes with none of its other conjugates, then $[x, G] \leq \mathrm{O}_{p'}(G)$.* It is well known that this theorem follows for odd p easily from the classification of finite simple groups, but it would be useful and instructive to find a direct proof.

Note that our assumption on the group element x is that its class sum C_x is contained in $x + \mathrm{Tr}_1^{\langle x\rangle}(\mathbb{Z}G)$, where $\mathrm{Tr}_1^{\langle x\rangle}$ is the usual relative trace map.

Let χ be an irreducible character of G, let ω_χ be the central character associated to χ, and let $\rho : G \to \mathrm{Mat}_n(\mathcal{O})$ be a representation of G affording χ, where $\mathcal{O}$ is the ring

[5] It can hardly be seen from the final version [71] of [70] that we first made this (simple) observation.
[6] Thus the given proof of [70, Theorem 2.3] readily extents to a proof of [70, Corollary 4.3].
[7] One might incorrectly conclude from the remarks in [71, p. 95] that we found this proof by a careful analysis of [70].

of integers of some finite extension field of the p-adic field $\mathbb{Q}_p$ containing a primitive pth root of unity ζ. Then $\rho(x) + \mathrm{Tr}_1^{\langle\rho(x)\rangle}(M) = \omega_\chi(C_x) \cdot \mathrm{Id}_n$ for some $M \in \mathrm{Mat}_n(\mathcal{O})$. Note that $\omega_\chi(C_x) \in R = \mathbb{Z}_p[\zeta]$.

Now let $p = 3$, and let C_3 be a cyclic group of order 3. Dieterich has shown that RC_3 is of finite representation type, and that there are 9 isomorphism classes of indecomposable RC_3-lattices. From that, we easily derive (30.5): *If $X \in \mathrm{GL}_n(R)$ is of order 3, and if for some $M \in \mathrm{Mat}_n(R)$ and some $\omega \in R$, we have $X + \mathrm{Tr}_1^{\langle X\rangle}(M) \equiv \omega \cdot \mathrm{Id}_n \pmod{3R}$, then the trace of X is an integral multiple of a power of ζ.*

We cannot suppose that $\mathcal{O} = R$, but $\mathcal{O}$ is a free R-module of finite rank m. Thus we have an R-linear embedding $\mathrm{Mat}_n(\mathcal{O}) \hookrightarrow \mathrm{Mat}_{nm}(R)$, and we obtain (in the $p = 3$ case) that *$\chi(x)$ is an integral multiple of a power of ζ.*

Let e_0 be the central idempotent belonging to the principal block B_0 of $\mathbb{Z}_{(3)}G$. It is well known that e_0C_x is a unit in B_0. Robinson observed that if the irreducible characters of G belonging to B_0 satisfy the above condition, then $u_x = e_0C_x(e_0C_{x^{-1}})^{-1}$ is a central unit of order 3 in B_0, and if u_x is a trivial unit, i.e., if $u_x = e_0g$ for some $g \in G$, then $[x, G] \leq \mathrm{O}_{3'}(G)$.

The latter observation links the problem whether $[x, G] \leq \mathrm{O}_{3'}(G)$ is true or not with the "defect group conjugacy question" for the principal block (see [128, p. 267]): Even some modest progress towards a positive answer to this question would imply that u_x is a trivial unit (see [115]).

Acknowledgments

My sincerest appreciation goes to Prof. Kimmerle, both for permitting me to pursue this research at the Department of Mathematics and for being patient with me through the entire process.

I would like to mention that this work was supported by the Deutsche Forschungsgemeinschaft (DFG).

The computer programs GAP and Maple proved to be especially helpful to carry out part of this research. The paper is typeset in LaTeX using the package KOMA-Script.

In the end, I would like to say that I am sorry that the rules of the international scientific world have encouraged me to write this thesis in a language I'm not too familiar with. As a result, the style of this text is as far from actual English as a "monkey see, monkey do" calculation is from actual calculus.

I. On the isomorphism problem for integral group rings

Non vitae, sed scholae discimus.
Discamus igitur non scholae, sed vitae.

In this chapter, we describe some problems which occur naturally when dealing with the isomorphism problem for integral group rings of finite groups G, and try to give at least partial solutions. These problems concern local–global aspects in connection with a generalization of Mazur's observation from [92], as well as the local structure of the known counterexample [57].

The integral group ring of the group G is by definition the group ring $\mathbb{Z}G$. We will, however, follow Graham Higman, who, in his thesis, called $\mathcal{O}G$ an "integral group ring" whenever $\mathcal{O}$ is a ring of algebraic integers. The isomorphism problem then asks: Does an isomorphism $\mathcal{O}X \cong \mathcal{O}Y$ of integral group rings imply an isomorphism $X \cong Y$ of the underlying (finite) groups?

1. Local–global considerations

Given a finite group G, a *G-adapted ring* R is an integral domain of characteristic zero such that if G has an element of order p, then p is not invertible in R.

It is well known that RG, where R is a G-adapted ring, has some specific properties. Among them, we mention that a nontrivial unit of finite order in RG has vanishing 1-coefficient; that RG has only trivial idempotents; that there is a class sum and a normal subgroup correspondence for group bases of RG available. For details, we refer the reader to [130] and [76, Chapters 2 and 3].

A basic example of a G-adapted ring is $R = \mathbb{Z}_\pi$, the intersection of the localizations $\mathbb{Z}_{(p)}$ with p ranging over a finite set π of primes which contains the set $\pi(G)$ of prime divisors of $|G|$. (Note that $\mathbb{Z}_\pi G$ is a semilocal ring.) Later on, we will see that it is more convenient to perform calculations in RG rather than in $\mathbb{Z}G$.

We could also call $\mathbb{Z}_{\pi(G)}G$ an integral group ring. With respect to the integral isomorphism problem, this is justified by the following proposition.

1.1 Proposition. *Let G and H be finite groups, and set $\pi = \pi(G)$. Then $\mathbb{Z}_\pi G \cong \mathbb{Z}_\pi H$ implies that $\mathcal{O}G \cong \mathcal{O}H$ for some ring $\mathcal{O}$ of algebraic integers.*

Proof. We may assume that $\mathbb{Z}_\pi G = \mathbb{Z}_\pi H$. Then $V = \mathbb{Z}G$ and $W = \mathbb{Z}H \cdot \mathbb{Z}G$ (the set of finite sums $\sum a_i b_i$ with $a_i \in \mathbb{Z}H$, $b_i \in \mathbb{Z}G$) are right $\mathbb{Z}G$-lattices (the action given by right multiplication). As $V \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathbb{Z}_p G = W \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for all $p \in \pi(G)$, the modules V and W lie in the same genus. By [68, Satz 7], there is a ring $\mathcal{O}$ of algebraic integers such that $\mathcal{O}G = V \otimes_{\mathbb{Z}} \mathcal{O}$ and $M := W \otimes_{\mathbb{Z}} \mathcal{O}$ are isomorphic as $\mathcal{O}G$-lattices; let $m_1 \in M$ be the image of $1 \in \mathcal{O}G$ under such an isomorphism $\mathcal{O}G \to M$. Note that M is contained in the algebra $\mathbb{Q}G \otimes_{\mathbb{Z}} \mathcal{O}$, that the operation of $\mathcal{O}G$ on M is just given by right multiplication, and that $\mathcal{O}H \cdot M \subseteq M$. Now for any $y \in \mathcal{O}H \subseteq M$, there is a unique $x_y \in \mathcal{O}G$ such that $ym_1 = m_1 x_y$. It follows that the map $\mathcal{O}H \to \mathcal{O}G$, defined by $y \mapsto x_y$, is an isomorphism of rings. (The map is clearly an isomorphism of abelian groups, and for $y, y' \in \mathcal{O}H$ we have $(yy')m_1 = y(y'm_1) = y(m_1 x_{y'}) = (ym_1)x_{y'} = (m_1 x_y)x_{y'} = m_1(x_y x_{y'})$, so $x_{yy'} = x_y x_{y'}$.) □

In this context, we may ask:

1.2 Problem.
1. Does the converse hold, i.e., does $\mathcal{O}G \cong \mathcal{O}H$ (for some ring $\mathcal{O}$ of algebraic integers) imply that $\mathbb{Z}_\pi G \cong \mathbb{Z}_\pi H$?
2. Let $\mathcal{O}$ be a ring of algebraic integers. If ϕ is an automorphism of $\mathcal{O}G$, is there an automorphism ψ of $\mathbb{Z}_\pi G$, agreeing with ϕ on $\mathbb{C}G$ up to an inner automorphism?
3. If ϕ is an automorphism of $\mathbb{Z}_\pi G$, is there an automorphism ψ of $\mathbb{Z}G$, agreeing with ϕ on $\mathbb{Q}G$ up to an inner automorphism?
4. If $\mathbb{Z}_\pi G \cong \mathbb{Z}_\pi H$, does it follow that $\mathbb{Z}G \cong \mathbb{Z}H$?

We could not answer the first two questions.

We will show in Section 12 that in general, Problem 1.2(3) has a negative answer. Nevertheless, it might be interesting to note that a positive answer to Problem 1.2(3) would have given a positive answer to Problem 1.2(4), by Kimmerle's $G \times G$-trick (see [81, Lemma 5.3]), which reduces questions about isomorphisms to questions about automorphisms. Briefly, the argument goes as follows: An isomorphism $\mathbb{Z}_\pi G \cong \mathbb{Z}_\pi H$ induces an automorphism ϕ of $\mathbb{Z}_\pi(G \times H)$ mapping $\mathbb{Z}_\pi G$ to $\mathbb{Z}_\pi H$ and conversely, and if ψ is an automorphism of $\mathbb{Z}(G \times H)$ agreeing with ϕ on $\mathbb{Q}G$ up to an inner automorphism, then ϕ maps the induced augmentation ideal of H onto the induced augmentation ideal of G, thus inducing an isomorphism $\mathbb{Z}G \cong \mathbb{Z}H$.

The next proposition is well known, and puts Problem 1.2(4) in another context. (If the module categories are equivalent, are the group rings isomorphic?) One direction is Corollary 1.2.6 from [119], where the converse is stated without proof on p. 609. For the readers convenience, we include a complete proof.

1.3 Proposition. *Let G, H be finite groups and set $\pi = \pi(G)$. Then $\mathbb{Z}_\pi G \cong \mathbb{Z}_\pi H$ if and only if the category of $\mathbb{Z}G$-modules is equivalent to that of $\mathbb{Z}H$-modules.*

Proof. Any equivalence of the module categories (as exhibited by an invertible bimodule) produces a corresponding equivalence over the enlarged ring $\mathbb{Z}_\pi$, and such an equivalence implies, by Swan's theorem, that $\mathbb{Z}_\pi G \cong \mathbb{Z}_\pi H$ (see [119, Corollary 1.2.6]).

Conversely, assume that $\mathbb{Z}_\pi G = \mathbb{Z}_\pi H$. Set $M = \mathbb{Z}G$, and consider $V := \mathbb{Q}M = \mathbb{Q}G$ as $(\mathbb{Q}G, \mathbb{Q}H)$-bimodule, the action of G and H given, respectively, by left and right multiplication. We will show that the restricted module $V|_{(\mathbb{Z}G,\mathbb{Z}H)}$ contains an invertible bimodule N (and then $-\otimes_{\mathbb{Z}G} N$ provides an equivalence of the categories of $\mathbb{Z}G$- and $\mathbb{Z}H$-modules). We will construct, for each prime p, an invertible $(\mathbb{Z}_{(p)}G, \mathbb{Z}_{(p)}H)$-bimodule $X(p)$ inside $V|_{(\mathbb{Z}_{(p)}G,\mathbb{Z}_{(p)}H)}$ such that $X(p) = M_{(p)} = \mathbb{Z}_{(p)}G$ almost everywhere. Then it follows from [106, (4.22)] that $N := \bigcap_p X(p)$ is a full $\mathbb{Z}$-lattice in $\mathbb{Q}G$, and $N_{(p)} = X(p)$ for all primes p. Thus N will be an invertible $(\mathbb{Z}G, \mathbb{Z}H)$-bimodule since invertibility is a "local" property (see [28, (35.4)]).

Let the set ω consist of those primes p such that $\mathbb{Z}G \nsubseteq \mathbb{Z}_{(p)}H$ or $\mathbb{Z}H \nsubseteq \mathbb{Z}_{(p)}G$ holds; note that ω is a finite set. Let p be a prime. If $p \notin \omega$, then $\mathbb{Z}_{(p)}G = \mathbb{Z}_{(p)}H$ and we set $X(p) = \mathbb{Z}_{(p)}G$. If $p \in \omega$, we necessarily have $p \notin \pi(G) = \pi(H)$, so $\mathbb{Z}_{(p)}G$ and $\mathbb{Z}_{(p)}H$ are maximal orders in $\mathbb{Q}G$, and are therefore conjugate: $u_p^{-1}(\mathbb{Z}_{(p)}G)u_p = \mathbb{Z}_{(p)}H$ for some unit u_p of $\mathbb{Q}G$ (see [106, (41.1), (10.5), (18.7)]). Then $X(p) := (\mathbb{Z}_{(p)}G)u_p$ is a submodule of $V|_{(\mathbb{Z}_{(p)}G,\mathbb{Z}_{(p)}H)}$, which is invertible since $X(p) \cong \mathbb{Z}_{(p)}G$ as left $\mathbb{Z}_{(p)}G$-modules and $\mathrm{End}_{\mathbb{Z}_{(p)}G}(X(p)) \cong u_p^{-1}(\mathbb{Z}_{(p)}G)u_p = \mathbb{Z}_{(p)}H$. □

Scott [127, Section 2] found a way to approach the construction of group ring automorphisms and isomorphisms in the semilocal case that avoids any explicit use of the theory of orders, though integral representation theory and Fröhlich's theory [36] are still important in the background.

A basic observation, already noted in [117], is given in the next proposition. We include a proof of it since the reader may wish to recall the construction when reading Chapter III. We shall use some standard results concerning the interpretation of automorphisms as invertible bimodules (which can be found in [106, Section 37], [27, § 55A] or [119, Section 1]).

Let R be a Dedekind ring with quotient field K of characteristic 0. Let P range over the prime ideals of R, and let R_P denote localization at P. By a semilocalization at a finite set π of primes in R, we just mean the intersection R_π of the localizations of R at the primes in π. (Note that R_π is a semilocal Dedekind ring, that is, a Dedekind ring with only a finite number of maximal ideals.)

1.4 Proposition. *Assume that there are given automorphisms α_P of R_PG which agree on KG up to central automorphisms. Then there is an invertible (RG, RG)-bimodule M such that for any semilocalization R_π, we have $R_\pi \otimes_R M \cong {}_1(R_\pi G)_{\alpha_\pi}$ for some automorphism $\alpha_\pi \in \mathrm{Aut}(R_\pi G)$ which differs on R_PG from α_P only by an inner automorphism, for all $P \in \pi$. The bimodule M is of the form $M = (RG)\nu$ for some idele ν of KG.*

Proof. Fix some prime ideal P_0 of R and let α be the automorphism α_{P_0} induces on KG. By the Skolem–Noether theorem, there are units ν_P of KG such that $\alpha_P^{-1}\alpha = \mathrm{conj}(\nu_P)$ for all P. Moreover, the ν_P's can be chosen such that $\nu_P \in (R_PG)^\times$ for all but a finite number of P's (see Proposition 5.2). Then $\nu = (\nu_P)$ is an idele of KG (relative to R), and $M = (RG)\nu := \bigcap_P R_PG{\cdot}\nu_P$ is a full R-lattice in KG with $M_P = R_PG{\cdot}\nu_P$ for each P (see [106, (4.22)]). Each $R_PG{\cdot}\nu_P$ can be viewed as a submodule of the (R_PG, R_PG)-bimodule ${}_1(KG)_\alpha$. Then $M \leq {}_1(KG)_\alpha$ as (RG, RG)-bimodules, and $M_P = R_PG{\cdot}\nu_P \cong {}_1(R_PG)_{\alpha_P}$. The bimodule M is invertible since invertibility is a "local" property (see [28, (35.4)]).

Note that $R_\pi \otimes_R M$ as $R_\pi G$-module is free from one side since this holds locally (see [106, Exercise 18.3]). Thus $R_\pi \otimes_R M \cong {}_1(R_\pi G)_{\alpha_\pi}$ for some automorphism $\alpha_\pi \in \mathrm{Aut}(R_\pi G)$, and localizing further shows that α_π differs on R_PG from α_P only by an inner automorphism, for all $P \in \pi$. □

Thus automorphisms of semilocal group rings can be specified 'a prime at a time', as described in [119, (1.2.9)]:

1.5 Proposition. *Let R be a semilocal Dedekind ring. Assume that there are given automorphisms α_P of R_PG which agree on KG up to central automorphisms. Then there is an automorphism of RG which agrees with each α_P up to an inner automorphism of R_PG.* □

Now let G and H be finite groups, and let R be a semilocal Dedekind ring. If given local *isomorphisms* $R_PG \to R_PH$ fit together rationally, that is, if each two agree on KG up to a central automorphism, then there is an isomorphism $RG \to RH$ which differs from each local isomorphism only by an inner automorphism.

This result can be obtained by making some minor modifications in the proof of Proposition 1.4. We will, however, take the opportunity to show how it can be derived from Proposition 1.4 using Kimmerle's $G \times G$-trick.

1.6 Proposition. *Let R be a semilocal Dedekind ring. For each prime ideal P of R, let $\beta_P : R_PG \longrightarrow R_PH$ be an augmentation-preserving ring isomorphism. Each β_P induces an isomorphism $\hat\beta_P : KG \to KH$. Assume that the automorphisms $\hat\beta_P \cdot \hat\beta_Q^{-1}$ of KG are inner automorphisms, for all prime ideals P, Q of R. Then there is an isomorphism $\beta : RG \to RH$ such that $\beta \cdot \beta_P^{-1}$ induces an inner automorphism of R_PG for all P.*

Proof. Note that for any coefficient ring S, we may identify $S(G \times H)$ with $SG \otimes_S SH$.

For each P, let $\alpha_P : R_P(G \times H) \to R_P(G \times H)$ be the "flip" induced by β_P, i.e., $(x \otimes y)\alpha_P = y\beta_P^{-1} \otimes x\beta_P$ for all $x \in R_PG$, $y \in R_PH$. Note that α_P has order 2, and that $(x \otimes y)\hat\alpha_P\hat\alpha_Q = x\hat\beta_P\hat\beta_Q^{-1} \otimes y\hat\beta_P^{-1}\hat\beta_Q$ for all P, Q and $x \in KG$, $y \in KH$. It follows from Proposition 1.5 that there is an automorphism $\alpha : R(G \times H) \to R(G \times H)$ agreeing with each α_P up to an inner automorphism of $R_P(G \times H)$. In particular, α maps the trace of H (the sum of the elements of H) to the trace of G. The annihilators of these elements

are the induced augmentation ideals $I_H = \mathrm{I}(H)(G\times H)$ and $I_G = \mathrm{I}(G)(G\times H)$, so α maps I_H onto I_G and induces an isomorphism $\beta : RG \cong R(G\times H)/I_H \to R(G\times H)/I_G \cong RH$, and it is easy to see that β has the desired property. □

Dade [30] constructed non-isomorphic finite groups G, H with isomorphic group rings over each field. It is also true that $\mathbb{Z}_{(p)}G \cong \mathbb{Z}_{(p)}H$ for these groups, for all primes p. However, such isomorphisms do not fit together rationally.

Based on the known counterexample [57], we give an example (in Section 3) where local isomorphisms fit together rationally. We do not know, however, whether the integral group rings are isomorphic.

2. Mazur's construction adapted to finite groups

A finite group G is embedded in the group $\mathrm{U}(\mathbb{Z}G)$ of units of its integral group ring $\mathbb{Z}G$, and the normalizer $\mathrm{N}_{\mathrm{U}(\mathbb{Z}G)}(G)$ of G therein has been the subject of much research in recent years [66, 122, 91, 54, 61, 58, 57, 72]. Its study includes the study of the center $\mathrm{Z}(\mathrm{U}(\mathbb{Z}G))$, which is already a very difficult and broad subject. Moreover, there is an apparently "small" quotient of the normalizer, naturally isomorphic to a certain subgroup of the outer automorphism group $\mathrm{Out}(G)$, which measures the extent to which there are "non-obvious" units normalizing G. (In Chapter V, this quotient will be studied in some detail for infinite groups G.)

To be more precise, we denote by $\mathrm{Aut}_{\mathbb{Z}}(G)$ the group of automorphisms of G which induce inner automorphisms of $\mathbb{Z}G$. Then the quotient under consideration is $\mathrm{Out}_{\mathbb{Z}}(G) = \mathrm{Aut}_{\mathbb{Z}}(G)/\mathrm{Inn}(G)$ — note that $\mathrm{Out}_{\mathbb{Z}}(G) \cong \mathrm{N}_{\mathrm{U}(\mathbb{Z}G)}(G)/G \cdot \mathrm{Z}(\mathrm{U}(\mathbb{Z}G))$. Interest in that group arose from the fact that a finite group G with $\mathrm{Out}_{\mathbb{Z}}(G) \neq 1$ gives rise to non-isomorphic (infinite polycyclic) groups $X = G \times \mathbb{Z}$ and Y with $\mathbb{Z}X \cong \mathbb{Z}Y$. This observation of Mazur [92] has been refined in [54, 57], where in addition it was shown that there are actually finite groups G with $\mathrm{Out}_{\mathbb{Z}}(G) \neq 1$. We will discuss this concept in more detail, including local–global aspects.

Multiplicative 1-cocycles

Let R be a commutative ring and Λ an R-order on which a finite group H acts via an R-algebra homomorphism $\iota : RH \to \Lambda$ (i.e., $\lambda^h = \lambda^{h\iota}$ for all $h \in H$). A *multiplicative 1-cocycle on H with values in Λ* is a map $\mu : H \to \Lambda$ satisfying $\mu(gh) = \mu(g)^h \cdot \mu(h)$ for all $g, h \in H$. Such a μ is called a *1-coboundary* provided there exists a unit $u \in \Lambda^\times$ such that $\mu(h) = u^{-h} \cdot u$ for all $h \in H$.

For any automorphism $\gamma \in \mathrm{Aut}(G)$, and $u \in RG$, we define the *norm* $\mathsf{N}_\gamma(u)$ of u with respect to γ by

$$\mathsf{N}_\gamma(u) := u\gamma^{n-1} \cdot \ldots \cdot u\gamma \cdot u, \quad \text{where } n \text{ is the order of } \gamma.$$

If $\mathsf{N}_\gamma(u) = 1$, then $\mu(\gamma) = u$ defines a (multiplicative) 1-cocycle $\mu : \langle\gamma\rangle \to RG$ (and conversely). Note that if $\mathsf{N}_\gamma(u)$ is a unit of finite order, there is a cyclic group $\langle c\rangle$ of finite order, acting via γ on RG (i.e., $x^c = x\gamma$ for all $x \in RG$), such that $\mu(c) = u$ defines a 1-cocycle $\mu : \langle c\rangle \to RG$.

For the rest of this section, let R denote a G-adapted ring. We are interested in cocycles $\langle c\rangle \to RG$ with values in $\mathrm{N}_{\mathrm{U}(RG)}(G)$.

2.1 Problem. Give examples of triples (G, u, γ), where G is a finite group, the unit $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ induces a non-inner automorphism $\alpha = \mathrm{conj}(u)$ of G of order m (say), and $\gamma \in \mathrm{Aut}(G)$ such that one of the following holds.

(P1) $\mathsf{N}_\gamma(u)$ is of finite order.

(P2) $\mathsf{N}_\gamma(u)$ is of finite order, and $\bar\gamma$ and $\bar\alpha\bar\gamma$ are not conjugate in $\mathrm{Out}(G)$.

(P3) $\mathsf{N}_\gamma(u^m)$ is of finite order.

2.2 Remark.

1. (P1), and in particular (P2), are very difficult problems. If (P2) is solved, it is possible to construct non-isomorphic groups X and Y with isomorphic group rings, $RX \cong RY$ (cf. [54, Proposition 5.6.1], and Proposition 2.3 below). If G and γ have odd order, the groups X and Y may be chosen to have odd order, too.
2. Problem (P2) is solved with G of even order in [54, 57].
3. Problem (P3) seems to be more accessible. At least we do know how cocycles with values in the central units look like (some simple examples are given below).
4. A connection between (P1) and (P3) is as follows. Assume that (P3) is solved, and that the $u\gamma^i$, $i \in \mathbb{N}$, commute pairwise (this happens, for example, when γ normalizes $\langle\alpha\rangle$). Then $\mathsf{N}_\gamma(u)$ has finite order and (P1) is solved. However, note that if γ acts coprime on $\langle\alpha\rangle$, we will *not* get a solution of (P2) in that way.
5. Given G, and $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ inducing a non-inner automorphism $\alpha = \mathrm{conj}(u)$ of G of order m, the central unit u^m may be calculated in the form c^m for some central unit c of KG, where K is some field containing R. The question, then, is whether there exists a central unit z of RG and $\gamma \in \mathrm{Aut}(G)$ so that $\mathsf{N}_\gamma(cz)$ is of finite order and γ acts on $\langle\alpha\rangle$ (for then we could replace u by uz, thus giving a solution of (P1)). This might turn out to be a practicable approach.

The next result is Mazur's observation [92] adapted to finite groups.

2.3 Proposition. *Let G be a finite group, $\gamma \in \mathrm{Aut}(G)$ and $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ such that $\mathsf{N}_\gamma(u)$ is of finite order. Set $\alpha = \mathrm{conj}(u) \in \mathrm{Aut}(G)$ and assume further that $\bar\gamma$ and $\bar\alpha\bar\gamma$ are not conjugate in $\mathrm{Out}(G)$. Then there are non-isomorphic groups X and Y such that $RX \cong RY$, and these groups are semidirect products $(G \times C_r) \rtimes C_n$, where n is the product of the orders of γ and $\mathsf{N}_\gamma(u)$, and r is a prime with $(r, n|G|) = 1$ such that C_n acts faithfully on C_r.*

Proof. To begin with, note that for any group K, $\kappa \in \mathrm{Aut}(K)$ of order r, and a cyclic group $\langle x \rangle$ whose order is divisible by r, we may define the semidirect product $S = K \rtimes \langle x \rangle$ with x acting via κ, i.e., $k^x = k\kappa$ for all $k \in K$. In this case, we also write $S = K \rtimes_\kappa \langle x \rangle$.

Let n be the product of the orders of γ and $\mathsf{N}_\gamma(u)$. If m denotes the order of γ, then $(\gamma\alpha)^m = \mathrm{conj}(\mathsf{N}_\gamma(u))$, so $\gamma^n = \mathrm{id}$ and $(\gamma\alpha)^n = \mathrm{id}$. Let $\langle c \rangle$ be a cyclic group of order n. Choose a cyclic group A of prime order r with $(r, n|G|) = 1$ such that n divides $r-1$ (what can be done by a special case of Dirichlet's theorem on primes in arithmetic progressions), and let $\langle \mu \rangle$ be an automorphism of A of order n. The groups X and Y are given as

$$X = (G \times A) \rtimes_{(\gamma \times \mu)} \langle c \rangle \quad \text{and} \quad Y = (G \times A) \rtimes_{(\gamma\alpha \times \mu)} \langle c \rangle.$$

Assume that $X \cong Y$, and fix an isomorphism $\phi : X \to Y$. Clearly $A\phi = A$, as A is a normal Hall subgroup of X and Y. It follows that $(GA)\phi = \mathrm{C}_X(A)\phi = \mathrm{C}_Y(A) = GA$, so $G\phi = G$. Note that the assumption on A and μ implies that there are $x \in G$ and $a \in A$ such that $c\phi = xac$. Thus for all $g \in G$,

$$g(\gamma \cdot \phi) = (g^c)\phi = (g\phi)^{(c\phi)} = (g\phi \cdot \mathrm{conj}(x))^c = g(\phi \cdot \mathrm{conj}(x) \cdot \alpha \cdot \gamma),$$

so $\phi|_G^{-1} \cdot \gamma \cdot \phi|_G = \mathrm{conj}(x) \cdot \alpha \cdot \gamma$, contradicting the assumption that $\bar\gamma$ and $\bar\alpha\bar\gamma$ are not conjugate in $\mathrm{Out}(G)$. Hence X and Y are non-isomorphic.

Note that $(cu)^m = c^m \mathsf{N}_\gamma(u)$ in RX (where m is the order of γ), so $cu \in RX$ has order n, and it is easy to see that the subgroup $U := \langle G, M, cu \rangle$ of $\mathrm{U}(RX)$ is isomorphic to Y, and that $RU = RX$. This proves $RX \cong RY$. □

2.4 Remark.

1. It should be evident that in the previous proof, the subgroup A of X is introduced only for "technical reasons". Instead, one could also increase the order of c to ensure that an isomorphism $X \to Y$ (if there is any) fixes G. Proceeding this way would be more closely to Mazur's construction for infinite groups.
2. It appears to be difficult to verify the non-conjugacy of $\bar\gamma$ and $\bar\alpha\bar\gamma$ in a concrete situation. To prove that X and Y are non-isomorphic it is probably better to use an obstruction theory as outlined in [80].
3. The obstruction theory just mentioned also gives information about how the group X should look like. As an example, assume that $X = Q \rtimes P$ is a semidirect product of a normal Sylow q-subgroup Q and a Sylow p-subgroup P. Let $R = \mathbb{Z}_{\pi(X)}$ and $RX = RY$. It is known that the images of X and Y in RP and in $RX/\mathrm{O}_p(X)$ are conjugate by rational units u and v, respectively, which gives rise to a class-preserving automorphism $\delta := \mathrm{conj}(\bar u \bar v^{-1}) \in \mathrm{Aut}(P/\mathrm{O}_p(X))$. The groups X and Y are isomorphic if and only if δ can be written as the product of two automorphisms, one induced from an automorphism of RP, the other induced from an automorphism of $RX/\mathrm{O}_p(X)$. In particular, if $\mathrm{Out}_\mathrm{c}(P/\mathrm{O}_p(X)) = 1$, then $X \cong Y$.

Cocycles with values in the central units

We give some examples of cocycles with values in commutative group rings. The first example was used to construct the counterexample to the isomorphism problem for integral group rings.

2.5 Example. (Cf. [57, Section 4].) Let $G = \langle w \rangle$ be a cyclic group of order 8, and let γ be the automorphism of G of order 2 defined by $w\gamma = w^5$. Then for the unit

$$\nu = \frac{1+w^4}{2} + \frac{1-w^4}{2}\big(3 + 2\big(w + w^{-1}\big)\big) \in \mathrm{U}(\mathbb{Z}G),$$

we have $\mathsf{N}_\gamma(\nu) = 1$, which simply means that γ inverts ν. For each $n \geq 2$, there are prime powers p^a and r^b so that $\nu^n \equiv 1 \mod p^a$ and $\nu^n \equiv w^4 \mod r^b$. For some values of n, these prime powers are listed in the following table.

n	2	3	4	5	6	7	8	...	24
p^a	2	7	$2^2, 3$	41	$2, 5, 7$	239	$2^3, 3, 17$	...	$2^3, 3^2, 5, 7, 11, 17, 1153$
r^b	3	5	17	29	$3^2, 11$	13^2	577	...	$97, 577, 13729$

We remark that the prime 97 is the smallest prime r such that there is $n \in \mathbb{N}$ with $\nu^n \equiv 1 \mod 8$ and $\nu^n \equiv w^4 \mod r$, and that this is the reason why the groups given in [57, Theorem B] have order divisible by 97.

Next, we present an example where G and γ are of odd order. We shall write $\epsilon_G = \frac{1}{|G|}\sum_{g\in G} g$ for the trivial idempotent and $\eta_G = 1 - \epsilon_G$.

2.6 Example. Let $G = \langle x \rangle$ be a cyclic group of order 7, and let γ be the automorphism of G of order 3 defined by $x\gamma = x^2$. Let ζ be a primitive 7th root of unity. Then $a = -1 - \zeta - \zeta^6$ is a unit in $\mathbb{Z}[\zeta]$ with $a^{21} \equiv 1 \mod 7$. Hence

$$\begin{aligned} u &= \epsilon_G + \eta_G(-1 - x - x^6)^{21} \\ &= -6910567 - 4308668(x + x^6) + 1537746(x^2 + x^5) + 6226206(x^3 + x^4) \end{aligned}$$

is a unit in $\mathbb{Z}G$ with $\mathsf{N}_\gamma(u) = 1$.

Given any abelian group G of odd order, and distinct primes p and r, a unit u of $\mathbb{Z}G$ cannot satisfy simultaneously the congruences $u \equiv 1 \mod p$ and $u \equiv g \mod r$ for some $1 \neq g \in G$. (This follows from Proposition 19.2; the same might be true for arbitrary G of odd order.) This is the reason why in the next examples, the coefficient ring is $\mathbb{Z}_{\pi(G)}$.

2.7 Remark. Let $\langle x \rangle$ be a cyclic group of order n, and let $a, b \in \mathbb{Z}$ with $(a, b) = 1$. Then $u := -a + bx$ is a unit in $\mathbb{Z}_{\pi(ab)}\langle x \rangle$ (where $\pi(ab)$ denotes the set of prime divisors of ab), with inverse

$$u^{-1} = \frac{1}{-a^n + b^n} \sum_{i=0}^{n-1} a^i b^{n-1-i} x^i.$$

2.8 Example. Keep the notation from Example 2.6. Let $u = 7x^5 - 6$. Then $u \equiv 1 \mod 7$ and $u \equiv x^5 \mod 3$. It follows that u is a unit in $\mathbb{Z}_{\{3,7\}}G$. Hence

$$v = \epsilon_G + \eta_G \mathsf{N}_\gamma(u^{-1})u^3$$

is a unit in $\mathbb{Z}_{\{3,7\}}G$ with $\mathsf{N}_\gamma(v) = 1$. Explicitly, we have

$$\begin{aligned} v = \frac{1}{543607}(&-82368 + 103831x + 559482x^2 - 106680x^3 \\ &- 522144x^4 + 101346x^5 + 490140x^6) \\ v^{-1} = \frac{1}{543607^2}(&-88071245394 + 350666925924x - 308485501128x^2 \\ &+ 275342849922x^3 - 247018545396x^4 \\ &+ 214383470616x^5 + 98690615905x^6). \end{aligned}$$

Note that $\mathsf{N}_\gamma(x) = 1$. It follows that $v \equiv x \mod 3$ and $v \equiv 1 \mod 7$.

In the final example, the action of γ on G is not coprime (cf. Remark 2.2(4)).

2.9 Example. Let $G = \langle x, y : x^9 = y^3 = [x, y] = 1\rangle \cong C_9 \times C_3$, and let γ be the automorphism of G of order 3 defined by $x\gamma = xy$ and $y\gamma = yx^6$. Then $\mathsf{N}_\gamma(x) = 1$. Let $u = -5x + 6$. Then $u \equiv 1 \mod 5$ and $u \equiv x \mod 3$. It follows that u is a unit in $\mathbb{Z}_{\{3,5\}}G$. Set $v = \mathsf{N}_\gamma(u^{-1}) \cdot u^3$. By construction, $\mathsf{N}_\gamma(v) = 1$. We have $v \equiv x^3 \mod 3$, and $v \equiv \mathsf{N}_\gamma(x^{-1})\mathsf{N}_\gamma(u^3) \equiv 1 \mod 5$.

Local–global aspect

Let G be a finite group, and let R be a semilocal Dedekind ring with quotient field K of characteristic 0. Assume that there are $\alpha, \gamma \in \mathrm{Aut}(G)$ such that for each prime ideal P of R, there is a local unit $u_P \in \mathrm{U}(R_PG)$ such that $\alpha = \mathrm{conj}(u_P)$, and $\mathsf{N}_\gamma(u_P)$ is of finite order. Let L be the collection of the u_P's.

Let $\langle c\rangle$ be a cyclic group whose order is divisible by the product of the orders of γ and the $\mathsf{N}_\gamma(u_P)$'s, and let c act on KG via γ. Then there are 1-cocycles $\delta_{P,Q} : \langle c\rangle \to \mathrm{Z}(KG)$, defined by $\delta_{P,Q}(c) = u_Q^{-1}u_P$, for all prime ideals P, Q.

This is easy to see, but we will demonstrate it anyway. Set $v = u_P$, $w = u_Q$, and write x^γ instead of $x\gamma$. If m denotes the order of γ, then using the centrality of $\delta_{P,Q}(c)$,

$$\begin{aligned} \delta_{P,Q}(c^m) &= w^{-\gamma^{m-1}}v^{\gamma^{m-1}} \cdots w^{-\gamma^2}v^{\gamma^2}(w^{-\gamma}v^\gamma)w^{-1}v \\ &= w^{-\gamma^{m-1}}v^{\gamma^{m-1}} \cdots (w^{-\gamma^2}v^{\gamma^2})w^{-1}w^{-\gamma}v^\gamma v \\ &= w^{-\gamma^{m-1}}v^{\gamma^{m-1}} \cdots w^{-1}w^{-\gamma}w^{-\gamma^2}v^{\gamma^2}v^\gamma v \end{aligned}$$

$$\begin{aligned}&\vdots\\ &= \mathsf{N}_\gamma(w)^{-1}\mathsf{N}_\gamma(v).\end{aligned}$$

We have $\mathrm{conj}(\mathsf{N}_\gamma(v)) = (\gamma\alpha)^m = \mathrm{conj}(\mathsf{N}_\gamma(w))$, so the elements $\mathsf{N}_\gamma(v)$ and $\mathsf{N}_\gamma(w)$ commute. Let n be the product of their orders. Since c^m acts trivial on KG, it follows that $\delta_{P,Q}(c^{mn}) = \mathsf{N}_\gamma(w)^{-n}\mathsf{N}_\gamma(v)^n = 1$.

If the 1-cocycles $\delta_{P,Q}$ are all 1-coboundaries, we will call (γ, L) a *local system of 1-cocycles.*

2.10 Proposition. *With notation as above, assume that $\bar\gamma$ and $\bar\alpha\bar\gamma$ are not conjugate in* $\mathrm{Out}(G)$*, and that (γ, L) is a local system of* 1*-cocycles. Then there are non-isomorphic groups X and Y involving G, as described in Proposition 2.3, such that $RX \cong RY$.*

Proof. Define groups X and Y as in Proposition 2.3; again there are isomorphisms $\phi(P) : R_PX \to R_PY$, defined by $x\phi(P) = x$ for all $x \in G\times A$ and $c\phi(P) = cu_P$. By assumption, there are $z(P,Q) \in \mathrm{Z}(KG)$ such that $\delta_{P,Q}(c) = z(P,Q)^{-c}z(P,Q)$ for all P, Q. Therefore $\phi(P)\cdot\phi(Q)^{-1}$, considered as automorphism of KX, maps c to $c\cdot\delta_{P,Q}(c) = c^{z(P,Q)}$, i.e., is given by conjugation with the unit $z(P,Q)$. Hence $RX \cong RY$ by Proposition 1.6. □

3. Semilocal analysis of the counterexample

In [57], two non-isomorphic groups X and Y, both of order $2^{21}\cdot 97^{28}$, have been constructed which have isomorphic integral group rings, $\mathbb{Z}X = \mathbb{Z}Y$. Having these groups at hand, we pursue the way prescribed by Proposition 1.6 to show that the group rings are semilocally isomorphic. This leads to new insight into the structure of these groups.

Actually, this allows us to make a small modification: We will replace the Sylow 97-subgroup by a Sylow 17-subgroup, without changing the structure of the groups.

3.1 Theorem. *There are non-isomorphic groups X and Y of order $2^{20}\cdot 17^{28}$ which have isomorphic semilocal group rings, $\mathbb{Z}_\pi X \cong \mathbb{Z}_\pi Y$, where $\pi = \{2, 17\}$.*

The proof will occupy the rest of this section.

The group X

The group X is a semidirect product $X = Q \rtimes P$, where Q is a normal Sylow 17-subgroup and P is a Sylow 2-subgroup of X, precisely

$$P = (\langle u : u^{32}\rangle \times \langle v : v^4\rangle \times \langle w : w^8\rangle) \rtimes (\langle a : a^{64}\rangle \times \langle b : b^2\rangle \times \langle c : c^8\rangle),$$

with the action of a given by

$$u^a = u, \quad v^a = u^{16}v \quad \text{and} \quad w^a = u^4w,$$

and $x^b = x^{-1}$, $x^c = x^5$ for all $x \in \langle u, v, w\rangle$. (Compared with the counterexample [57, Theorem B], only the order of a has changed.)

The normal Sylow 17-subgroup Q of X and the action of P on Q is defined in total analogy to the counterexample [57, Theorem B], but anyway, we will repeat it.

The group Q is the direct product of normal subgroups N and M of X, defined as follows. Let $D = (\langle d_3\rangle \times \langle d_2\rangle) \rtimes \langle d_1\rangle \cong C_{17}^{(2)} \rtimes C_{17}$ with $d_2^{d_1} = d_3 d_2$ and $[d_3, d_1] = 1$, and let $R = D^{(2)}$ (the direct product of two copies of D). Then $N = R^{(4)}$. The group M is the additive group of the finite field $\mathbb{F}_{17^4}$.

The largest normal 2-subgroup of X is $\mathrm{O}_2(X) = \mathrm{C}_P(Q) = \langle u, v, c^2\rangle$. We have

$$\bar{P} = P/\mathrm{C}_P(Q) = \langle \bar{a}\rangle \times \langle \bar{w}, \bar{b}, \bar{c}\rangle = \langle \bar{a}\rangle \times \underbrace{C_8 \rtimes (C_2 \times C_2)}_{\text{Wall's Group (1947)}}.$$

The subgroup $\langle w, b, c\rangle$ of P centralizes M, and a operates on M via multiplication with a (fixed) primitive 64th root of unity of $\mathbb{F}_{17^4}$.

An automorphism $\delta \in \mathrm{Aut}(D)$ is given by

$$\delta : \begin{cases} d_1 \mapsto d_2^3 \\ d_2 \mapsto d_1 \\ d_3 \mapsto d_3^{-3} \end{cases}.$$

From $3^8 \equiv -1 \mod 17$ it follows that

$$\delta^8 : \begin{cases} d_1 \mapsto d_1^{3^4} \\ d_2 \mapsto d_2^{3^4} \\ d_3 \mapsto d_3^{-1} \end{cases} \quad \text{and} \quad \delta^{16} : \begin{cases} d_1 \mapsto d_1^{-1} \\ d_2 \mapsto d_2^{-1} \\ d_3 \mapsto d_3 \end{cases},$$

so δ has order 32, and an automorphism $\rho \in \mathrm{Aut}(R)$ of order 64 is defined by $(x, y)\rho = (y, x\delta)$ for all $x, y \in D$.

The operation of P on N is defined by

$$\begin{aligned} (r_1, r_2, r_3, r_4)^a &= (r_1\rho, r_2\rho, r_3\rho, r_4\rho), \\ (r_1, r_2, r_3, r_4)^w &= (r_4\rho^{64}, r_1, r_2, r_3), \\ (r_1, r_2, r_3, r_4)^b &= (r_1, r_4\rho^{64}, r_3\rho^{64}, r_2\rho^{64}), \\ (r_1, r_2, r_3, r_4)^c &= (r_1, r_2\rho^{64}, r_3, r_4\rho^{64}), \end{aligned}$$

for all $(r_1, \ldots, r_4) \in N$.

The group X is now completely fixed, and can be illustrated as follows.

$$\big(\langle a\rangle \times \underbrace{\langle b\rangle \times \langle c\rangle}\big) \ltimes \big(\underbrace{\langle w\rangle} \times \langle v\rangle \times \langle u\rangle\big)$$

acts faithfully | acts diagonally | acts via "monomial" matrices

$$Q = \quad C_{17}^{(4)} \quad \times \quad \Big(R_{17^3}^{(2)} \times R_{17^3}^{(2)} \times R_{17^3}^{(2)} \times R_{17^3}^{(2)}\Big)$$

By construction, we have that

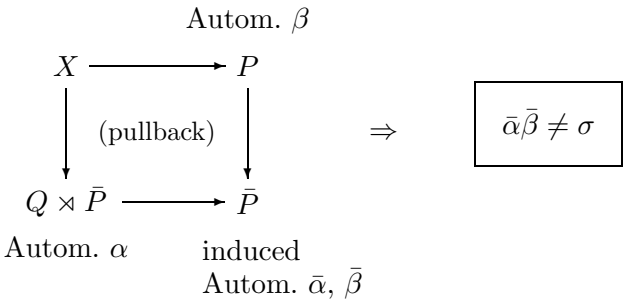
- conjugation by a^{16} induces fixed-point free automorphisms of $\mathrm{Z}(Q)$ and of $Q/\mathrm{Z}(Q)$,
- conjugation by a^{32} induces the identity on $\mathrm{Z}(N)$,
- $\mathrm{End}_H(N/\mathrm{Z}(N)) \cong \mathrm{Mat}_4(\mathbb{F}_{17})$, where $H = \langle w, b, c\rangle$.

Using these facts, the following crucial properties of X are proved in complete analogy to [57, Claims 2–5]:

- *The group-theoretical obstruction (see Lemma 16.14):*

  A class-preserving automorphism σ of $\bar{P}$ is defined by $\bar{c} \mapsto \bar{w}^4 \cdot \bar{c}$, and $\bar{w}$, $\bar{b}$, $\bar{a}$ stay fixed. Note that
  $$\{\bar{g}^{-1}(\bar{g}\sigma) \mid \bar{g} \in \bar{P}\} = \{1, \bar{w}^4\}.$$

  The group-theoretical obstruction ensures that a certain twist of X involving σ (see below) really yields another group Y. It can be depicted as follows:

  We remark that for this reason, the group Q has the additional factor $M = \mathbb{F}_{17^4}$.

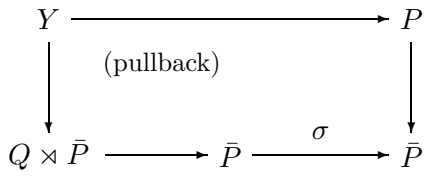
- *The inertia group:*

  We have $\eta_Q := 1 - \frac{1}{|Q|}\sum_{g\in Q} g = e + f$ with orthogonal central idempotents e and f of $\mathbb{Q}Q$. The inertia group of e in X is
  $$\mathsf{T}(e) = Q\langle u, v, w, a^2, b, c\rangle \quad \text{(which is of index 2 in } X\text{; we have } e^a = f\text{)}.$$

  Here, the important fact is that the subgroup $\langle w^4\rangle$, which measures the 'difference' between the elements $\bar{g}$ and $\bar{g}\sigma$, centralizes $\mathsf{T}(e) \cap P$.

The group Y

The group Y will be a twisted version of X,



We search for a nice embedding

$$Y \hookrightarrow \mathbb{Z}\big[\tfrac{1}{2}\big]X.$$

There are central subgroups of X:

$$\begin{aligned} Z_1 &:= [w^4, P] = \langle u^{16} \rangle \leq \mathrm{Z}(X), \\ Z_2 &:= [v \cdot w^4, P] = \langle v^2 \rangle \leq \mathrm{Z}(X), \\ Z_3 &:= [u^8 v \cdot w^4, P] = \langle u^{16} v^2 \rangle \leq \mathrm{Z}(X). \end{aligned}$$

Note that

$$\langle Z_i \mid i = 1, 2, 3 \rangle \cong C_2 \times C_2.$$

In particular, X has no faithful irreducible complex representation! In fact, we will construct Y as a subgroup of $\mathrm{V}(\mathbb{Z}\big[\tfrac{1}{2}\big]X)$ such that Y *agrees* with X on each block of $\mathbb{C}X$.

Further on, note that the action of w^4 on P can be compensated, on each block of $\mathbb{Z}\big[\tfrac{1}{2}\big]X$, by group elements acting trivially on Q.

There are automorphisms σ_i of the factor groups P/Z_i, defined by

$$\begin{aligned} \sigma_1 : &\quad c \mapsto w^4 \cdot c, \\ \sigma_2 : &\quad c \mapsto v \cdot w^4 \cdot c, \\ \sigma_3 : &\quad c \mapsto u^8 v \cdot w^4 \cdot c, \end{aligned}$$

and elements of the quotient of

$$S = \langle u, v, w, a, b \rangle$$

by Z_i stay fixed. (We hope that the reader is not disturbed by the somewhat sloppy notation.)

Note that

$$X = QS \rtimes \langle c \rangle.$$

In $\mathbb{Z}[\frac{1}{2}]\langle u^{16}, v^2\rangle$, there is an orthogonal central decomposition

$$1 = e_1 + e_2 + e_3,$$

with Z_i in the kernel of $e_i\mathbb{Q}X$. Set

$$t = e_1 + e_2 \cdot v + e_3 \cdot u^8 v, \quad \text{and} \quad d = t \cdot c.$$

Then

$$\begin{aligned} x^d &= x^c, \qquad (x \in Q), \\ s^d &= s^{w^4 c} \quad (s \in S). \end{aligned}$$

Thus,

$$Y = QS \rtimes \langle d \rangle$$

is a subgroup of $\mathrm{V}(\mathbb{Z}[\frac{1}{2}]X)$ of the same order as X.

There are isomorphisms

$$\begin{aligned} \alpha: \quad & S \rtimes \langle d \rangle \to S \rtimes \langle c \rangle = P, \\ & \boxed{d \mapsto w^4 c}, \ s \text{ in } S \text{ stay fixed}, \end{aligned}$$

and

$$\begin{aligned} \beta: \quad & Y/\mathrm{O}_2(Y) \to X/\mathrm{O}_2(X), \\ & \boxed{d \mapsto c}, \ y \text{ in } QS \text{ stay fixed}. \end{aligned}$$

It follows that the group Y is the twisted pullback:

$$\begin{array}{ccccc} Y & \longrightarrow & S \rtimes \langle d \rangle & \xrightarrow{\alpha} & P \\ \text{via } \beta \downarrow & & \text{(pullback)} & & \downarrow \\ Q \rtimes \bar{P} & \longrightarrow & \bar{P} & \xrightarrow{\sigma} & \bar{P} \end{array}$$

Thus, by the group-theoretical obstruction, the groups X and Y are non-isomorphic.

Isomorphism of semilocal group rings

We wish to prove

$$\mathbb{Z}_\pi X \cong \mathbb{Z}_\pi Y, \quad \pi = \pi(X) = \{2, 17\}.$$

By construction,

$$\mathbb{Z}[\tfrac{1}{2}]X = \mathbb{Z}[\tfrac{1}{2}]Y.$$

According to Proposition 1.6, we have to find local isomorphisms which fit together rationally. Thus, we have to prove existence of an isomorphism

$$\phi : RX \to RY, \quad R = \mathbb{Z}\big[\tfrac{1}{17}\big],$$

which induces a central automorphism of $\mathbb{Q}X$.

We will define ϕ piecewise, using the decompositions

$$RX = \epsilon_Q RX \oplus \eta_Q RX,$$
$$RY = \epsilon_Q RY \oplus \eta_Q RY,$$

where

$$\epsilon_Q = \tfrac{1}{|Q|}\sum_{g\in Q} g, \quad \eta_Q = 1 - \epsilon_Q.$$

Choose $e_1 = \frac{1+u^{16}}{2}$, so that

$$e_2 = (1-e_1)\tfrac{1+v^2}{2}, \quad e_3 = (1-e_1)\tfrac{1+u^{16}v^2}{2}.$$

The isomorphism of Sylow 2-subgroups

$$\alpha^{-1}: \quad P = S \rtimes \langle c\rangle \to S \rtimes \langle d\rangle,$$
$$\boxed{c \mapsto w^4 d}, \ s \text{ in } S \text{ stay fixed},$$

extends to an isomorphism

$$\phi_1 : \epsilon_Q RX \to \epsilon_Q RY,$$

agreeing on $e_i\epsilon_Q RX$ with the group automorphism σ_i. Thus, the following lemma tells us that ϕ_1 induces a central automorphism of $\epsilon_Q\mathbb{Q}X$.

3.2 Lemma. (i) *σ_1 is a class-preserving automorphism of G/Z_1;*

(ii) *σ_2 fixes each irreducible character which does not contain Z_1 in its kernel;*

(iii) *σ_3 fixes each irreducible character which does not contain Z_1 in its kernel.*

Proof. (i) It suffices to prove that for all $x \in \langle a,b\rangle c$, there is $k \in \langle u,v,w\rangle$ with $x\sigma_1 = x^k$. This follows from

$$a^w = u^{-4}a, \quad c^{u^{27}} = u^4 c \quad \text{and} \quad (bc)^{u^4} = u^8 bc,$$

which implies that for all $i \in \mathbb{N}$,

$$(a^i c)^{wu^{27i}} = a^i(w^4 c) = (a^i c)\sigma_1,$$
$$(a^i bc)^{w^2u^{4i}} = a^i b(w^4 c) = (a^i bc)\sigma_1.$$

(ii) Let $\chi \in \mathrm{Irr}(P/\langle v^2\rangle)$ with $u^{16} \notin \ker(\chi)$. Let ψ be an irreducible constituent of $\chi|_{\langle u\rangle}$. The inertia group of ψ is $\mathsf{T}(\psi) = \langle u, v, w, a\rangle \trianglelefteq P/\langle v^2\rangle$. Since σ_2 leaves each element of $\mathsf{T}(\psi)$ fixed, $\chi(g) = \chi(g\sigma_2) = \chi^{\sigma_2}(g)$ for all $g \in \mathsf{T}(\psi)$. If $g \in G \setminus \mathsf{T}(\psi)$, then $\chi(g) = \chi(0) = \chi(g\sigma_2)$ as χ is induced from a character of the normal subgroup $\mathsf{T}(\psi)$ (see Proposition 8.1).

(iii) This is proved in complete analogy to (ii). □

To construct an isomorphism

$$\phi_2 : \eta_Q RX \to \eta_Q RY,$$

we invoke (elementary) Clifford theory. Recall that

$$\eta_Q = e + f$$

with orthogonal central idempotents e, f of $\mathbb{Q}Q$, so that the inertia groups (with respect to X and to Y!) are

$$\mathsf{T}_X(e) = Q\langle u, v, w, a^2, b\rangle \rtimes \langle c\rangle,$$
$$\mathsf{T}_Y(e) = Q\langle u, v, w, a^2, b\rangle \rtimes \langle d\rangle.$$

Recall that

$$w^4 \text{ centralizes } \mathsf{T}_X(e) \cap P,$$
$$s^d = s^{w^4 c} \quad \text{for } s \in \langle u, v, w, a, b\rangle.$$

Thus we have an isomorphism of inertia groups:

$$\gamma : \mathsf{T}_X(e) \to \mathsf{T}_Y(e),$$
$$\boxed{c \mapsto d},\ x \in \langle u, v, w, a^2, b\rangle \text{ stay fixed.}$$

Now Clifford theory yields an isomorphism

$$\theta_X : \eta_Q RX \xrightarrow{\cong} \mathrm{Mat}_2(eR\mathsf{T}_X(e)), \quad m \mapsto \begin{bmatrix} eme & emae \\ ea^{-1}me & ea^{-1}mae \end{bmatrix},$$

and similarly for $\eta_Q RY$. Thus we have a commutative diagram

$$\begin{array}{ccc} \eta_Q RX & \xrightarrow{\phi_2} & \eta_Q RY \\ \downarrow{\scriptstyle \theta_X} & & \downarrow{\scriptstyle \theta_Y} \\ \mathrm{Mat}_2(eR\mathsf{T}_X(e)) & \xrightarrow{\gamma} & \mathrm{Mat}_2(eR\mathsf{T}_Y(e)) \end{array}$$

The isomorphism ϕ_2 agrees on $e_i\eta_Q\mathbb{Q}X$ with a group automorphism ρ_i of $\mathsf{T}_X(e)/Z_i$. These automorphisms are

$$\rho_1 = \mathrm{id},$$
$$\rho_2 : \begin{cases} c \mapsto v \cdot c \\ x \in Q\langle u, v, w, a^2, b\rangle \text{ stay fixed} \end{cases},$$

$$\rho_3 : \begin{cases} c \mapsto u^8 v \cdot c \\ x \in Q\langle u, v, w, a^2, b\rangle \text{ stay fixed} \end{cases}.$$

The automorphisms ρ_2 and ρ_3 fix each irreducible complex character which does not contain Z_1 in its kernel (this is proved in the very same way as Lemma 3.2 is proved). Thus, ϕ_2 induces a central automorphism on $\eta_Q\mathbb{Q}X = \mathrm{Mat}_2(e\mathbb{Q}\mathsf{T}(e))$.

Together, the isomorphism $\phi = \phi_1 \oplus \phi_2$ induces a central automorphism on $\mathbb{Q}X$, and Theorem 3.1 is proved.

3.3 Remark. For this semilocal counterexample, we have confirmed Scott's inertial group picture. In [127], Scott wrote "... my picture in the solvable case of a group ring automorphism is a collection of group isomorphisms on inertial groups that fit together rationally. ... What does this general picture say about the isomorphism problem itself? ... it just says that all group ring isomorphisms should be obtained from some system of group isomorphisms on related groups, usually smaller. There is a prospect for an elegant theory here, even if the isomorphism problem ... has a negative answer."

3.4 Problem. Does the groups of Theorem 3.1 yield a global counterexample, i.e., does $\mathbb{Z}X \cong \mathbb{Z}Y$ hold?

3.5 Remark. We briefly point out the connection with the normalizer problem (cf. [57, Section 1]). Recall that for $t = e_1 + e_2 \cdot v + e_3 \cdot u^8 v$,

$$x^t = x \quad (x \in Q), \qquad s^t = s^{w^4} \quad (s \in S), \tag{$*$}$$

and that

$$Y = G \rtimes \langle tc\rangle, \quad G = QS.$$

Thus

$$t \in \mathrm{N}_{\mathrm{V}(\mathbb{Q}G)}(G).$$

If, by some "accident", this becomes

$$t \in \mathrm{N}_{\mathrm{V}(\mathbb{Z}G)}(G),$$

still satisfying $(*)$ and the cocycle condition $(tc)^8 = 1$, we would conclude that $\mathbb{Z}X \cong \mathbb{Z}Y$.

4. A group-theoretical problem related to the isomorphism problem

Motivated by the semilocal analysis of the counterexample [57] in the previous section, we present the following example (which was found during an interactive Maple session).

4.1 Example. For any prime p, there is a p-group P having the following properties. There is $C_p \times C_p \cong Z \leq N \trianglelefteq P$, with Z contained in the center of P, such that:

(1) There is a class-preserving automorphism σ of P/N, which cannot be lifted to an automorphism of P;

(2) For a suitable labeling $Z_0, Z_1, \ldots, Z_p$ of the nontrivial cyclic subgroups of Z, σ can be lifted to automorphisms σ_i of P/Z_i, and

   (a) σ_0 is a class-preserving automorphism,

   (b) σ_i fixes each irreducible character of P/Z_i which does not contain Z_0 in its kernel ($i > 0$).

4.2 Remark. This example should be seen as a contribution towards the construction of non-isomorphic $p^a q^b$-groups X and Y having isomorphic integral group rings (over $\mathbb{Z}_{\{p,q\}}$).

We remark that it is a general fact that there are finite q-groups Q of nilpotency class 2 on which P/N acts faithfully such that only the inner automorphisms of P/N can be lifted to automorphisms of the semidirect product $Q(P/N)$. This was noted by Pettet [103], as an observation about a construction of Heinecken and Liebeck [50] (and a subsequent extension of Webb [145]). Thus it is unproblematic to obtain a group-theoretical obstruction.

To construct a counterexample to the isomorphism problem (with underlying group $X = QP$), it remains to refine such a construction to have P/N acting 'suitably' on the central idempotents of the rational group ring of Q, to obtain suitable inertia groups. So far, we did not follow up this job.

We begin with defining a group H by

$$H = \langle\, a, b, c \;:\; a^{p^2} = b^{p^2} = c^{p^2} = [a,b]^p = 1,\ [a,c] = [b,c] = 1,\\ [a,[a,b]] = [b,[a,b]] = 1 \,\rangle.$$

Then H is a group of order p^7, and

$$H = \{\, [a,b]^i a^j b^k c^l \mid 0 \leq i < p,\ 0 \leq j,k,l < p^2 \,\}.$$

Let A, B and C be the following matrices of $\mathrm{GL}_7(\mathbb{Z}/p^2\mathbb{Z})$:

$$A = \begin{bmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & p & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix},$$

$$B = \begin{bmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot \\ p & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & p \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & p \\ \cdot & \cdot & \cdot & \cdot & \cdot & p & 1 \end{bmatrix},$$

$$C = \begin{bmatrix} 1 & -p & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix}.$$

We claim that H is isomorphic to the group $\langle A, B, C\rangle$, with a, b and c corresponding to A, B and C, respectively. Therefore, check that A and B commute with C, and that their commutator

$$[A, B] = \begin{bmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & p \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & p \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & p \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix}$$

(of order p) commutes with A and B. Furthermore, the pth powers of the matrices A, B and C have order p:

$$A^p = \begin{bmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & p & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & p & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix}, \quad B^p = \begin{bmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & p & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & p \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix},$$

$$C^p = \begin{bmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & p \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & p & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix},$$

and the matrix

$$A^{pj}B^{pk}C^{pl} = \begin{bmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & pl \\ \cdot & 1 & \cdot & \cdot & \cdot & pk & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & pl & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & pj & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & pj & pk \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix}$$

is not a power of $[A, B]$ unless it is the identity matrix. This proves $H \cong \langle A, B, C\rangle$.

Via this representation, let H act on

$$V = (\mathbb{Z}/p^2\mathbb{Z})^{(6)} = \mathbb{Z}/p^2\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^2\mathbb{Z},$$

and let

$$P = V \rtimes H$$

be the corresponding semidirect product, i.e., $a^{-1}va = v^a = vA$ for all $v \in V$ etc.

Let $e_i \in V$ be the element whose i-th entry is 1, and 0 otherwise. We also set

$$\begin{aligned} u &= e_5 = (0,0,0,0,1,0,0), \\ v &= e_6 = (0,0,0,0,0,1,0), \\ w &= e_7 = (0,0,0,0,0,0,1). \end{aligned}$$

Let

$$N = \langle u^p, v^p, w\rangle,$$

a normal subgroup of P, and

$$Z = \langle v^p, w^p \rangle \cong C_p \times C_p,$$

a central subgroup of P contained in N. We label the $p+1$ subgroups of Z isomorphic to C_p as follows:

$$Z_0 = \langle w^p \rangle, \quad Z_i = \langle v^{pi} w^p \rangle,\ 0 < i < p, \quad \text{and} \quad Z_p = \langle v^p \rangle.$$

Note that $\langle A, B \rangle \trianglelefteq H$ and $H/\langle A, B \rangle = \langle C \rangle \cong C_{p^2}$. (We hope that the reader accepts that we will denote a group element and its image in a factor group by the same symbol whenever the precise meaning is obvious from the context.) Moreover, v maps to a central element (of order p^2) in P/Z_0. Hence an automorphism σ_0 of P/Z_0 is defined by

$$\mathrm{Aut}(P/Z_0) \ni \sigma_0 : \begin{cases} c \mapsto c \cdot v \\ \text{'other' generators, i.e., the elements of } \langle V, a, b \rangle, \text{ stay fixed} \end{cases}$$

The automorphism σ_0 induces on P/N an automorphism which will be denoted by σ. Let $M \trianglelefteq P$ with $M \leq N$; we ask whether σ can be lifted to an automorphism $\hat{\sigma}$ of P/M, i.e., whether there exists

$$\mathrm{Aut}(P/M) \ni \hat{\sigma} : \begin{cases} a \mapsto a \cdot u^{pr} v^{ps} w^t \\ b \mapsto b \cdot u^{pk} v^{pl} w^m \\ c \mapsto c \cdot v \cdot u^{px} v^{py} w^z \\ \quad \vdots \end{cases}$$

If we let

$$\begin{aligned} t_a &= (0,0,0,0,pr,ps,t), \\ t_b &= (0,0,0,0,pk,pl,m), \\ t_c &= (0,0,0,0,px,1+py,z), \end{aligned}$$

then $a\hat{\sigma} = a \cdot t_a$, and similarly for b and c. The condition that $a\hat{\sigma}$ and $c\hat{\sigma}$ have to commute gives

$$ac(t_a)^c t_c \equiv a t_a c t_c \equiv c t_c a t_a \equiv ca(t_c)^a t_a \mod M.$$

Equivalently, $(t_a)^c t_a^{-1} \equiv (t_c)^a t_c^{-1} \mod M$, which means that the elements $d_i \in V$, defined by

$$\begin{aligned} d_1 &= t_c(A-E) - t_a(C-E) = (0,0,0,0,0,px,0), \\ d_2 &= t_c(B-E) - t_b(C-E) = (0,0,0,0,0,pz,p(x+1)), \end{aligned}$$

are contained in M (here E denotes the identity matrix). Note that there do not exist elements x, z such that $d_1 = 0 = d_2$, showing that

- σ does not lift to an automorphism of P.

However, if $0 < i < p$ and $x = 0$, $z = i$, then $d_1, d_2 \in Z_i$, and if $x = -1$, $z = 0$, then $d_1, d_2 \in Z_p$. Hence we can record:

- σ lifts to an automorphism σ_i of P/Z_i for all i, with

$$\mathrm{Aut}(P/Z_i) \ni \sigma_i : \begin{cases} c \mapsto c \cdot v \cdot w^i \\ \text{other generators stay fixed} \end{cases} \qquad (0 < i < p)$$

$$\mathrm{Aut}(P/Z_p) \ni \sigma_p : \begin{cases} c \mapsto c \cdot v \cdot u^{-p} \\ \text{other generators stay fixed} \end{cases}$$

Write $h = [a,b]^i a^j b^k c^l$ for some element $h \in H$. We shall show that h is conjugate to an element of the coset $hv^l Z_0$, via an element of V. Note that for $x \in V$,

$$h^{(-x)} = h \cdot x([A,B]^i A^j B^k C^l - E), \quad (E \text{ the identity matrix}),$$

and that it is easily checked that

$$[A,B]^i A^j B^k C^l - E = \begin{bmatrix} \cdot & -pl & \cdot & \cdot & \cdot & \cdot & l \\ \cdot & \cdot & \cdot & \cdot & \cdot & k & pk(k-1)/2 \\ pk & \cdot & \cdot & \cdot & pj & l & p(i+kl) \\ \cdot & \cdot & \cdot & \cdot & \cdot & j & p(i+k+jk) \\ \cdot & \cdot & \cdot & \cdot & \cdot & j & p(i+kj) \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & pk \\ \cdot & \cdot & \cdot & \cdot & \cdot & pk & \cdot \end{bmatrix}.$$

If $(p,k) = 1$ or $(p,j) = 1$, it follows from $h^{(-e_2)} \in hv^k Z_0$ or $h^{(-e_4)} \in hv^j Z_0$, respectively, that h is conjugate to hv in P/Z_0. Hence we may assume that h is of the form $h = [a,b]^i a^{pj} b^{pk} c^l$. But then $h^{(-e_3)} \in hv^l Z_0$, as desired. We really have proved:

- σ_0 is a class-preserving automorphism.

Again, let $h = [a,b]^i a^j b^k c^l \in H$. Then

$$h^{e_1} = h \cdot e_2^{pl} w^{-l} \quad \text{and} \quad h^{(e_1^p)} = h \cdot w^{-pl},$$

so if $h \notin \langle A, B \rangle$, i.e., if $(l,p) = p$ or $(l,p) = 1$, then h and hw^p are conjugate via an element of V. Let $i > 0$ and let χ be an irreducible character of P/Z_i which does not contain $Z_0 = \langle w^p \rangle$ in its kernel. Note that if ρ is a representation of P affording χ, then $(w^p)\rho$ is ζ_p times the identity matrix, where ζ_p is a primitive pth root of unity. Thus if $g \in P \setminus \langle V, A, B \rangle$, then

$$\chi(g) = \chi(gw^p) = \zeta_p \cdot \chi(g),$$

which implies that $\chi(g) = 0$. Altogether, we have $\chi(g) = \chi(g\sigma_i)$ for all $g \in P$, and we have shown:

- If $i > 0$, then σ_i fixes each irreducible character of P/Z_i which does not contain Z_0 in its kernel.

This concludes Example 4.1.

5. Automorphisms of group rings of abelian by nilpotent groups

Scott proved that a finite abelian by nilpotent group is determined by its integral group ring (cf. [119, p. 601], [118]). Let G be a finite abelian by nilpotent group, and let A be the smallest abelian normal subgroup of G with nilpotent quotient G/A (note that A is well defined, see [65, III 2.5]). In this section, we show that if α is an augmentation-preserving automorphism of the integral group ring $\mathbb{Z}G$, then there is an automorphism ρ of G such that $\rho\alpha$ induces a central automorphism of $\mathbb{Z}G/A$. Then, an application of Kimmerle's $G \times G$-trick will yield another proof of Scott's result.

We shall make freely use of the elementary properties of the normal subgroup correspondence. For example, with G, A and α as above, α induces an automorphism of $\mathbb{Z}G/A$. For if B denotes the normal subgroup correspondent of $A\alpha$ in G, we have $\mathbb{Z}G/B \cong \mathbb{Z}G/A$, so G/B is nilpotent and $B = A$.

Lifting class-preserving group automorphisms

We shall need an elementary fact about lifting of group automorphisms. Let G be a finite group with a normal subgroup N, and let $\sigma \in \mathrm{Aut}(G/N)$. We say that σ *lifts* to G if there is $\hat{\sigma} \in \mathrm{Aut}(G)$ which fixes N and induces σ on G/N.

The next lemma shows a circumstance under which a class-preserving group automorphism of G/N lifts, provided that N is abelian. Another criterion is given in [80, Lemma 4.12].

5.1 Lemma. *Let G be a finite group with an abelian normal subgroup A. Assume that some $\sigma \in \mathrm{Aut}_{\mathrm{c}}(G/A)$ induces an inner automorphism of $\mathbb{Z}_{\pi(A)}G/A$. Then σ lifts to an automorphism of G.*

Proof. For a group H, let $\mathrm{I}(H)$ be the augmentation ideal of $\mathbb{Z}H$. Consider the exact sequence

$$0 \longrightarrow \frac{\mathrm{I}(A)G}{\mathrm{I}(A)\mathrm{I}(G)} \longrightarrow \frac{\mathbb{Z}G}{\mathrm{I}(A)\mathrm{I}(G)} \longrightarrow \mathbb{Z}G/A \longrightarrow 0.$$

The middle term is called the *small group ring of G* over $\mathbb{Z}$ associated with G and A, and will be denoted by $s(G, A)$ (cf. [119, 1.1.8]). The left term is an ideal in $s(G, A)$, of square zero, and is additively isomorphic to to the abelian group A. Suggestively,

we denote it by $\{A-1\}$. Tensoring the exact sequence with $\mathbb{Z}_{\pi(A)} \underset{\mathbb{Z}}{\otimes} -$ yields the exact sequence

$$0 \longrightarrow \{A-1\} \longrightarrow \mathbb{Z}_{\pi(A)} \underset{\mathbb{Z}}{\otimes} s(G,A) \longrightarrow \mathbb{Z}_{\pi(A)}G/A \longrightarrow 0.$$

By assumption, σ induces an inner automorphism of $\mathbb{Z}_{\pi(A)}G/A$, and since $\{A-1\}$ is an ideal of square zero, this automorphism lifts to an (inner) automorphism $\hat{\sigma}$ of $\mathbb{Z}_{\pi(A)} \underset{\mathbb{Z}}{\otimes} s(G,A)$. The natural copy of G in $\mathbb{Z}_{\pi(A)} \underset{\mathbb{Z}}{\otimes} s(G,A)$ is the pre-image of G/A and is therefore fixed by $\hat{\sigma}$. This proves the lemma. □

In a particular case, each class-preserving automorphism induces an inner automorphism of the semilocal group ring:

5.2 Proposition ([119, 1.2.13]). *If G is a finite group and S is a semilocal Dedekind domain in which $|G|$ is invertible, then* $\mathrm{Picent}(SG) = \mathrm{Outcent}(SG) = 1$.

5.3 Corollary. *Let G be a finite group with abelian normal subgroups A_1 and A_2 of coprime order. Assume that $\bar{G} = G/A_1A_2$ is nilpotent, and let $\beta \in \mathrm{Aut}_{\mathrm{c}}(\bar{G})$. Then there are $\sigma_i \in \mathrm{Aut}(G/A_i)$, both inducing class-preserving automorphisms $\bar{\sigma}_i$ of $\bar{G}$, such that $\beta = \bar{\sigma}_1\bar{\sigma}_2$.*

Proof. Since $\bar{G}$ is nilpotent and $(|A_1|, |A_2|) = 1$, we have a decomposition $\bar{G} = N_1 \times N_2$ where $(|A_i|, |N_i|) = 1$. Write $\beta = \tau_1\tau_2$ with $\tau_i|_{N_i} = \mathrm{id}|_{N_i}$. Note that by Proposition 5.2, τ_1 induces an inner automorphism of $\mathbb{Z}_{\pi(A_2)}\bar{G}$, and τ_2 induces an inner automorphism of $\mathbb{Z}_{\pi(A_1)}\bar{G}$. It follows from Lemma 5.1 that the class-preserving group automorphism τ_i lifts to an automorphism σ_i of G/A_i, as desired. □

Automorphisms of group rings of abelian by nilpotent groups

We shall need the following special case of a theorem due to Roggenkamp and Scott (see [62, Theorem 4.6]).

5.4 Theorem. *Let G be a finite group with a normal Sylow p-subgroup P satisfying $\mathrm{C}_G(P) \subseteq P$. Then for any $\alpha \in \mathrm{Aut}_{\mathrm{n}}(\mathbb{Z}G)$, the groups G and $G\alpha$ are conjugate in the units of $\mathbb{Z}_pG$.*

We are now in a position to prove the following theorem (in the spirit of [79]).

5.5 Theorem. *Let G be a finite abelian by nilpotent group, and let A be the smallest abelian normal subgroup of G with nilpotent quotient G/A. Then for any $\alpha \in \mathrm{Aut}_{\mathrm{n}}(\mathbb{Z}G)$, there is $\rho \in \mathrm{Aut}(G)$ such that $\rho\alpha$ induces a central automorphism of $\mathbb{Z}G/A$.*

Proof. By [119, Corollary 3] (Zassenhaus conjecture in the nilpotent group case), we may assume that $A \neq 1$. The theorem is proved by induction on the order of G. Set $\bar{G} = G/A$. We shall distinguish the following two cases.

Case 1 A is not a p-group. Then $A = A_1 \times A_2$ for some nontrivial normal subgroups A_1 and A_2 of G of coprime order. There are commutative diagrams

$$\begin{array}{ccc} G & \longrightarrow & G/A_1 \\ \downarrow & (*) & \downarrow \\ G/A_2 & \longrightarrow & \bar{G} \end{array} \qquad \text{and} \qquad \begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \mathbb{Z}G/A_1 \\ \downarrow & & \downarrow \\ \mathbb{Z}G/A_2 & \longrightarrow & \mathbb{Z}\bar{G} \end{array} .$$

By the normal subgroup correspondence, α induces automorphisms $\alpha_i \in \mathrm{Aut}_{\mathrm{n}}(\mathbb{Z}G/A_i)$. We may assume inductively that there are $\rho_i \in \mathrm{Aut}(G/A_i)$ such that each $\rho_i\alpha_i$ induces a central automorphism of $\mathbb{Z}\bar{G}$. Each ρ_i induces an automorphism $\bar{\rho}_i \in \mathrm{Aut}(\bar{G})$, and $\beta := \bar{\rho}_1\bar{\rho}_2^{-1}$ is a class-preserving group automorphism of $\bar{G}$. By Corollary 5.3, there are $\sigma_i \in \mathrm{Aut}(G/A_i)$, inducing class-preserving automorphisms $\bar{\sigma}_i$ of $\bar{G}$, such that $\beta = \bar{\sigma}_1^{-1}\bar{\sigma}_2$. Then $\bar{\sigma}_1\bar{\rho}_1 = \bar{\sigma}_2\bar{\rho}_2$, so there is $\rho \in \mathrm{Aut}(G)$ inducing $\sigma_i\rho_i$ on G/A_i (since $(*)$ is a pullback diagram), and $\rho\alpha$ induces the central automorphism $\bar{\sigma}_1(\bar{\rho}_1\bar{\alpha}_1)$ on $\mathbb{Z}\bar{G}$.

Case 2 A is a p-group. By Theorem 5.4, we may assume that $\mathrm{O}_{p'}(G) \neq 1$. Then there is a prime q, different from p, such that $B := \mathrm{Z}(\mathrm{O}_q(G)) \neq 1$. Set $\tilde{G} = G/AB$, and consider the commutative diagrams

$$\begin{array}{ccc} G & \longrightarrow & \bar{G} \\ \downarrow & (*) & \downarrow \\ G/B & \longrightarrow & \tilde{G} \end{array} \qquad \text{and} \qquad \begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \mathbb{Z}\bar{G} \\ \downarrow & & \downarrow \\ \mathbb{Z}G/B & \longrightarrow & \mathbb{Z}\tilde{G} \end{array} .$$

Arguing as in Case 1, we obtain $\varphi \in \mathrm{Aut}(G)$ such that $\beta := \varphi\alpha$ induces a central automorphism $\tilde{\beta}$ of $\mathbb{Z}\tilde{G}$. The automorphism β induces an automorphism $\bar{\beta}$ of $\mathbb{Z}\bar{G}$, and by [119, Corollary 3] (Zassenhaus conjecture in the nilpotent group case), there is $\sigma \in \mathrm{Aut}(\bar{G})$ such that $\sigma\bar{\beta}$ is a central automorphism. Note that σ induces an automorphism $\tilde{\sigma}$ of $\tilde{G}$. Since $\tilde{\beta}$ is a central automorphism, we may assume that σ induces the identity on $\mathrm{O}_{q'}(\bar{G})$. Also, σ induces a class-preserving group automorphism of $\mathrm{O}_q(\bar{G})/B$, so $\tilde{\sigma}$ induces an inner automorphism of $\mathbb{Z}_{(p)}\tilde{G}$ (see [119, 1.2.13]). Hence $\tilde{\sigma}$ lifts to G/B by Lemma 5.1, and there is $\psi \in \mathrm{Aut}(G)$ inducing σ. If we set $\rho = \psi^{-1}\varphi$, then $\rho\alpha$ induces the central automorphism $\sigma\bar{\beta}$ of $\mathbb{Z}\bar{G}$. □

The isomorphism problem for group rings of abelian by nilpotent groups

We give a variation of Kimmerle's $G \times G$-trick [81, Lemma 5.3].

5.6 Lemma. *Let G be an indecomposable finite group, and let H be another finite group with $\mathbb{Z}G \cong \mathbb{Z}H$. Assume that for every $\alpha \in \mathrm{Aut}_{\mathrm{n}}(\mathbb{Z}(G \times H))$ there is $\rho \in \mathrm{Aut}(G \times H)$*

and a proper normal subgroup M of H such that $\rho\alpha$ fixes the trace $\widehat{G \times M}$ (i.e., the sum of the elements of $G \times M$). Then $G \cong H$.

Proof. Let $\phi : \mathbb{Z}G \to \mathbb{Z}H$ be an isomorphism which maps G into $\mathrm{V}(\mathbb{Z}H)$. Note that $\mathbb{Z}G$ and $\mathbb{Z}H$ naturally embed into $\mathbb{Z}(G \times H)$.

There is $\alpha \in \mathrm{Aut}_{\mathrm{n}}(\mathbb{Z}(G \times H))$ with $(G \times H)\alpha = H\phi^{-1} \times G\phi$ (a "flip"). By assumption, we may modify α by a group automorphism of $G \times H$ such that α fixes the trace $\widehat{G \times M}$, for some proper normal subgroup M of H, and such that $(G \times H)\alpha = H\phi^{-1} \times G\phi$ still holds.

We calculate the image of

$$S := \left\{ x \in G \times H \;\middle|\; \widehat{G \times M} \cdot (x - 1) = 0 \right\} = G \times M$$

under α. By the normal subgroup correspondence, there is $N \trianglelefteq G$ with $\widehat{N\phi} = \widehat{M}$. It follows that

$$S\alpha := \left\{ y \in H\phi^{-1} \times G\phi \;\middle|\; \widehat{G \times M} \cdot (y - 1) = 0 \right\} \supseteq H\phi^{-1} \times N\phi$$

(note that α is augmented). Hence $G\alpha \times M\alpha = H\phi^{-1} \times N\phi$. Since $G\alpha$ is indecomposable, it follows that $G \cong G\alpha \cong H\phi^{-1} \cong H$ by the Krull–Remak–Schmidt theorem [65, I 12.5]. □

5.7 Theorem. *Let G be a finite abelian by nilpotent group, and let H be a group with $\mathbb{Z}G \cong \mathbb{Z}H$. Then $G \cong H$.*

Proof. By the normal subgroup correspondence, also H is abelian by nilpotent, and we may assume inductively that G is indecomposable. Let M be the smallest normal abelian subgroup of H with nilpotent quotient H/M. We may assume that M is a proper subgroup of H (otherwise G would be abelian). Let $\alpha \in \mathrm{Aut}_{\mathrm{n}}(\mathbb{Z}(G \times H))$. By Theorem 5.5, there is $\rho \in \mathrm{Aut}(G \times H)$ such that $\rho\alpha$ fixes the trace of $G \times M$. Hence $G \cong H$ by Lemma 5.6. □

II. On the Zassenhaus conjecture

> –Eh bien, mon vieux Barbicane, répondit Michel, on m'eût plutôt coupé la tête, en commençant par les pieds, que de me faire résoudre ce problème-là ! –Parce que tu ne sais pas l'algèbre, répliqua tranquillement Barbicane.
>
> *Jules Verne*
> *Autour de la lune, 1873*

This chapter contains various results related to the Zassenhaus conjecture (concerning automorphisms of integral group rings).

Let G be a finite group, and let S be a *G-adapted ring*, that is, an integral domain of characteristic 0 in which no prime divisor of $|G|$ is invertible. Following [127, p. 327], we shall say that an automorphism of SG has a *Zassenhaus factorization* if the automorphism is the composition of a group automorphism of G (extended to a ring automorphism) and a *central* automorphism (an automorphism of SG fixing the center element-wise). (This notion actually depends on the chosen group basis G.) We say that the Zassenhaus conjecture holds for G if each augmentation-preserving automorphism of $\mathbb{Z}G$ has a Zassenhaus factorization.

6. Some general observations

In this section, we briefly point out the role played by antihomomorphisms associated to group bases in connection with the Zassenhaus conjecture.

Though not in direct connection with the Zassenhaus conjecture, we point out a criterion for an element of the complex group ring to be conjugate to a group element.

Antihomomorphisms associated with group bases

We want to take the opportunity to collect in an omnibus lemma some properties of antihomomorphisms of group rings associated to group bases which are related to the Zassenhaus conjecture (see Proposition 6.1(ix)) and to the group $\mathrm{Out}_{\mathcal{C}}(G)$ of automorphisms of G which induce inner automorphisms of $\mathcal{C}G$ (see Proposition 6.1(xi)–(xiv)).

We do not claim that these results are really new; actually, most of them are well known in the basic $\mathcal{O} = \mathbb{Z}$ case (see Remark 6.2 to whom credit is due).

We fix the following notation.

- G is a finite group;
- $\mathcal{O}$ is a ring of algebraic integers in an algebraic number field (contained in $\mathbb{C}$);
- μ is the group of roots of units in $\mathcal{O}$;
- K is the normal closure of the field of fractions of $\mathcal{O}$;
- $\mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$;
- $\sigma \in \mathcal{G}$ is the complex conjugation on K;
- $\sigma^{\mathcal{G}}$ denotes the conjugacy class of σ in $\mathcal{G}$;
- For $x \in \mathbb{C}G$, let $x_g \in \mathbb{C}$ $(g \in G)$ be the coefficient of g in x, i.e., $x = \sum_{g\in G} x_g g$.

Let $*_G^\gamma$ be the antihomomorphism of KG associated with the group basis G and the automorphism $\gamma \in \mathcal{G}$, i.e.,

$$\Big(\sum_{g\in G} x_g g\Big)^{*_G^\gamma} = \sum_{g\in G} x_g^\gamma g^{-1} \quad (x_g \in K).$$

When $\gamma = \sigma$ is complex conjugation, then $*_G = *_G^\sigma$ is the well known anti-involution of KG.

6.1 Proposition. (i) *If $u^{*_G^\gamma} u \in \mu G$ for some $u \in \mathrm{U}(\mathcal{O}G)$ and all $\gamma \in \sigma^{\mathcal{G}}$, then $u \in \mu G$.*

(ii) *If $\mathcal{O}G = \mathcal{O}H$ and $*_G^\gamma = *_H^\gamma$ for all $\gamma \in \sigma^{\mathcal{G}}$, then $G = H$.*

(iii) $*_G^{\gamma^{-1}} \cdot *_{G^u}^\gamma = [*_G^\gamma, \mathrm{conj}(u)] = \mathrm{conj}(u^{*_G^\gamma} u)$ *for all $u \in \mathrm{U}(KG)$ and $\gamma \in \mathcal{G}$.*

(iv) $u^{*_G^\gamma} u \in \mathrm{Z}(KG)$ *for all $u \in \mathrm{N}_{\mathrm{U}(KG)}(G)$ and $\gamma \in \mathcal{G}$.*

(v) $(uu^{-*_G^\tau})^{*_G^\tau}(uu^{-*_G^\tau}) = 1$ *for all $u \in \mathrm{N}_{\mathrm{U}(KG)}(G)$ and all involutions $\tau \in \mathcal{G}$.*

(vi) *If $u \in \mathrm{N}_{\mathrm{U}(KG)}(\mathcal{O}G)$ and $\mathcal{O}G = \mathcal{O}H$ with $*_G^{\gamma^{-1}} \cdot *_H^\gamma = \mathrm{conj}(u^{*_G^\gamma} u)$ for all $\gamma \in \sigma^{\mathcal{G}}$, then $H = G^u$.*

(vii) *If for some $u \in \mathrm{U}(\mathcal{O}G)$, $u^{*_G^\gamma} u \in \mathrm{Z}(KG)$ for all $\gamma \in \sigma^{\mathcal{G}}$, then $u \in \mathrm{N}_{\mathrm{U}(\mathcal{O}G)}(G)$.*

(viii) *If $\alpha \in \mathrm{Aut}_{\mathrm{n}}(\mathcal{O}G)$ commutes with $*_G^\gamma$ for all $\gamma \in \sigma^{\mathcal{G}}$, then $\alpha \in \mathrm{Aut}(G)$.*

(ix) *Let $\alpha \in \mathrm{Aut}_{\mathrm{n}}(\mathcal{O}G)$. Then $[*_G^\gamma, \alpha] = \mathrm{conj}(u^{*_G^\gamma} u)$ for some $u \in \mathrm{N}_{\mathrm{U}(KG)}(\mathcal{O}G)$ and all $\gamma \in \sigma^{\mathcal{G}}$ if and only if α admits a Zassenhaus decomposition with respect to G, i.e., if there is $\rho \in \mathrm{Aut}(G)$ such that $\alpha \cdot \rho \in \mathrm{Inn}(KG)$.*

(x) *If $\sigma \in \mathrm{Z}(\mathcal{G})$, then $uu^{-*_G^\sigma} \in \mu G$ for all $u \in \mathrm{N}_{\mathrm{U}(\mathcal{O}G)}(G)$.*

(xi) *The exponent of* $\mathrm{Out}_{\mathcal{O}}(G)$ *divides* $2|\mathcal{N}|$, *where* $\mathcal{N} = \langle [\sigma, \mathcal{G}]^\gamma \,:\, \gamma \in \mathcal{G} \rangle \trianglelefteq \mathcal{G}$.

(xii) *If* $\sigma \in \mathrm{Z}(\mathcal{G})$, *then* $\mathrm{Out}_{\mathcal{O}}(G)$ *is an elementary abelian* 2*-group.*

(xiii) $[u, v]^{*_G^\gamma}[u, v] = 1$ *for all* $u, v \in \mathrm{N}_{\mathrm{U}(KG)}(G)$ *and* $\gamma \in \mathcal{G}$.

(xiv) *Let* A *be the ring of all algebraic integers in* $\mathbb{C}$. *Then* $\mathrm{Out}_A(G)$ *is contained in the center of* $\mathrm{Out}_{\mathrm{c}}(G)$. *In particular,* $\mathrm{Out}_A(G)$ *is an abelian group.*

Proof. (i) Let $u = \sum_{g \in G} u_g g$ and $\gamma \in \sigma^{\mathcal{G}}$. Then $c(\gamma)_1 = \sum_{g \in G} u_g^\gamma u_g$ is the coefficient of 1 in $c(\gamma) = u^{*_G^\gamma} u$, so either $c(\gamma)_1 = 0$ or $c(\gamma)_1 \in \mu$. If $u_g = 0$ or $u_g \in \mu$ for all $g \in G$, then $c(\sigma)_1 = \sum_{g \in G} |u_g| = \sharp\{g \in G \mid u_g \neq 0\} \in \mu$ implies that $u \in \mu G$. Now assume that $0 \neq u_h \notin \mu$ for some $h \in G$. By a theorem of Kronecker (see [95, Theorem 2.1]), there is $\alpha \in \mathcal{G}$ with $|u_h^\alpha| > 1$. Then $(c(\sigma^{\alpha^{-1}})_1)^\alpha = \sum_{g \in G} u_g^{\alpha\sigma} u_g^\alpha = \sum_{g \in G} |u_g^\alpha|^2 > 1$, which implies that $0 \neq c(\sigma^{\alpha^{-1}})_1 \notin \mu$, a contradiction.

(ii) Let $h \in H$. By assumption, $h^{*_G^\gamma} h = h^{*_H^\gamma} h = 1$ for all $\gamma \in \sigma^{\mathcal{G}}$, so $h \in \mu G$ by (i). Taking augmentation gives $h \in G$.

(iii) $*_G^{\gamma^{-1}} \cdot \underbrace{\mathrm{conj}(u^{-1}) \cdot *_G^\gamma \cdot \mathrm{conj}(u)}_{= *_{G^u}^\gamma \text{ (consider effect on } G^u)} = \underbrace{*_G^{\gamma^{-1}} \cdot \mathrm{conj}(u^{-1}) \cdot *_G^\gamma}_{= \mathrm{conj}(u^{*_G^\gamma})} \cdot \mathrm{conj}(u)$.

(iv) Immediate from (iii).

(v) $(uu^{-*_G^\tau})^{*_G^\tau}(uu^{-*_G^\tau}) = u^{-1}(u^{*_G^\tau} u)u^{-*_G^\tau} = 1$ by (iv).

(vi) By (iii), $*_H^\gamma = *_{G^u}^\gamma$ for all $\gamma \in \sigma^{\mathcal{G}}$. Hence $H = G^u$ by (ii).

(vii) By (iii), $*_G^\gamma = *_{G^u}^\gamma$ for all $\gamma \in \sigma^{\mathcal{G}}$. Hence $G = G^u$ by (ii).

(viii) If $\alpha \in \mathrm{Aut}_{\mathrm{n}}(\mathcal{O}G)$ commutes with $*_G^\gamma$, then $(g\alpha)^{*_G^\gamma}(g\alpha) = (g^{*_G^\gamma}\alpha)(g\alpha) = 1$ for all $g \in G$. Hence the assertion follows from (i).

(ix) Since $[*_G^\gamma, \alpha] = *_G^{\gamma^{-1}} \cdot *_{G\alpha}^\gamma$, this follows from (iii) and (vi).

(x) Immediate from (i) and (v).

(xi) Let $u \in \mathrm{N}_{\mathrm{U}(\mathcal{O}G)}(G)$. Note that by (iv), $u^{*_G^\gamma}$ commutes with u and $u^{*_G^{\gamma'}}$, for all $\gamma, \gamma' \in \mathcal{G}$. Again by (iv), $z := \big(\prod_{\gamma \in \mathcal{N}} u^{*_G^\gamma}\big) u^n \in \mathrm{Z}(KG)$, where $n = |\mathcal{N}|$. Let E be the fixed field under $\mathcal{N}$, with ring of integers $\mathcal{O}_E$. By the fundamental theorem of Galois theory, the Galois group of E over $\mathbb{Q}$ is naturally isomorphic to the factor group $\mathcal{G}/\mathcal{N}$; by construction of $\mathcal{N}$, the complex conjugation σ is contained in the center. Clearly $zu^{-n} = \prod_{\gamma \in \mathcal{N}} u^{*_G^\gamma} \in \mathrm{U}(\mathcal{O}_E G)$, so

$$z^2 u^{-2n} = \underbrace{(zu^{-n})(zu^{-n})^{-*_G^\sigma}}_{\in \mu G \text{ by (x)}} \underbrace{(zu^{-n})^{*_G^\sigma}(zu^{-n})}_{\in \mathrm{Z}(KG) \text{ by (iv)}},$$

and $\mathrm{conj}(u^{2n}) \in \mathrm{Inn}(G)$.

(xii) Follows from (xi).

(xiii) Let $* = *_G^\gamma$. It follows from (iv) that

$$\begin{aligned}[u,v]^*[u,v] &= v^*u^*v^{-*}u^{-*}u^{-1}v^{-1}uv = v^*(u^*u)u^{-1}v^{-*}u^{-*}u^{-1}v^{-1}uv \\ &= v^*u^{-1}v^{-*}u^{-*}(u^*u)u^{-1}v^{-1}uv = v^*u^{-1}v^{-*}v^{-1}uv \\ &= (v^*v)v^{-1}u^{-1}v^{-*}v^{-1}uv = v^{-1}u^{-1}v^{-*}(v^*v)v^{-1}uv = 1.\end{aligned}$$

(xiv) Let $\phi \in \mathrm{Aut_c}(G)$ and $\alpha \in \mathrm{Aut}_A(G)$; we have to show $[\phi,\alpha] \in \mathrm{Inn}(G)$. There is $u \in \mathrm{U}(\mathbb{Q}G)$ with $\phi = \mathrm{conj}(u)$ and $v \in \mathrm{U}(AG)$ with $\alpha = \mathrm{conj}(v)$. It follows

$$[u,v] = u^{-1}\underbrace{(v^{-1}uv)}_{\in \mathbb{Q}G} = \underbrace{(u^{-1}v^{-1}u)}_{\in AG}v \in \mathbb{Q}G \cap AG = \mathbb{Z}G.$$

By (xiv) and (i), $[u,v] = g$ for some $g \in G$, so $[\phi,\alpha] = \mathrm{conj}(g) \in \mathrm{Inn}(G)$. □

6.2 Remark. For $\mathcal{O} = \mathbb{Z}$, (i) is due to Berman. The version presented here follows [93, Theorem 2], but the result already appeared in work of Bovdi [15, p. 374–5]. For $\mathcal{O} = \mathbb{Z}$, (ii) is due to Banaschewski. Item (v) for $\mathcal{O} = \mathbb{Z}$ is an observation of Krempa (see [66]); the present form is taken from [93]. Sandling [125, 5.15, 5.16] recorded (ix) for $\mathcal{O} = \mathbb{Z}$. Items (x) and (xi) are from Mazur's paper [93]. Item (xii) in the $\mathcal{O} = \mathbb{Z}$ case is again Krempa's observation. Items (xiii) and (xiv) reproduce [58, Proposition 3.1] (cf. also Proposition 19.1).

Finally, we remark that a special feature of the integral group ring $\mathbb{Z}G$ is that for each $u \in \mathrm{N}_{\mathrm{U}(\mathbb{Z}G)}(G)$, there is $h \in \mathrm{C}_G(u)$ such that hu is $*_G$-invariant (see the proof of Proposition 19.2).

Conjugacy of torsion units and partial augmentation

Let G be a finite group. For $u = \sum_{g\in G} u_g g$ (all u_g in $\mathbb{C}$), we adopt the notation from [90] and write $\tilde{u}(g) = \sum_{x\sim g} u_x$. The $\tilde{u}(g)$'s are called the *partial augmentations* of u. The partial augmentations of u vanish if and only if u is contained in the additive commutator $[\mathbb{C}G,\mathbb{C}G] = \{xy - yx \mid x,y \in \mathbb{C}G\}$.

Marciniak, Ritter, Sehgal and Weiss proved the following [90, Theorem 2.5]:

6.3 Theorem. *Let U be a periodic subgroup of $\mathrm{V}(\mathbb{Z}G)$. Then the following are equivalent:*

(i) *For every $u \in U$ there exists a group element $g \in G$ such that such that u is conjugate to g in $\mathrm{U}(\mathbb{Q}G)$.*

(ii) *For every* $u = \sum u_g g \in U$, *there exists a* g_0, *unique up to conjugacy, such that* $\tilde{u}(g_0) \neq 0$.

We point out another criterion for $u \in \mathbb{C}G$ to satisfy condition Theorem 6.3(ii). Yamauchi [148] observed that a central unit $u \in \mathrm{V}(\mathbb{C}G)$ of finite order is trivial (i.e., contained in G) if $\chi\psi(u) = \chi(u)\psi(u)$ for all $\chi, \psi \in \mathrm{Irr}(G)$. Note that $\chi\psi$ is defined by $\chi\psi(g) = \chi(g)\psi(g)$ for all $g \in G$, and linear extension to $\mathbb{C}G$. This observation is generalized by the following proposition.

6.4 Proposition. *Let* $u \in \mathbb{C}G \setminus [\mathbb{C}G, \mathbb{C}G]$. *Then there exists a* $g \in G$, *unique up to conjugacy in* G, *with* $\tilde{u}(g) \neq 0$ *if and only if* $\chi\psi(u) = \chi(u)\psi(u)$ *for all* $\chi, \psi \in \mathrm{Irr}(G)$.

We remark that Hasse [49] proved a similar result.

Let $a(\mathbb{C}G)$ be the character ring of G, and set $A(\mathbb{C}G) = \mathbb{C} \otimes_{\mathbb{Z}} a(\mathbb{C}G)$. The proposition follows from the fact that each species of $A(\mathbb{C}G)$ (i.e., a nonzero $\mathbb{C}$-algebra homomorphism $A(\mathbb{C}G) \to \mathbb{C}$) is of the form $\chi \mapsto \chi(g)$ for some $g \in G$. Nevertheless, we shall give an elementary proof below.

If H is a group basis of $\mathbb{Z}G$, then each element of H is conjugate to some element of G in the units of $\mathbb{Q}G$, by the class sum correspondence. However, the following conjecture of Zassenhaus is still an open problem.

(ZC 1) If $u \in \mathrm{V}(\mathbb{Z}G)$ is of finite order, then u is conjugate to some $g \in G$ within the units of $\mathbb{Q}G$.

We have the following reformulation of this conjecture.

6.5 Corollary. (ZC 1) *holds for* G *if and only if for all* $u \in \mathrm{V}(\mathbb{Z}G)$ *of finite order, and all* $\chi, \psi \in \mathrm{Irr}(G)$, *there is an equality* $\chi\psi(u) = \chi(u)\psi(u)$.

Proof. Immediate from Theorem 6.3 and Theorem 6.4. □

One might speculate whether there is some analogue for units in blocks of $\mathbb{Z}_{(p)}G$.

Proposition 6.4 follows from two simple lemmas. The first one can also be seen as an application of Artin's theorem, cf. [85, Ch. VI Corollary 4.2].

6.6 Lemma. *Let* $h \in \mathbb{N}$, *and* $c, a_i \in \mathbb{C}$, $b_i \in \mathbb{C} \setminus \{0\}$ $(1 \leq i \leq h)$ *such that the* b_i *are pairwise distinct, and at least one of the* a_i *is different from* 0. *Assume that for all* $1 \leq n \leq h+1$,

$$c^n = a_1 b_1^n + a_2 b_2^n + \ldots + a_h b_h^n. \qquad (*)$$

Then $a_{i_0} = 1$ *for some index* i_0, *and* $a_i = 0$ *for* $i \neq i_0$.

Proof. Consider the matrix equation

$$\begin{bmatrix} c \\ c^2 \\ \vdots \\ c^h \end{bmatrix} = \begin{bmatrix} b_1 & b_2 & \dots & b_h \\ b_1^2 & b_2^2 & \dots & b_h^2 \\ \vdots & \vdots & & \vdots \\ b_1^h & b_2^h & \dots & b_h^h \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_h \end{bmatrix}.$$

The Vandermonde determinant of the matrix (b_i^j) does not vanish. Since some $a_i \neq 0$, it follows that $c \neq 0$. Dividing $(*)$ by c^n, we may assume that $c = 1$. But then $[a_1b_1, a_2b_2, \dots, a_hb_h]^{\mathrm{T}}$ is also a solution of the matrix equation, and it follows that $a_ib_i = a_i$, so either $a_i = 0$ or $b_i = 1$ for all i. Since the b_i's are distinct, and at least one a_i is different from 0, the assertion follows. □

6.7 Lemma. *Let $u \in \mathbb{C}G$. If $\chi\psi(u) = \chi(u)\psi(u)$ for all $\chi, \psi \in \mathrm{Irr}(G)$, then this equality also holds for all virtual characters χ and ψ of G.*

Proof. Let $\chi_i, \psi_j \in \mathrm{Irr}(G)$, and $a_i, b_j \in \mathbb{C}$. Then

$$\begin{aligned} \Big(\sum_i a_i\chi_i\Big)\Big(\sum_j b_j\psi_j\Big)(u) &= \sum_{i,j} a_ib_j\chi_i\psi_j(u) \\ &= \sum_{i,j} a_ib_j\chi_i(u)\psi_j(u) \qquad \text{(by assumption)} \\ &= \sum_i a_i\chi_i(u) \cdot \sum_j b_j\psi_j(u) = \Big(\sum_i a_i\chi_i\Big)(u)\Big(\sum_j b_j\psi_j\Big)(u), \end{aligned}$$

as desired. □

Proof of Proposition 6.4. Let $u \in \mathbb{C}G \setminus [\mathbb{C}G, \mathbb{C}G]$.

If there is $g \in G$, unique up to conjugacy in G, with $\tilde{u}(g) \neq 0$, then $\chi\psi(u) = \chi\psi(g) = \chi(g)\psi(g) = \chi(u)\psi(u)$ for all $\chi, \psi \in \mathrm{Irr}(G)$.

To prove the converse, let $g_1, \dots, g_h$ be representatives of the conjugacy classes of G, and set $\tilde{u}_i = \tilde{u}(g_i)$. Let μ be a (virtual) character of G which separates the conjugacy classes of G, i.e., $\mu(g_i) \neq \mu(g_j)$ for all $i \neq j$, and which satisfies $\mu(g_i) \neq 0$ for all i. By Lemma 6.7, $\mu(u)^n = \mu^n(u)$ for all $n \in \mathbb{N}$, so

$$\begin{aligned} \mu(u)^n = \mu^n(u) &= \tilde{u}_1\mu^n(g_1) + \tilde{u}_2\mu^n(g_2) + \dots + \tilde{u}_h\mu^n(g_h) \\ &= \tilde{u}_1\mu(g_1)^n + \tilde{u}_2\mu(g_2)^n + \dots + \tilde{u}_h\mu(g_h)^n. \end{aligned}$$

Now apply Lemma 6.6 with $c = \mu(u)$, $a_i = \tilde{u}_i$ and $b_i = \mu(g_i)$ to conclude that all $\tilde{u}_i$, except one, vanish. □

7. A pullback diagram for integral group rings

Let G be a finite group. Roggenkamp and Scott [117] showed that in the presence of normal subgroups of G of pairwise coprime order, an integral group ring RG can be described by a pullback diagram (Theorem 7.1) which proved to be very useful to construct counterexamples to the Zassenhaus conjecture. (This will be illustrated by examples we give in the next chapter.)

Aleev [1, Theorem 13] determined the unit group of the integral group ring of a cyclic group of order 10. The lengthy calculation makes essential use of properties of Fibonacci numbers. We show that Aleev's result can be quickly derived from the pullback description, and our method apparently can be applied to compute other unit groups.

An integral part of the pullback description will be used to put recent work of Lam and Leung [84] on vanishing sums of mth roots of unity into a more general context, the results being formulated entirely in the language of group rings.

For a normal subgroup N of G, we set

$$\hat{N} = \sum_{n \in N} n.$$

We have corresponding central idempotents

$$\epsilon_N = \frac{1}{|N|}\hat{N} \quad \text{and} \quad \eta_N = 1 - \epsilon_N.$$

Let R be an integral domain of characteristic 0 with field of fractions K. Let N be a normal subgroup of G. We write $\mathrm{I}_R(N)$ for the augmentation ideal of RN, so $\mathrm{I}_R(N)G$ is the kernel of the natural map $RG \to R(G/N)$. The ideals $\mathrm{I}_R(N)G$ and $(RG) \cdot \hat{N}$ intersect trivially, and their sum is the ideal generated by $\mathrm{I}_R(N)G$ and $|N|$. Thus we have the following well known pullback diagram of rings:

$$\begin{array}{ccc} RG & \longrightarrow & RG/N \\ \downarrow & & \downarrow \\ RG/(\hat{N}) & \longrightarrow & (R/|N|R)\,(G/N) \end{array}$$

Roggenkamp and Scott [117] gave the following generalization.

7.1 Theorem (Roggenkamp, Scott). *Let $N_1, \ldots, N_r \trianglelefteq G$, with N_j and N_k of coprime order for all $j \neq k$. Set $R_i = R/|N_i|R$. Then there is a commutative diagram*

with exact rows (the maps being the natural ones):

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \bigcap_i \mathrm{I}_R(N_i)G & \longrightarrow & RG & \longrightarrow & \bigoplus_i RG/N_i & & \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \bigcap_i \mathrm{I}_R(N_i)G & \longrightarrow & \dfrac{RG}{\sum_i (RG)\cdot \hat{N}_i} & \longrightarrow & \bigoplus_i \dfrac{R_iG/N_i}{\sum_{j\neq i}(R_iG/N_i)\cdot \hat{N}_j} & \longrightarrow & 0
\end{array}$$

We will record an essential part of the proof of this theorem in a separate lemma. Roggenkamp and Scott proved the equality stated in this lemma by showing equality at the localization of all maximal ideals of R, but we can give an even shorter proof.

7.2 Lemma. *Let $N_1, \ldots, N_r \trianglelefteq G$, with N_j and N_k of coprime order for all $j \neq k$. Then*

$$\sum_{i=1}^{r} (RG)\cdot \hat{N}_i = RG \cap \Big(\sum_{i=1}^{r} KG \cdot \epsilon_{N_i} \Big).$$

Proof. The inclusion "$\subseteq$" in (ii) is obvious. The reverse inclusion is proved by induction on r. Set $e_i = \epsilon_{N_i}$, and take any $x \in RG \cap \sum_i KG \cdot e_i$. If $r = 1$, then we may write $x = \sum_{g\in T} k_g \hat{N}_1 g$ where T is a system of coset representatives of N_1 in G and $k_g \in K$ for all $g \in T$. Since $x \in RG$, it follows that all k_g lie in R and consequently $x \in (RG)\cdot \hat{N}_1$. So let $r > 1$, and fix some index j. Then

$$x \cdot |N_j|(1 - e_j) \in RG \cap \sum_{i\neq j} KG \cdot e_i,$$

and we may assume inductively that

$$x \cdot |N_j| - x \cdot \hat{N}_j = x \cdot |N_j|(1 - e_j) \in \sum_{i\neq j} (RG)\cdot \hat{N}_i.$$

Hence $x \cdot |N_j| \in \sum_{i=1}^{r} (RG)\cdot \hat{N}_i$. As $(|N_1|, |N_2|) = 1$, we obtain $x \in \sum_{i=1}^{r} (RG)\cdot \hat{N}_i$. □

We continue with a proof of the above theorem which differs somewhat from the original presentation given by Roggenkamp and Scott.

Proof (of Theorem 7.1). Set $e_i = \epsilon_{N_i}$ and $f = \prod_i (1 - e_i)$. Note that

$$\bigcap_i \mathrm{I}_K(N_i)G = KG \cdot f \quad \text{and} \quad \sum_i KG \cdot e_i = KG \cdot (1 - f).$$

There are two-sided ideals

$$S = \sum_i (RG)\cdot \hat{N}_i, \quad D = \bigcap_i \mathrm{I}_R(N_i)G \quad \text{and} \quad J_i = S + \mathrm{I}_R(N_i)G$$

of RG. We shall prove

(i) $D = RG \cap (\bigcap_i \mathrm{I}_K(N_i)G) = RG \cap KG \cdot f$;

(ii) $S = RG \cap (\sum_i KG \cdot e_i) = RG \cap KG \cdot (1-f)$;

(iii) $S \cap D = 0$;

(iv) $S + D = \bigcap_i J_i$;

(v) $J_i + J_k = RG$ for all $i \neq k$.

(i) is obvious, and (ii) is Lemma 7.2.

(iii) follows directly from (i) and (ii).

In order to prove (iv), we first show that $(\bigcap_i J_i)f \subseteq D$ by induction on r. If $r = 1$, then

$$J_1 f = (S + \mathrm{I}_R(N_1)G)f \overset{\text{(ii)}}{=} \mathrm{I}_R(N_1)G \cdot f = Df \overset{\text{(i)}}{=} D.$$

Now let $r > 1$, take any $x \in \bigcap_i J_i$ and fix some index j. Then

$$x \cdot |N_j|(1-e_j) \in \bigcap_{i \neq j} \left(\sum_{k \neq j} (RG) \cdot \hat{N}_k \right) + \mathrm{I}_R(N_i)G,$$

so we may assume inductively that

$$x \cdot |N_j| \cdot f = x \cdot |N_j|(1-e_j) \cdot \prod_{i \neq j}(1-e_i) \in \bigcap_{i \neq j} \mathrm{I}_R(N_i)G \subseteq RG.$$

Since $(|N_1|, |N_2|) = 1$, it follows that $xf \in RG$. Hence $xf \in D$ by (i), and we have proved $(\bigcap_i J_i)f \subseteq D$. Again, let $x \in \bigcap_i J_i$. We have seen that $xf \in D$. Since $x(1-f) \in S$ by (ii), $x = x(1-f) + xf \in S + D$ and (iv) is proved.

Since $|N_i| = \hat{N}_i - (\hat{N}_i - |N_i|) \in J_i$ and $(|N_i|, |N_k|) = 1$, it follows that $1 \in J_i + J_k$ and (v) is proved.

By (iii), there is a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & D & \longrightarrow & RG & \longrightarrow & RG/D & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & D & \longrightarrow & RG/S & \longrightarrow & RG/S + D & \longrightarrow & 0 \end{array}$$

By (iv) and (v), we may apply the Chinese remainder theorem to get the natural isomorphism

$$RG/S + D = RG/\bigcap_i J_i \cong \bigoplus_i RG/J_i.$$

Since the kernel of the natural homomorphism

$$RG \to \frac{R_iG/N_i}{\sum_{j \neq i}(R_iG/N_i) \cdot \hat{N}_j}$$

— recall that $R_i = R/|N_i|R$ — is precisely J_i, this proves the theorem. □

The following example shows how the pullback can be used to compute unit groups of integral group rings.

7.3 Example. Let $C_{10} = \langle x \rangle$ be the cyclic group of order 10. We shall compute the unit group of $\mathbb{Z}C_{10}$ using the pullback description of $\mathbb{Z}C_{10}$ given by Theorem 7.1. We remark that the unit group has already been computed by Aleev [1, Theorem 13]. However, his calculation is somewhat special and occupies, including some corollaries, about 15 pages.

By Theorem 7.1, we have a commutative diagram

$$\begin{array}{ccc} \mathbb{Z}C_{10} & \longrightarrow & \mathbb{Z}C_5 \oplus \mathbb{Z}C_2 \\ \downarrow & & \downarrow \\ \dfrac{\mathbb{Z}C_{10}}{(\hat{C}_5, \hat{C}_2)} & \longrightarrow & \dfrac{\mathbb{F}_2C_5}{(\hat{C}_5)} \oplus \dfrac{\mathbb{F}_5C_2}{(\hat{C}_2)} \end{array} \qquad (*)$$

which can be written as

$$\begin{array}{ccc} \mathbb{Z}C_{10} & \longrightarrow & \mathbb{Z}C_5 \oplus \mathbb{Z}C_2 \\ \downarrow & & \downarrow \\ \mathbb{Z}[\zeta_{10}] & \longrightarrow & \mathbb{F}_2(\zeta_5) \oplus \mathbb{F}_5 \end{array}$$

Here, ζ_n denotes a primitive nth root of unity (clearly $\mathbb{Z}[\zeta_{10}] = \mathbb{Z}[\zeta_5]$). Note that we obtain a pullback diagram if we replace $\mathbb{Z}C_5 \oplus \mathbb{Z}C_2$ by the pullback Γ over the augmentation ε, that is, $\Gamma = \{(s,t) \mid (s,t) \in \mathbb{Z}C_5 \oplus \mathbb{Z}C_2 \text{ and } \varepsilon(s) = \varepsilon(t)\}$.

Clearly the image of $\mathrm{U}(\mathbb{Z}C_2)$ in $\mathbb{F}_5$ is $\{\pm 1\}$. Let $\zeta_5 = \exp(2\pi i/5)$. Then

$$\omega := -\zeta_5^2 - \zeta_5^3 = \frac{1+\sqrt{5}}{2}$$

is a fundamental unit of $\mathbb{Z}[\zeta_5]$ and $\mathrm{U}(\mathbb{Z}[\zeta_5]) = \langle -\zeta_5 \rangle \times \langle \omega \rangle$. Let $\bar{x}$ be the image of x under the map $\mathbb{Z}C_{10} \to \mathbb{Z}C_5$. Then it is easy to see that

$$\mathrm{U}(\mathbb{Z}C_5) = \langle -\bar{x} \rangle \times \langle -1 + \bar{x}^2 + \bar{x}^3 \rangle$$

(this is well known). Let $\zeta_{10} = -\zeta_5$. Then $1 + \zeta_{10}^2 - \zeta_{10}^3 = 1 + \zeta_5^2 + \zeta_5^3 = \frac{1-\sqrt{5}}{2}$ is a fundamental unit of $\mathbb{Z}[\zeta_{10}]$ (this choice will yield the generators for the unit group given by Aleev).

Let $w \in \mathrm{U}(\mathbb{Z}C_{10})$. Multiplying w with a trivial unit, and inverting w if necessary, we may assume that for some $n \geq 0$, the elements w and $(1+x^2-x^3)^n$ have the same image in $\Lambda = \mathbb{Z}C_{10}/(\hat{C}_5, \hat{C}_2)$. The following table lists the relevant congruences ($\Phi_i(x)$ denotes

the i-th cyclotomic polynomial).

n	$(1+x^2-x^3)^n$		$(-1+x^2+x^3)^n$
	$\bmod (\Phi_5(x), 2)$	$\bmod (\Phi_2(x), 5)$	$\bmod (\Phi_5(x), 2)$
1	$1+x^2+x^3$	3	$1+x^2+x^3$
2	x^2+x^3	-1	x^2+x^3
3	1	2	1

It follows that $n \neq 1$, and that there are units $u, v \in \mathrm{V}(\mathbb{Z}C_{10})$, defined via the diagram $(*)$ as indicated below.

$$\begin{array}{ccc} u & \longmapsto & ((-1+x^2+x^3)^2, x) \\ \downarrow & & \downarrow \\ (1+x^2-x^3)^2 & \longmapsto & (1+x^2+x^3, -1) \end{array} \qquad \begin{array}{ccc} v & \longmapsto & ((-1+x^2+x^3)^3, 1) \\ \downarrow & & \downarrow \\ 1 & \longmapsto & (1,1) \end{array}$$

Moreover, it easily follows that $w = u^i v^j$ for some uniquely determined $i, j \in \mathbb{Z}$. Hence

$$\mathrm{U}(\mathbb{Z}C_{10}) = \langle -1 \rangle \times \langle x \rangle \times \langle u \rangle \times \langle v \rangle.$$

We give the units u, v explicitly (they coincide with the units given by Aleev):

$$\begin{aligned} u &= 2 + (x + x^5 + x^9) - (x^2 + x^3 + x^7 + x^8), \\ u^{-1} &= 2 + (x^3 + x^5 + x^7) - (x + x^4 + x^6 + x^9), \\ v &= -3 - 4x^5 - (x + x^4 + x^6 + x^9) + 3(x^2 + x^3 + x^7 + x^8), \\ v^{-1} &= -3 - 4x^5 - (x^2 + x^3 + x^7 + x^8) + 3(x + x^4 + x^6 + x^9). \end{aligned}$$

Aleev's calculations take place in the complex group ring, but it seems to be more convenient to work in the rational group ring. We make some additional comments. Identify $\mathbb{Q}C_{10}$ with its Wedderburn decomposition,

$$\begin{aligned} \mathbb{Q}C_{10} &= \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(\zeta_5) \oplus \mathbb{Q}(\zeta_5), \quad \zeta_5 = \exp(2\pi i/5), \\ x &= (1, -1, \zeta_5, -\zeta_5). \end{aligned}$$

Then $\mathbb{Z}C_{10}$ is contained in the maximal order

$$M = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}[\zeta_5] \oplus \mathbb{Z}[\zeta_5].$$

For a cyclic group C, Künzer and Weber [83, Corollary 5.8] calculated the index of $\mathbb{Z}C$ in the maximal order of $\mathbb{Q}C$. The index of $\mathbb{Z}C_{10}$ in M is $2^5 \cdot 5^2$; in fact, we have

$$M/\mathbb{Z}C_{10} \cong (\mathbb{Z}/2\mathbb{Z})^{(5)} \oplus (\mathbb{Z}/5\mathbb{Z})^{(2)} \quad \text{as additive groups.}$$

Let us compute the index of $\mathrm{U}(\mathbb{Z}C_{10})$ in $\mathrm{U}(M)$. Since

$$1+\zeta_{10}^2-\zeta_{10}^3=-\omega^{-1} \quad \text{and} \quad -1+\zeta_5^2+\zeta_5^3=-\omega^2,$$

it follows that

$$u=(1,-1,\omega^4,\omega^{-2}) \quad \text{and} \quad v=(1,1,-\omega^6,1).$$

From that, we easily obtain Corollary 4 of [1]. Namely, if ϕ_i denotes the natural map from $\mathrm{V}(\mathbb{Z}C_{10})$ to the unit group of the i-th component of $\mathbb{Q}C_{10}$ (in the given order), then

$$\begin{aligned}
&\ker(\phi_2)=\langle x^2\rangle\times\langle xu\rangle\times\langle v\rangle\cong C_5\times C_\infty\times C_\infty,\\
&\ker(\phi_3)=\langle x^5\rangle\times\langle u^3v^{-2}\rangle\cong C_2\times C_\infty, \quad \operatorname{coker}(\phi_3)\cong C_2\times C_2,\\
&\ker(\phi_4)=\langle v\rangle\cong C_\infty, \quad \operatorname{coker}(\phi_4)\cong C_2.
\end{aligned}$$

From that, it has been deduced in [1, Corollary 4] that $l=2$ is the least natural number such that $\mathrm{U}(M)^l\subseteq\mathrm{U}(\mathbb{Z}C_{10})$. However, this is not correct; we have

$$Q:=\mathrm{U}(M)/\mathrm{U}(\mathbb{Z}C_{10})\cong C_4\times C_4\times C_3\times C_5.$$

(Check that $Q=\langle\bar y_1,\bar y_2,\bar y_3\rangle$ with $y_1=(1,1,\omega,1)$, $y_2=(1,1,\omega^{-2},\omega)$ and $y_3=(1,1,1,\zeta)$. If $\bar y_1^a\bar y_2^b\bar y_3^c\in\mathrm{U}(\mathbb{Z}C_{10})$ for $a,b,c\in\mathbb{Z}$, then $12\mid a$, $4\mid b$ and $5\mid c$.)

In particular, the index of $\mathrm{U}(\mathbb{Z}C_{10})$ in $\mathrm{U}(M)$ is $2^4\cdot3\cdot5=240$ and the smallest number l with $\mathrm{U}(M)^l\subseteq\mathrm{U}(\mathbb{Z}C_{10})$ is $l=60$.

On vanishing sums of roots of unity

Lam and Leung [84] solved the following problem in number theory: Given a natural number m, what are the possible integers n for which there exist mth roots of unity $\alpha_1,\dots,\alpha_n\in\mathbb{C}$ such that $\alpha_1+\dots+\alpha_n=0$? (Such an equation is said to be a *vanishing sum* of mth roots of unity of *weight* n.)

We will put the crucial results from [84] into a more general context. Our results are stated entirely in the language of group rings, since we use Lemma 7.2 to dispense with some linear disjointness arguments from [84].

If m has prime factorization $p_1^{a_1}\dots p_r^{a_r}$ $(a_i>0)$, then it is easy to see that any linear combination of $p_1,\dots,p_r$ with non-negative integer coefficients occurs as weight of some vanishing sum of mth roots of unity. Lam and Leung [84] proved the converse:

7.4 Theorem (Lam, Leung). *For any $m=p_1^{a_1}\dots p_r^{a_r}$ as above, the set of weights of vanishing sums of mth roots of unity is exactly given by $\mathbb{N}_0p_1+\dots+\mathbb{N}_0p_r$.*

The key technique used for the proof is that of group rings; in fact, group rings provide a very natural setting for studying linear relations among roots of unity, as was demonstrated in [84].

To be more precise, let $G = \langle z \rangle$ be a cyclic group of order m, and let ζ be a (fixed) primitive mth root of unity. Let $\varphi : \mathbb{Z}G \to \mathbb{Z}[\zeta]$ be the natural homomorphism given by $\varphi(z) = \zeta$. Then the elements of $\ker(\varphi)$ correspond precisely to all $\mathbb{Z}$-linear relations among the mth roots of unity. For vanishing sums of mth roots of unity, we have to look at $\mathbb{N}_0 G \cap \ker(\varphi)$. If $x \in \mathbb{N}_0 G \cap \ker(\varphi)$, the weight of the corresponding vanishing sum of mth roots of unity is exactly the augmentation $\varepsilon(x)$.

Note that an element x of $\mathbb{Z}G$ lies in $\ker(\varphi)$ if and only if $\chi(x) = 0$ for each faithful irreducible character χ of G. Thus, if $m = p_1^{a_1} \dots p_r^{a_r}$ as above, and N_i is the subgroup of G of order p_i, then $x \in \ker(\varphi)$ if and only if $fx = 0$, where f is the idempotent $\prod_{i=1}^{r}(1 - \epsilon_{N_i})$. Lemma 7.2 now yields the following theorem, called the Rédei–de Bruin–Schoenberg theorem in [84, Section 2]. As noted in [84], it gives a natural family of ideal generators of $\ker(\varphi)$, which is just the principal ideal generated by the mth cyclotomic polynomial.

7.5 Theorem. *With notation as above, we have* $\ker(\varphi) = \sum_{i=1}^{r} \mathbb{Z}G \cdot \hat{N}_i$.

However, this does not imply Theorem 7.4 directly (by taking augmentation, see [84, Remark 5.3]) unless $r \leq 2$ (see Proposition 7.7). What follows from Theorem 7.5 is that all sufficiently large integers occur as weights of vanishing sums of mth roots of unity, by the following elementary number-theoretic fact:

7.6 Lemma. *Let p, q be relatively prime positive integers. If n is an integer satisfying $n \geq (p-1)(q-1)$, then $n \in \mathbb{N}_0 p + \mathbb{N}_0 q$.*

Proof. Write $n = sp + tq$ with $s, t \in \mathbb{Z}$. Adding vq to s and subtracting vp from t, for suitable $v \in \mathbb{Z}$, we may assume that $0 \leq s < q$. Then $(p-1)(q-1) \leq n \leq (q-1)p + tq$, which implies that $-q + 1 \leq tq$, and $t \in \mathbb{N}_0$. □

To give an idea of the proof of Theorem 7.4, we introduce the following notions. Let G be an arbitrary finite group, and $N_1, \dots, N_r \trianglelefteq G$. We say that a nonzero element of $\mathbb{N}_0 G \cap \sum_{i=1}^{r} \mathbb{Z}G \cdot \hat{N}_i$ is *minimal* if it cannot be decomposed into a sum of two nonzero elements in $\mathbb{N}_0 G \cap \sum_{i=1}^{r} \mathbb{Z}G \cdot \hat{N}_i$. An element of $\sum_{i=1}^{r} \mathbb{N}_0 G \cdot \hat{N}_i$ will be called *symmetric*.

If G is cyclic of order m, the subgroups $N_1, \dots, N_r$ are chosen as above, and $p_1 < p_2 < \dots < p_r$, then Lam and Leung showed that if $x \in \mathbb{N}_0 G \cap \sum_{i=1}^{r} \mathbb{Z}G \cdot \hat{N}_i$ is minimal, then x is either symmetric, or we will have $r \geq 3$ and $\varepsilon(x) > (p_1 - 1)(p_2 - 1)$ (which clearly implies their principal result on vanishing sums). Theorem 7.11 below generalizes this result.

From now on, G will denote an arbitrary finite group.

The following proposition generalizes [84, Theorem 3.3], and will set the stage for the inductive proof of Theorem 7.10.

7.7 Proposition. *Let A and B be normal subgroups of G with $A \cap B = 1$. Then*

$$\mathbb{N}_0 G \cap (\mathbb{Z}G \cdot \hat{A} + \mathbb{Z}G \cdot \hat{B}) = \mathbb{N}_0 G \cdot \hat{A} + \mathbb{N}_0 G \cdot \hat{B}.$$

Proof. We need only prove the inclusion $\subseteq$. Let $w \in \mathbb{N}_0G \cap (\mathbb{Z}G\cdot\hat{A}+\mathbb{Z}G\cdot\hat{B})$. We wish to show that $w \in \mathbb{N}_0G\cdot\hat{A}+\mathbb{N}_0G\cdot\hat{B}$, and proceed by induction on the augmentation $\varepsilon(w)$ of w. We have $\varepsilon(w)=0$ if and only if $w=0$, so we can assume that $w\neq 0$. We can write $w=x+y$ with $x\in\mathbb{Z}G\cdot\hat{A}$, $y\in\mathbb{Z}G\cdot\hat{B}$ such that $|\mathrm{supp}(x)|+|\mathrm{supp}(y)|$ is minimal. Write $x=\sum_{g\in G}x_gg$ with integer coefficients x_g, and likewise for other group ring elements. Choose $h\in G$ such that $x_h\geq x_g$ for all $g\in G$. Reversing roles of A and B, if necessary, we may assume that $x_h>0$. Set $w'=w-h\hat{A}$. By way of contradiction, we will show $w'\in\mathbb{N}_0G$. So assume that there is $k\in A$ with $w'_{hk}<0$. Since $w'_{hk}=w_{hk}-1\geq -1$, it follows that $w_{hk}=0$, that is, $y_{hk}=-x_{hk}$. Note that for any $g\in G$, we have $x_{ga}=x_g$ for all $a\in A$ and $y_{gb}=y_g$ for all $b\in B$. Take any $b\in B$. Then $-x_h=-x_{hk}=y_{hk}=y_{hkb}$, so $x_{hkb}-x_h=x_{hkb}+y_{hkb}\geq 0$, and $x_{hkb}=x_h$ by assumption on h. It follows that

$$x=\underbrace{x_{hk}h\hat{A}\hat{B}}_{\in\mathbb{Z}G\cdot\hat{B}}+\underbrace{\sum_{g\notin h\hat{A}\hat{B}}x_gg}_{\in\mathbb{Z}G\cdot\hat{A}},\qquad y=-x_{hk}hk\hat{B}+\underbrace{\sum_{g\notin hk\hat{B}}y_gg}_{\in\mathbb{Z}G\cdot\hat{B}}.$$

Thus, if we set $x'=x-x_{hk}h\hat{A}\hat{B}\in\mathbb{Z}G\cdot\hat{A}$ and $y'=y+x_{hk}h\hat{A}\hat{B}\in\mathbb{Z}G\cdot\hat{B}$, then $w=x'+y'$ with $|\mathrm{supp}(x')|=|\mathrm{supp}(x)|-|AB|$ and $|\mathrm{supp}(y')|\leq|\mathrm{supp}(y)|-|B|+(|A|-1)|B|$, contradicting our choice of the decomposition $w=x+y$. We have shown that $w'\in\mathbb{N}_0G$. Since $\varepsilon(w')<\varepsilon(w)$, we may assume inductively that $w'\in\mathbb{N}_0G\cdot\hat{A}+\mathbb{N}_0G\cdot\hat{B}$, and then also $w=w'+h\hat{A}\in\mathbb{N}_0G\cdot\hat{A}+\mathbb{N}_0G\cdot\hat{B}$, as desired. □

The next lemma generalizes [84, Theorem 3.1].

7.8 Lemma. *Let $N_1,\dots,N_r\trianglelefteq G$, with N_j and N_k of coprime order for all $j\neq k$. Set $N=N_1N_2\cdots N_r$, and let $g_1,\dots,g_s$ be a complete system of coset representatives of N in G. Then*

$$\mathbb{N}_0G\cap\sum_{i=1}^{r}\mathbb{Z}G\cdot\hat{N}_i=\sum_{j=1}^{s}g_j\Big(\mathbb{N}_0N\cap\sum_{i=1}^{r}\mathbb{Z}N\cdot\hat{N}_i\Big).$$

Proof. We need only prove the inclusion $\subseteq$. Let $x\in\mathbb{N}_0G\cap\sum_i\mathbb{Z}G\cdot\hat{N}_i$, and write $x=\sum_j g_jx_j$ with $x_j\in\mathbb{Z}N$. Then $x_j\in\mathbb{N}_0N$ for all j. Let, as in the proof of Theorem 7.1, f be the idempotent $\prod_i(1-\epsilon_{N_i})$. Then $\sum_j g_j(x_jf)=xf=0$ implies that $x_jf=0$ for all j, so $x_j\in\sum_i\mathbb{Z}N\cdot\hat{N}_i$ by Lemma 7.2. This completes the proof. □

We can define a partial ordering on $\mathbb{Z}G$, by declaring that $y\geq x$ if $y-x\in\mathbb{N}_0G$. We will need a technical lemma, the proof of which closely follows the proof of [84, Theorem 4.1].

7.9 Lemma. *Let $N=N_1\times N_2\times\cdots\times N_r$ be the direct product of groups N_i of order n_i such that $n_1<n_2<\cdots<n_r$ and $(n_j,n_k)=1$ for all $j\neq k$. Let $x,y\in\mathbb{N}_0N$ such that $x-y\in\sum_{i=1}^{r}\mathbb{Z}N\cdot\hat{N}_i$. If $|\mathrm{supp}(x)|\leq n_1$, then we have either* (A) *$y\geq x$ or* (B)

$|\mathrm{supp}(y)| \geq (n_1 - |\mathrm{supp}(x)|)(n_2 - 1)$. *In Case* (A), *we have* $|\mathrm{supp}(y)| \geq |\mathrm{supp}(x)|$, *and in Case* (B), *we have* $|\mathrm{supp}(y)| > |\mathrm{supp}(x)|$.

Proof. The last statement in the theorem follows since, in Case (B), we will have

$$|\mathrm{supp}(y)| \geq (n_1 - |\mathrm{supp}(x)|)(n_2 - 1) \geq n_2 - 1 > n_1 - 1 \geq |\mathrm{supp}(x)|.$$

The proof of the theorem will be by induction on $r \geq 2$. Set $M = N_1 \cdots N_{r-1}$. There are unique expressions

$$x = \sum_{g \in N_r} x_g g, \qquad y = \sum_{g \in N_r} y_g g,$$

where $x_g, y_g \in \mathbb{N}_0 M$. Set $I = \{g \mid x_g = 0\}$. This is a nonempty set, since $|\mathrm{supp}(x)| \leq n_1 - 1 < n_r$. In the set $\{y_g \mid g \in I\}$, choose y_h such that $|\mathrm{supp}(y_h)|$ is the smallest. Set $f = \prod_{i=1}^{r-1}(1 - \epsilon_{N_i})$ and $f_r = 1 - \epsilon_{N_r}$. From the hypothesis $x - y \in \sum_i \mathbb{Z}N \cdot \hat{N}_i$, we have $f_r f(x - y) = 0$, that is, $f(x - y) \in \mathbb{Q}M \cdot \hat{N}_r$, and consequently $f(x_g - y_g) = f(x_h - y_h)$ for all $g \in N_r$. Since $x_h = 0$, equivalently

$$f y_g = f(x_g + y_h). \tag{1}$$

Choose k such that $|\mathrm{supp}(x_k)|$ is maximum (among all $|\mathrm{supp}(x_g)|$'s). We shall distinguish the following two main cases.

Case 1 $|\mathrm{supp}(x_k)| + |\mathrm{supp}(y_h)| \geq n_1$. Let $t := n_r - |I|$, which is the number of nonzero x_g's. We may assume that $t \geq 1$, for otherwise $x = 0$ and $y \geq x$ holds. Note the following obvious upper and lower bounds on $|\mathrm{supp}(x)|$:

$$|\mathrm{supp}(x_k)| + t - 1 \leq |\mathrm{supp}(x)| \leq |\mathrm{supp}(x_k)|t.$$

Using the definition of y_h, we have

$$\begin{aligned}
|\mathrm{supp}(y)| &\geq |I| \cdot |\mathrm{supp}(y_h)| = (n_r - t)|\mathrm{supp}(y_h)| \\
&\geq (n_2 - t)(n_1 - |\mathrm{supp}(x_k)|) \\
&= n_1 n_2 - t n_1 - |\mathrm{supp}(x_k)|n_2 + |\mathrm{supp}(x_k)|t \\
&= n_1 n_2 + t(n_2 - n_1) - n_2 - (|\mathrm{supp}(x_k)| + t - 1)n_2 + |\mathrm{supp}(x_k)|t \\
&\geq n_1 n_2 + (n_2 - n_1) - n_2 - |\mathrm{supp}(x)|n_2 + |\mathrm{supp}(x)| \\
&= (n_1 - |\mathrm{supp}(x)|)(n_2 - 1),
\end{aligned}$$

so we have proved (B) in this case.

Case 2 $|\mathrm{supp}(x_k)| + |\mathrm{supp}(y_h)| \leq n_1 - 1$. This case assumption means that $|\mathrm{supp}(x_g)| + |\mathrm{supp}(y_h)| \leq n_1 - 1$ for all $g \in N_r$. We shall first take care of the case $r = 2$ (to start the induction). In this case, $M = N_1$ and $f = 1 - \epsilon_M$, so by (1),

$$\text{for all } g \in N_2, \quad y_g = x_g + y_h + z_g \hat{M} \quad \text{for some } z_g \in \mathbb{Z}. \tag{2}$$

If some $z_g < 0$, then $x_g + y_h = y_g + |z_g|\hat{M}$ implies that $|\mathrm{supp}(x_g)| + |\mathrm{supp}(y_h)| \geq |\mathrm{supp}(x_g + y_h)| = n_1$, a contradiction. Therefore, we must have $z_g \geq 0$ for all $g \in N_2$. It follows from (2) that $y_g \geq x_g$ for all $g \in N_2$, and hence $y \geq x$ in this case.

Assume now $r \geq 3$. Note that (1) is equivalent to

$$(x_g + y_h) - y_g \in \sum_{i=1}^{r-1} \mathbb{Z}M \cdot \hat{N}_i,$$

by Lemma 7.2. Since $|\mathrm{supp}(x_g + y_h)| \leq |\mathrm{supp}(x_g)| + |\mathrm{supp}(y_h)| \leq n_1 - 1$, we can apply the inductive hypothesis to the pair y_g and $x_g + y_h$ in $\mathbb{N}_0 M$. In particular, we will have

$$|\mathrm{supp}(y_g)| \geq |\mathrm{supp}(x_g + y_h)| \quad \text{for all } g \in N_r. \tag{3}$$

If $y_g \geq x_g + y_h$ for all $g \in N_r$, then $y_g \geq x_g$ for all $g \in N_r$, and we have $y \geq x$, proving (A) in this case. Otherwise, our inductive hypothesis implies that there exists an $l \in N_r$ such that

$$|\mathrm{supp}(y_l)| \geq (n_1 - |\mathrm{supp}(x_l + y_h)|)(n_2 - 1).$$

Note that, from (3), $|\mathrm{supp}(y_g)| \geq |\mathrm{supp}(y_h)|$ for all $g \in N_r$. Using this, we have

$$\begin{aligned} |\mathrm{supp}(y)| &= |\mathrm{supp}(y_l)| + \sum_{g \in N_r \setminus \{l\}} |\mathrm{supp}(y_g)| \\ &\geq (n_1 - |\mathrm{supp}(x_l + y_h)|)(n_2 - 1) + (n_r - 1)|\mathrm{supp}(y_h)| \\ &\geq (n_1 - |\mathrm{supp}(x_l)|)(n_2 - 1) + (n_r - n_2)|\mathrm{supp}(y_h)| \\ &\geq (n_1 - |\mathrm{supp}(x)|)(n_2 - 1), \end{aligned}$$

proving (B) in this case. □

As in [84], we are now ready to establish a lower bound theorem for the augmentation of the non-symmetric minimal elements in $\mathbb{N}_0 G \cap \sum_{i=1}^{r} \mathbb{Z}G \cdot \hat{N}_i$. The proof closely follows the proof of [84, Theorem 4.8]. As in [84, Section 6], the theorem could be used to give more precise information on the non-symmetric minimal elements of smallest augmentation, but we will not pursue these ideas any further.

7.10 Theorem. *Let $N_1, N_2, \ldots, N_r$ be normal subgroups of G, with N_i of order n_i, such that $(n_j, n_k) = 1$ for all $j \neq k$ and $n_1 < n_2 < \cdots < n_r$. For any minimal element $x \in \mathbb{N}_0 G \cap \sum_{i=1}^{r} \mathbb{Z}G \cdot \hat{N}_i$, we have either* (A) *$x$ is symmetric, or* (B) *$r \geq 3$ and $\varepsilon(x) \geq |\mathrm{supp}(x)| \geq n_1(n_2 - 1) + n_3 - n_2 \geq n_3$.*

Proof. By Lemma 7.8, we may assume that $G = N$. The proof will be again by induction on r. In the case $r = 2$, Proposition 7.7 implies that x is necessarily symmetric, so (A) always holds in this case. This starts the induction, and we may now proceed to the case $r \geq 3$.

Write $x = \sum_{g\in N_r} x_g g$ as in the proof of Lemma 7.9, where $x_g \in \mathbb{N}_0 M$ and $M = N_1 \cdots N_{r-1}$. Since $x \in \sum_i \mathbb{Z}N \cdot \hat{N}_i$, it follows as in the proof of Lemma 7.9 that $fx_{g_1} = fx_{g_2}$ for all $g_1, g_2 \in N_r$, where $f = \prod_{i=1}^{r-1}(1 - \epsilon_{N_i})$. Choose h such that $|\mathrm{supp}(x_h)|$ is the smallest. We shall argue in the following three cases.

Case 1 $|\mathrm{supp}(x_h)| \geq n_1$. In this case, we have

$$\begin{aligned}|\mathrm{supp}(x)| &\geq |\mathrm{supp}(x_h)|n_r \geq n_1 n_3 = n_1(n_2 + n_3 - n_2)\\ &> n_1 n_2 + n_3 - n_2 > n_1(n_2 - 1) + n_3 - n_2.\end{aligned}$$

Case 2 $|\mathrm{supp}(x_h)| = 0$. This means that $x_h = 0$, so we have $fx_g = fx_h = 0$ for all $g \in N_r$, i.e., $x_g \in \mathbb{N}_0 M \cap \sum_{i=1}^{r-1} \mathbb{Z}M \cdot \hat{N}_i$ by Lemma 7.2. Since x is minimal, we must have $x = x_k k$ for some $k \in N_r$, with x_k necessarily minimal in $\mathbb{N}_0 M \cap \sum_{i=1}^{r-1} \mathbb{Z}M \cdot \hat{N}_i$. Invoking the inductive hypothesis, x_k is either symmetric, or we have $r - 1 \geq 3$ and $|\mathrm{supp}(x)| = |\mathrm{supp}(x_k)| \geq n_1(n_2 - 1) + n_3 - n_2$, as desired.

Case 3 We may assume now that $1 \leq |\mathrm{supp}(x_h)| \leq n_1 - 1$. Note that $f(x_{g_1} - x_{g_2}) = 0$ implies that $x_{g_1} - x_{g_2} \in \mathbb{N}_0 M \cap \sum_{i=1}^{r-1} \mathbb{Z}M \cdot \hat{N}_i$, by Lemma 7.2. By Lemma 7.9 (applied to the elements $x_h, x_g \in \mathbb{N}_0 M$, where g ranges over the elements of N_r), we have the following two possibilities:

Subcase 1 $x_g \geq x_h$ for all $g \in N_r$. In this case,

$$x = \sum_{g\in N_r} x_g g \geq \sum_{g\in N_r} x_h g = x_h \hat{N}_r.$$

Since x is minimal, we must have $x = x_h \hat{N}_r$ and $x_h \in M$, so x is symmetric in this case.

Subcase 2 There exists $l \in N_r$ such that $|\mathrm{supp}(x_l)| \geq (n_1 - |\mathrm{supp}(x_h)|)(n_2 - 1)$. In this case,

$$\begin{aligned}|\mathrm{supp}(x)| &= |\mathrm{supp}(x_l)| + \sum_{g\in N_r\setminus\{l\}} |\mathrm{supp}(x_g)|\\ &\geq (n_1 - |\mathrm{supp}(x_h)|)(n_2 - 1) + (n_r - 1)|\mathrm{supp}(x_h)|\\ &= n_1(n_2 - 1) + (n_r - n_2)|\mathrm{supp}(x_h)|\\ &\geq n_1(n_2 - 1) + n_r - n_2\\ &\geq n_1(n_2 - 1) + n_3 - n_2.\end{aligned}$$

In any case, we have shown that either (A) or (B) holds. (For the last inequality in (B), note that $n_1(n_2 - 1) + n_3 - n_2 = n_1 n_2 - n_2 - n_1 + n_3 \geq (n_2 - n_1) + n_3 \geq n_3$.) □

The following theorem immediately implies Theorem 7.4, as explained above.

7.11 Theorem. *Let $N_1, \ldots, N_r$ be normal subgroups of G which are of pairwise coprime order. Then for any $x \in \mathbb{N}_0 G \cap \sum_{i=1}^{r} \mathbb{Z}G \cdot \hat{N}_i$, we have $\varepsilon(x) \in \sum_{i=1}^{r} \mathbb{N}_0 |N_i|$.*

Proof. Clearly, we may assume that $r \geq 2$. Since x can be decomposed into minimal elements in $\sum_i \mathbb{Z}G \cdot \hat{N}_i$, it suffices to prove the theorem for minimal elements x. By Theorem 7.10, either x is symmetric, or we will have $r \geq 3$ and $\varepsilon(x) \geq n_1(n_2-1)+n_3-n_2$, where $n_i = |N_i|$ and the normal subgroups N_i are suitably arranged. In the former case, $\varepsilon(x) = n_i$ for some i. In the latter case,

$$\varepsilon(x) > n_1(n_2 - 1) > (n_1 - 1)(n_2 - 1),$$

and Lemma 7.6 implies that $\varepsilon(x) \in \mathbb{N}_0\, n_1 + \mathbb{N}_0\, n_2 \subseteq \sum_{i=1}^{r} \mathbb{N}_0\, |N_i|$. □

8. Semilocal counterexamples

In this section, we present three semilocal counterexamples to the Zassenhaus conjecture: We will construct group ring automorphisms in the semilocal case, i.e., group ring automorphisms of $\mathbb{Z}_{\pi(G)}G$, which do not have a Zassenhaus factorization, i.e., which do not differ from a group automorphism by a central automorphism.

The examples include a metabelian A-group G, a supersolvable group G and a Frobenius group G.

Following Scott [127, Section 2], we will avoid any explicit use of the theory of orders. We merely construct a single group automorphism σ of G which acts in a prescribed way on the irreducible characters of G, and show that if some other automorphism ρ of G acts in the same way, then either ρ or $\rho\sigma$ moves certain characters.

Therefore we are asking for useful criteria for when a group automorphism σ of G fixes some character χ of G. If for any $g \in G$, either g and $g\sigma$ are conjugate or $\chi(g) = 0 = \chi(g\sigma)$, then clearly $\chi^\sigma = \chi$. On the other hand, we know of certain instances when character values are zero.

Roggenkamp and Scott [117] used the following well known criterion.

8.1 Proposition. *Let $\chi \in \mathrm{Irr}(G)$, $N \trianglelefteq G$, and let $\psi \in \mathrm{Irr}(N)$ be a constituent of $\chi|_N$. Let $G_\psi = \{x \in G \mid \psi^x = \psi\}$ be the inertia group of ψ. Then $x^G \cap G_\psi = \emptyset$ for some $x \in G$ implies that $\chi(x) = 0$.*

Proof. By Clifford's theorem, χ is induced from some character $\eta \in \mathrm{Irr}(G_\psi)$ (see [28, (11.4)]). □

The following criterion is particularly easy to verify. A proof using the Second Orthogonality Relation is given in [28, exercise 9.15].

8.2 Proposition. *Let $N \trianglelefteq G$, let $x \in G$ with $\mathrm{C}_G(x) \cap N = 1$, and let $\chi \in \mathrm{Irr}(G)$ with $N \not\leq \ker(\chi)$. Then $\chi(x) = 0$.*

Proof. This follows from $|N| \cdot \chi(x) = \chi(\sum_{n\in N} x^n) = \chi(x \cdot \sum_{n\in N} n) = 0$. □

As a corollary, we obtain

8.3 Corollary. *Let G be a Frobenius group with Frobenius kernel F, and let $\sigma \in \mathrm{Aut}(G)$. Then $\chi^\sigma = \chi$ holds for every character $\chi \in \mathrm{Irr}(G)$ with $F \not\leq \ker(\chi)$ if and only if $g\sigma$ is conjugate to g for all $g \in F$.* □

8.4 Example. (Affine semi-linear groups.) Let F be a finite field. Write $F^\times$ for its group of units, and V for F, if considered as an additive group only. Let ϕ be the Frobenius automorphism of F. The affine semi-linear group is the semidirect product

$$S = V \rtimes F^\times \rtimes \langle \phi \rangle.$$

We have a homomorphism $\theta : F^\times \to F^\times$, $m \mapsto (m\phi)m^{-1}$. Let $U \leq F^\times$ with $F^\times\theta \leq U$. Then $G = V \rtimes U \leq S$ is a Frobenius group with Frobenius kernel V. Conjugation with $\phi \in S$ induces an automorphism $\sigma \in \mathrm{Aut}(G)$, and by choice of U, the elements $v\sigma$ and v are conjugate for all $v \in V$. Thus σ fixes each irreducible character of G which does not contain V in its kernel, by Corollary 8.3.

The next lemma shows that given certain non-conjugate group elements lying in a product MN of normal subgroups M and N of G, there is an irreducible character of G which takes different values on the group elements and which does not have one of the subgroups M and N in its kernel. We will apply the lemma in the examples below. A similar result, together with a different proof, is given in [60, Lemma 2.4].

8.5 Lemma. *Let $M, N \trianglelefteq G$ with $M \cap N = 1$. Suppose that there are given elements $u, v \in MN$ which are not conjugate in G, and that $|\mathrm{C}_G(u)| = |\mathrm{C}_G(v)|$. Assume further that of both of these elements, not one is contained in M and the other in N. Then there exists $\chi \in \mathrm{Irr}(G)$ such that $M, N \not\leq \ker(\chi)$ and $\chi(u) \neq \chi(v)$.*

Proof. We shall use that by the Second Orthogonality Relation, for a finite group X and elements $s, t \in X$ that are not conjugate in X, we have

$$\sum_{\chi \in \mathrm{Irr}(G)} |\chi(s) - \chi(t)|^2 = |\mathrm{C}_X(s)| + |\mathrm{C}_X(t)|.$$

Furthermore, given $x \in X$ and $Y \trianglelefteq X$ such that x is conjugate to xy (in X) for exactly k elements $y \in Y$, we have

$$|\mathrm{C}_{X/Y}(\overline{x})| = \frac{k}{|Y|}|\mathrm{C}_X(x)|.$$

Now assume that the assertion of the lemma does not hold. Then

$$2|\mathrm{C}_G(u)| = \sum_{\chi \in \mathrm{Irr}(G/M)} |\chi(\overline{u}) - \chi(\overline{v})|^2 + \sum_{\chi \in \mathrm{Irr}(G/N)} |\chi(\overline{u}) - \chi(\overline{v})|^2, \qquad (*)$$

and none of the sums on the right hand side vanish. To estimate the first sum, let

$$|\mathrm{C}_{G/M}(\overline{u})| = \frac{k_1}{|M|}|\mathrm{C}_G(u)|, \quad |\mathrm{C}_{G/M}(\overline{v})| = \frac{k_2}{|M|}|\mathrm{C}_G(u)|.$$

Since $\overline{u}$ and $\overline{v}$ are not conjugate in G/N, we have $k_1 + k_2 \leq |M|$, and if this is an equality, then either $u \in N$ or $v \in N$. The second sum can be treated similarly. Since $(*)$ is an equality, we can assume without lost of generality that $u = 1$, which produces a contradiction. This proves the lemma. □

We give a typical application:

8.6 Corollary. *Let G be a Frobenius group, and assume that the Frobenius kernel of G is the direct product of nontrivial normal subgroups M and N of G. Let $\sigma \in \mathrm{Aut}(G)$ with $M\sigma = M$ and $N\sigma = N$. If $\chi^\sigma = \chi$ for every $\chi \in \mathrm{Irr}(G)$ with $M, N \not\leq \ker(\chi)$, then $\sigma \in \mathrm{Aut}_{\mathrm{c}}(G)$.*

Proof. By Lemma 8.5, we have that $x\sigma$ is conjugate to x, for all $x \in MN$. Choose $n_0 \in \mathrm{Z}(N) \setminus \{1\}$, and $g \in G$ with $n_0\sigma = n_0^g$. Then for any $m \in \mathrm{Z}(M)$, there is $h \in G$ with $n_0^g(m\sigma) = (n_0 m)\sigma = n_0^h m^h$, and since G is a Frobenius group, we may choose $h = g$. Thus we can assume that $m\sigma = m$ for all $m \in \mathrm{Z}(M)$. Then $g\sigma \in g\mathrm{C}_G(\mathrm{Z}(M)) = gMN$ for all $g \in G$, and therefore $\sigma \in \mathrm{Aut}_{\mathrm{c}}(G)$ by Corollary 8.3. □

Let us recall the following proposition, which is a consequence of Proposition 1.5 (cf. [54, Proposition 2.1.3]).

8.7 Proposition. *Assume that G has nontrivial normal subgroups M and N of coprime order, and that some $\sigma \in \mathrm{Aut}(G)$ with $(MN)\sigma = MN$ satisfies the following conditions:*

1. *The automorphism of G/MN induced by σ is not class-preserving;*
2. *σ fixes each irreducible character of G which has exactly one of the normal subgroups M and N in its kernel;*
3. *If another automorphism ρ of G satisfies the above conditions (which are fulfilled by σ), then one of the following hold:*
   - *ρ moves some irreducible character of G which does not has M in its kernel;*
   - *The automorphism of G/M induced by $\rho\sigma$ is not class-preserving.*

Let S be a semilocal Dedekind ring of characteristic 0. Then SG has an augmentation-preserving automorphism α which has no Zassenhaus factorization, i.e., there is no $\rho \in \mathrm{Aut}(G)$ such that $\rho\alpha$ is a central automorphism of SG.

Proof. Let P be a prime ideal of S. If $|M| \notin P$, then $S_PG = \epsilon_M S_PG \oplus \eta_M S_PG$ (where $\epsilon_M = \frac{1}{|M|}\sum_{m\in M} m$ and $\eta_M = 1 - \epsilon_M$), and an automorphism $\alpha(P)$ of S_PG is defined as follows: $\alpha(P)$ fixes $\epsilon_M S_PG$ element-wise, and agrees with σ on $\eta_M S_PG$. Otherwise $|N| \notin P$, and $\alpha(P)$ is defined correspondingly, using the normal subgroup N instead of M. By Proposition 1.5, there is an automorphism α of SG which agrees with each $\alpha(P)$ up to an inner automorphism of S_PG. The third condition precisely says that α has no Zassenhaus factorization. □

We are now ready to produce semilocal counterexamples to the Zassenhaus conjecture with relatively minor effort.

8.8 Example (A metabelian A-Group). A metabelian group G having abelian Sylow subgroups and a Sylow tower, $|G| = 2^2 \cdot 3^2 \cdot 5$, is presented such that SG, where $S = \mathbb{Z}_{\pi(G)}$, has an augmentation-preserving automorphism without Zassenhaus factorization.

Let $X = \langle x\rangle \cong C_4$, $M = \langle s, t\rangle \cong C_3 \times C_3$ and $N = \langle n\rangle \cong C_5$. Then G is the semidirect product $G = (M \times N) \rtimes X$ where $s^x = t$, $t^x = s^2$ and $n^x = n^{-1}$.

An automorphism $\sigma \in \mathrm{Aut}(G)$ is defined by $x\sigma = x^3$, $s\sigma = s$, $t\sigma = t^2$ and $n\sigma = n$. (In fact, x operates on M via the matrix $\left[\begin{smallmatrix}0 & 1\\ 2 & 0\end{smallmatrix}\right]$, which is inverted by the matrix $\left[\begin{smallmatrix}1 & 0\\ 0 & 2\end{smallmatrix}\right]$.)

Obviously, σ induces on G/MN an automorphism which is not class-preserving. Since m is conjugate to $m\sigma$ for all $m \in M$, it follows from Proposition 8.2 that σ fixes each irreducible character of G which has exactly one of the normal subgroups M and N in its kernel.

Assume that some $\rho \in \mathrm{Aut}(G)$ fixes each faithful irreducible character of G; we will show that ρ is an inner automorphism. By Lemma 8.5, each element a of MN is conjugate to its image $a\rho$. Thus we may assume that $n\rho = n$. Then for each $m \in M$, we have $m\rho = m^g$ for some $g \in \mathrm{C}_G(n)$ since $(m\rho)n$ is conjugate to mn, i.e., either $m\rho = m$ or $m\rho = m^{-1}$. This means that either $\rho|_M = \mathrm{id}$ or $\rho|_M = \mathrm{conj}(x^2)$, so that we can assume that $\rho|_{MN} = \mathrm{id}$. Furthermore, we can assume that $X\rho = X$, and since X acts faithfully on M, it follows that $\rho = \mathrm{id}$.

Now Proposition 8.7 shows that SG has an augmentation-preserving automorphism without Zassenhaus factorization.

It should be remarked that in [60, Theorem B], a group of order $2^4 \cdot 3 \cdot 5^2$, with abelian Sylow subgroups and a Sylow tower, is given for which the Zassenhaus conjecture does not hold.

8.9 Example (A supersolvable group). A supersolvable group G of order $2^3 \cdot 3^2 \cdot 5$ is presented such that SG, where $S = \mathbb{Z}_{\pi(G)}$, has an augmentation-preserving automorphism without Zassenhaus factorization.

Let $Q_8 = \langle a, b\rangle$ be the quaternion group of order 8, and let $L = \langle l : l^3\rangle$, $M = \langle m : m^3\rangle$, $N = \langle n : n^5\rangle$. The group G is the semidirect product $G = (L \times M \times N) \rtimes Q_8$

where $[l,a] = [m,b] = [n,ab] = 1$, and none of the normal subgroups L, M and N is central in G.

An automorphism $\sigma \in \mathrm{Aut}(G)$ is defined by $l\sigma = l^{-1}$, and the remaining generators m, n, a, b stay fixed.

The automorphism induced on G/MN by σ is not class-preserving since the images of la and $(la)\sigma = l^{-1}a$ in G/MN are not conjugate.

We will show that σ fixes each irreducible character of G which has exactly one of the normal subgroups M and N in its kernel. Take any $\chi \in \mathrm{Irr}(G)$ with $N \le \ker(\chi)$ and $M \not\le \ker(\chi)$; we have to show $\chi(x\sigma) = \chi(x)$ for $x \in LMQ_8$. But this is obvious if $x\sigma$ is conjugate to x, and otherwise we have $x, x\sigma \notin LM\langle b\rangle$, therefore $\mathrm{C}_G(x) \cap M = 1$ and $\chi(x\sigma) = 0 = \chi(x)$ by Proposition 8.2. The corresponding statement, with roles of M and N interchanged, is verified analogously.

Finally, let ρ be an automorphism of G which also fixes each irreducible character of G which has exactly one of the normal subgroups M and N in its kernel, and assume that ρ fixes each $\chi \in \mathrm{Irr}(G)$ with $M \not\le \ker(\chi)$. Then we will show that the automorphism of G/M induced by $\rho\sigma$ is not class-preserving. Assume the contrary. Then $\rho\sigma$ induces an inner automorphism of G/MN, and we can assume that $x\rho = x$ for all $x \in Q_8$, and $l\rho = l^{-1}$. By assumption, ρ fixes each character $\chi \in \mathrm{Irr}(G)$ with $M \not\le \ker(\chi)$ or $N \not\le \ker(\chi)$. Consequently, $(mb)\rho$ is conjugate to mb and $(nab)\rho$ is conjugate to nab, which implies that $m\rho = m$ and $n\rho = n$. Hence $(lmn)\rho$ is not conjugate to lmn, contradicting Lemma 8.5.

Now Proposition 8.7 shows that SG has an augmentation-preserving automorphism without Zassenhaus factorization.

This example seems to be a really "small one", so it might be worthwhile to expand on it. The reader may have noticed that the normal subgroups L, M and N can be replaced by any cyclic subgroups of prime order so that two of them are of coprime order, thus producing a whole family of semilocal counterexamples.

We leave it (as an exercise?) to the reader to figure out what family members give rise to counterexamples to the Zassenhaus conjecture (cf. Section 10). Therefore, one should write $\mathbb{Z}G$ as a pullback as described in Theorem 7.1 (possibly involving three normal subgroups!).

8.10 Example (A Frobenius group). A Frobenius group G of order $3 \cdot 2^3 \cdot 5^2 \cdot 11^2$ is presented such that SG, where $S = \mathbb{Z}_{\pi(G)}$, has an augmentation-preserving automorphism without Zassenhaus factorization.

A Frobenius complement H of G is given by

$$H = \langle a, b, t \,:\, a^4, a^2 = b^2, b^a = b^{-1}, t^3, a^t = b^3a, b^t = a\rangle \cong Q_8 \rtimes C_3.$$

We have faithful representations $\pi_5 : H \to \mathrm{SL}(2,5)$ and $\pi_{11} : H \to \mathrm{SL}(2,11)$, given by

$$a\pi_5 = \begin{bmatrix} 0 & 4 \\ 1 & 0 \end{bmatrix}, \quad b\pi_5 = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}, \quad t\pi_5 = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix},$$

$$a\pi_{11} = \begin{bmatrix} 4 & 6 \\ 10 & 7 \end{bmatrix}, \quad b\pi_{11} = \begin{bmatrix} 0 & 7 \\ 3 & 0 \end{bmatrix}, \quad t\pi_{11} = \begin{bmatrix} 5 & 7 \\ 5 & 5 \end{bmatrix}.$$

The group G is the corresponding semidirect product

$$G := \left(\mathbb{F}_5^{(2)} \oplus \mathbb{F}_{11}^{(2)}\right) \rtimes H,$$

a Frobenius group, since none of the matrices from $H\pi_i$ has eigenvalue 1.

We claim that there is $\sigma \in \mathrm{Aut}(G)$ having the following properties: g is conjugate to $g\sigma$ for each group element g from one of the normal subgroups $M := \mathbb{F}_5^{(2)}$, $N := \mathbb{F}_{11}^{(2)}$, and σ induces an automorphism of H which is not class-preserving.

First, note that $\eta \in \mathrm{Aut}(H)$, defined by $a\eta = ba$, $b\eta = b^3$ and $t\eta = t^2$, is not a class-preserving automorphism since η induces a non-inner automorphism of the cyclic quotient $\overline{H} \cong \langle t \rangle$. Furthermore, for $S_5 = \left[\begin{smallmatrix} 0 & 3 \\ 1 & 0 \end{smallmatrix}\right] \in \mathrm{GL}(2,5)$ and $S_{11} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 10 \end{smallmatrix}\right] \in \mathrm{GL}(2,11)$, we have $(h\eta)\pi_i = S_i^{-1}(h\pi_i)S_i$ for all $h \in H$ $(i = 5, 11)$. Thus there is $\sigma \in \mathrm{Aut}(G)$ extending η (meaning that $h\sigma = h\eta$ for all $h \in H$), and $(a,b)\sigma = (a,b) \cdot S_i$ for all $(a,b) \in \mathbb{F}_i^{(2)}$ $(i = 5, 11)$.

Since $|H| = 24$ and $|M| = 25$, it is obvious that $m\sigma$ is conjugate to m for all $m \in M$.

Let ζ_5 be a primitive 5th root of unity in $\mathbb{F}_{11}$. Note that no matrix from $K := \langle H\pi_{11}, S_{11} \rangle$ has eigenvalue ζ_5 (simply because $(|K|, 5) = 1$). It follows that under the action of H on $N \setminus \{1\}$, there are 5 orbits, with set of representatives $\{(\zeta_5^j, 0) \mid 0 \le j \le 4\}$ (since $5 \cdot 24 = 11^2 - 1$). Further on, $n\sigma$ is conjugate to n for all $n \in N$.

Thus σ has the desired properties. It follows that σ fixes each irreducible character of G which has exactly one of the normal subgroups M and N in its kernel, by Proposition 8.2.

Finally, if an automorphism ρ of G fixes each character $\chi \in \mathrm{Irr}(G)$ with $M, N \not\leq \ker(\chi)$, then $\rho \in \mathrm{Aut}_c(G)$ by Corollary 8.6.

Now Proposition 8.7 shows that SG has an augmentation-preserving automorphism without Zassenhaus factorization.

This example shows that Frobeniusgroups are qualified to yield semilocal counterexamples, which might come as a surprise. It is known that a weaker version of the Zassenhaus conjecture holds for Frobenius groups (see [56, Corollary 7]).

9. Group- and character table automorphisms of $(\mathbb{Z}/r\mathbb{Z}) \wr S_n$

The automorphisms of a finite Coxeter group W, its integral group ring $\mathbb{Z}W$, and the associated generic Iwahori-Hecke algebra are classified in [14] (in particular, the Zassenhaus conjecture holds for W), and in [14, p. 620] the opinion has been expressed that at least some of these results should extend to the case where W is a finite complex reflection group.

Shephard and Todd classified in [133] the finite complex reflection groups. These groups are direct products of irreducible ones, which either belong to one of two infinite

series or to a list of 34 groups. For these exceptional groups, the Zassenhaus conjecture is valid (see [63, Section 5]).

We shall calculate the group- and character table automorphisms for the groups of one of the infinite families. In particular, we show that the Zassenhaus conjecture holds for these groups. This family comprises the Coxeter groups of type B_n, and its members are the wreath products $G_{n,r} = (\mathbb{Z}/r\mathbb{Z}) \wr S_n$, for the natural action of the symmetric group S_n on the set $\{1, 2, \ldots, n\}$ (n and r are natural numbers).

The complex reflection group $G_{n,r}$ can be identified with the group of all monomial matrices of size n whose nonzero entries are rth roots of unity. We assume that $n, r > 1$, and exclude the case $n = r = 2$ ($G_{2,2}$ is the dihedral group of order 8).

Automorphisms of $(\mathbb{Z}/r\mathbb{Z}) \wr S_n$

The outer automorphism group of $G_{n,r}$ is described by the following proposition.

9.1 Proposition. *Let $G_{n,r}$ be as above. If $2 \mid r$ and $n > 2$, there is a unique central automorphism δ of $G_{n,r}$ of order 2 which fixes each element of the base group.*[1] *Let $N \leq \mathrm{Aut}(G_{n,r})$ consist of those automorphisms of $G_{n,r}$ which stabilize the base group, and fix its complement S_n element-wise. Then N is an abelian group which intersects $\mathrm{Inn}(G_{n,r})$ trivially. We have*

$$\mathrm{Out}(G_{n,r}) \cong \begin{cases} N \times \langle \delta \rangle & \text{if } 2 \mid r \text{ and } n > 2, \\ N & \text{otherwise.} \end{cases}$$

Let $N_p \leq N$ consist of those automorphisms which fix each p'-element of the base group; then $N = \prod_p N_p$, where p runs over the prime divisors of r. For such a p, let p^a be the highest power of p dividing r. Then

$$N_p \cong \begin{cases} (\mathbb{Z}/p^a\mathbb{Z})^\times \times (\mathbb{Z}/p^a\mathbb{Z})^\times & \text{if } p \nmid n, \\ (\mathbb{Z}/p^a\mathbb{Z})^\times \times C_{p^a} & \text{if } p \text{ is odd and } p \mid n, \text{ or if } p = 2 \text{ and } 4 \mid n, \\ (\mathbb{Z}/2^a\mathbb{Z})^\times \times C_{2^{a-1}} \times C_2 & \text{if } p = 2 \text{ and } n/2 \text{ is odd.} \end{cases}$$

Explicit generators of the cyclic subgroups are given in Table II.1 on page 69.

Proof. Let B be the base group of $G_{n,r}$, so that $G_{n,r} = B \rtimes S_n$. As S_n-module, B is induced from $\mathbb{Z}/r\mathbb{Z}$, considered as trivial S_{n-1}-module. By the Eckmann-Shapiro Lemma for Ext,

$$\begin{aligned} \mathrm{H}^1(S_n, B) &= \mathrm{H}^1(S_n, (\mathbb{Z}/r\mathbb{Z})\uparrow_{S_{n-1}}^{S_n}) \cong \mathrm{H}^1(S_{n-1}, \mathbb{Z}/r\mathbb{Z}) \\ &\cong \mathrm{Hom}(S_{n-1}, \mathbb{Z}/r\mathbb{Z}) \cong \begin{cases} C_2 & \text{if } 2 \mid r \text{ and } n > 2, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

[1] called a "duality automorphism" in [14]

Hence if $2 \mid r$ and $n > 2$, there is a non-inner automorphism δ of $G_{n,r}$ which fixes B element-wise and induces the identity on $G_{n,r}/B$. Indeed, we may assume that δ is central, i.e., that δ induces the identity modulo the center of $G_{n,r}$; then δ is unique (in particular, central in $\mathrm{Aut}(G_{n,r})$), and of order 2.

Now let $\alpha \in \mathrm{Aut}(G_{n,r})$. Note that the base group B is characteristic in $G_{n,r}$ (in our special situation, it is easily seen that B is the unique abelian normal subgroup of order r^n). Thus multiplying α by an inner automorphism, and, if necessary, with δ as above, we may assume that α stabilizes B and its complement S_n.

Let ξ be a primitive rth root of unity. Then $\langle \xi \rangle \cong \mathbb{Z}/r\mathbb{Z}$, and each $b \in B$ can be written in the form $b = (\xi^{u_1}, \xi^{u_2}, \ldots, \xi^{u_n})$ with $u_i \in \mathbb{Z}$. Note that $\mathrm{C}_{S_n}(b)$ is a Young subgroup. In particular, the centralizer of $t = (\xi, 1, \ldots, 1)$ in S_n has order $(n-1)!$, and since automorphisms preserve the class lengths, it easily follows that

$$t\alpha = (\xi, 1, \ldots, 1)\alpha = (\xi^v, \ldots, \xi^v, \xi^u, \xi^v, \ldots, \xi^v)$$

for some $u, v \in \mathbb{Z}$ with $\xi^u \neq \xi^v$.

We will see at once that α induces on S_n an inner automorphism: Otherwise $n = 6$ and $\alpha|_{S_n}$ maps the class of cycle type (2) to the class of cycle type $(2,2,2)$, and as t is centralized by a transposition of S_n, its image $t\alpha$ is centralized by an element of S_n of cycle type $(2,2,2)$, which is impossible by the description of $t\alpha$ given above.

Further modifying α by an inner automorphism, we assume from now on that α stabilizes B and fixes the complement S_n element-wise, i.e., that $\alpha \in N$. Then t and $t\alpha$ have the same centralizer in S_n, so that

$$t\alpha = (\xi, 1, \ldots, 1)\alpha = (\xi^u, \xi^v, \ldots, \xi^v).$$

Since $(t^g)\alpha = (t\alpha)^g$ for all $g \in S_n$, the action of α on B is determined by $t\alpha$, and can be described by the $(n \times n)$-matrix

$$M = M(u,v) = \begin{pmatrix} u & v & \ldots & v \\ v & u & \ddots & \vdots \\ \vdots & \ddots & \ddots & v \\ v & \ldots & v & u \end{pmatrix}.$$

Since

$$M(a,b)M(u,v) = M(au + (n-1)bv, bu + av + (n-2)bv) = M(u,v)M(a,b),$$

it follows that N is an abelian group.

Clearly $N = \prod_p N_p$ as claimed, so we assume from now on that $r = p^a$ is the power of a prime p. Let $\mathcal{M}^\times$ be the set of matrices $M := M(u,v)$ with $\det(M)$ a unit in $R := \mathbb{Z}/p^a\mathbb{Z}$. (We shall consider M also as an element of $\mathrm{Mat}_n(R)$.) Note that $M := M(s,t)$ defines

an automorphism (lying in N) if and only if $M \in \mathcal{M}^\times$, so that we can identify N with $\mathcal{M}^\times$. The matrix

$$A = \begin{pmatrix} 1 & -1 & 0 & \dots & 0 \\ 1 & 0 & -1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 1 & 0 & \dots & 0 & -1 \\ 1 & 1 & \dots\dots & & 1 \end{pmatrix}$$

has inverse

$$A^{-1} = \frac{1}{n} \begin{pmatrix} 1 & 1 & \dots\dots & & 1 \\ 1-n & 1 & \dots\dots & & 1 \\ 1 & 1-n & 1 & \dots & 1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 1 & \dots & 1 & 1-n & 1 \end{pmatrix},$$

and

$$AMA^{-1} = \operatorname{diag}(u-v, u-v, \dots, u-v, u+(n-1)v).$$

Thus M, when considered as element of $\operatorname{Mat}_n(R)$, is invertible if and only if its eigenvalues $u-v$ and $u+(n-1)v$ are units in R.

We first handle the case when $p \nmid n$. Let $\mu \in R^\times$. Clearly $\operatorname{diag}(\mu, \dots, \mu) \in A\mathcal{M}^\times A^{-1}$, and setting $v = u-1$, we see that also $\operatorname{diag}(1, \dots, 1, \mu) \in A\mathcal{M}^\times A^{-1}$. Obviously $A\mathcal{M}^\times A^{-1}$ is generated by all matrices of this shape, and it follows that $\mathcal{M}^\times = \{M(\mu, 0) \mid \mu \in R^\times\} \times \{M(1+\frac{\mu-1}{n}, \frac{\mu-1}{n}) \mid \mu \in R^\times\}$.

Now assume that $p \mid n$. Then $u-v \in R^\times$ if and only if $u+(n-1)v \in R^\times$, and given $u \in R$, any $\mu \in R^\times$ can be written as $\mu = u-(u-\mu)$. Thus $\mathcal{M}^\times$ has order $p^{a-1}(p-1)p^a$. Clearly, $\{M(\mu, 0) \mid \mu \in R^\times\} \leq \mathcal{M}^\times$ has order $p^{a-1}(p-1)$. Note that

$$M(u,v)^k = \frac{1}{n} M\big((n-1)(u-v)^k + (u+(n-1)v)^k, -(u-v)^k + (u+(n-1)v)^k\big).$$

In particular,

$$\begin{aligned} M(0,-1)^k &= \frac{1}{n} M\big(n-1+(1-n)^k, -1+(1-n)^k\big) \\ &= M(1-S(k), -S(k)) \quad \text{with} \quad S(k) = \sum_{i=1}^{k} \tbinom{k}{i} (-n)^{i-1}, \end{aligned}$$

and for any $m \in \mathbb{N}$,

$$S(p^m) = p^m + p^m \sum_{i=2}^{p^m} \tbinom{p^m-1}{i-1} \frac{(-n)^{i-1}}{i}.$$

Assume that p is odd, or that $p = 2$ and $4 \mid n$. Let $i \geq 2$. If $p^b \mid i$ for some $b \geq 1$, then $i-1 \geq p^b - 1 \geq b$, with $p^b - 1 > b$ if p is odd. Hence the nominator $(-n)^{i-1}$ is divided

by a higher power of p than the denominator i, and it follows that $S(p^m) \in p^m + p^{m+1}\mathbb{Z}$. Thus $M(0,-1) \in \mathcal{M}^\times$ has order p^a, and

$$M(0,-1)^{p^{a-1}} = M(1-p^{a-1}, p^{a-1}) \quad \text{in} \quad \mathrm{GL}_n(\mathbb{Z}/p^a\mathbb{Z})$$

implies that $\langle M(0,-1)\rangle \cap \{M(\mu,0) \mid \mu \in R^\times\} = 1$. Consequently, $\mathcal{M}^\times$ is generated by $M(0,-1)$ and the diagonal matrices $M(\mu,0)$.

We are left with the case $p = 2$ and $n = 2d$ for odd d. We have

$$M(1,2)^k = M\big((-1)^k + \tilde{S}(k), \tilde{S}(k)\big) \quad \text{with} \quad \tilde{S}(k) = 2\sum_{i=1}^{k} \tbinom{k}{i}(2n)^{i-1}(-1)^{k-i},$$

and for any $m \in \mathbb{N}$,

$$\tilde{S}(2^m) = 2\left(2^m + 2^m \sum_{i=2}^{2^m} \tbinom{2^m-1}{i-1} \frac{(2n)^{i-1}}{i}(-1)^{2^m-i}\right).$$

For $i \geq 2$, the nominator $(2n)^{i-1}$ is divided by a higher power of 2 than the denominator i. Hence $\tilde{S}(2^m) \in 2^{m+1} + 2^{m+2}\mathbb{Z}$, and

$$M(1,2)^{2^{a-2}} = M(1+2^{a-1}, 2^{a-1}) \quad \text{in} \quad \mathrm{GL}_n(\mathbb{Z}/2^a\mathbb{Z}) \quad \text{for} \quad a \geq 3.$$

It follows that $M(1,2) \in \mathcal{M}^\times$ has order 2^{a-1}, and that $M(1,2)$ intersects the group of diagonal matrices trivially.

Note that $M(0,1)^2 = M(n-1, n-2)$, so $M(0,1)$ has order 2 in $\mathrm{GL}_n(\mathbb{Z}/4\mathbb{Z})$ by assumption on n.

Finally, note that $M(1-\frac{1}{d}, -\frac{1}{d})$ is an element of $\mathcal{M}^\times$ of order 2.

Altogether, it follows that N is of the form as shown in Table II.1 on page 69. □

Character table automorphisms of $(\mathbb{Z}/r\mathbb{Z}) \wr S_n$

Set $t = \mathrm{diag}(\xi, 1, \ldots, 1)$ and let s_i be the permutation matrix which permutes the ith and the $(i+1)$th basis vector (and leaves the remaining fixed). Then $G_{n,r} = \langle t, s_1, \ldots, s_{n-1}\rangle$. For all $u, v \in \mathbb{Z}$, there are representations

$$\begin{aligned} \rho^+_{u,v},\, \rho^-_{u,v} : G_{n,r} \to \mathrm{GL}_n(\mathbb{C}), \quad & \text{defined by} \\ & \rho^+_{u,v}(t) = \rho^-_{u,v}(t) = \mathrm{diag}(\xi^u, \xi^v, \ldots, \xi^v), \\ & \rho^+_{u,v}(s_i) = s_i \quad \text{and} \quad \rho^-_{u,v}(s_i) = -s_i \quad \text{for all } 1 \leq i \leq n-1. \end{aligned}$$

The irreducible characters of $G_{n,r}$ can be obtained by the "method of little groups" (see [132]). From this description, it follows that each n-dimensional irreducible character

Case 1: $p \nmid n$.
$N = \{M(\mu, 0) \mid \mu \in R^\times\} \times \{M(1 + \frac{\mu-1}{n}, \frac{\mu-1}{n}) \mid \mu \in R^\times\}$
$\cong (\mathbb{Z}/p^a\mathbb{Z})^\times \times (\mathbb{Z}/p^a\mathbb{Z})^\times$
Case 2: p odd and $p \mid n$, or $p = 2$ and $4 \mid n$.
$N = \{M(\mu, 0) \mid \mu \in R^\times\} \times \langle M(0, -1)\rangle \cong (\mathbb{Z}/p^a\mathbb{Z})^\times \times C_{p^a}$
Case 3: $p^a = 2^a$ and $n = 2d$ with d odd.
$a = 1: \quad N = \langle M(0, 1)\rangle \cong C_2$
$a = 2: \quad N = \{M(\mu, 0) \mid \mu \in R^\times\} \times \langle M(1, 2)\rangle \times \langle M(0, 1)\rangle \cong C_2 \times C_2 \times C_2$
$a \geq 3: \quad N = \{M(\mu, 0) \mid \mu \in R^\times\} \times \langle M(1, 2)\rangle \times \langle M(1 - \frac{1}{d}, -\frac{1}{d})\rangle$
$\cong C_{2^{a-2}} \times C_2 \times C_{2^{a-1}} \times C_2$

Table II.1.: Structure of N for $G = C_{p^a} \wr S_n$.

of $G_{n,r}$ is afforded by some representation $\rho^\epsilon_{u,v}$, and if two such representations are distinct, then they are non-equivalent except for the case $n = 2$ and the characters $\rho^+_{u,v}$ and $\rho^-_{u,v}$. Note that a representation $\rho^\epsilon_{u,v}$ is faithful if and only if the determinant of the matrix $M(u, v)$ is a unit in $\mathbb{Z}/r\mathbb{Z}$. A faithful character afforded by some $\rho^+_{u,v}$ will be called a *natural reflection character*. It is obvious that the subgroup $N \leq \mathrm{Aut}(G_{n,r})$ defined in Proposition 9.1 acts simply transitive on the natural reflection characters.

The conjugacy classes of $G_{n,r}$ are indexed by a set of multipartitions. We shall only need the following facts. Set

$$Z(d, a) := \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ a & & & \end{pmatrix}_{d \times d}$$

(a monomial $d \times d$-matrix). Then each element of $G_{n,r}$ is conjugate to a block diagonal matrix of the form

$$M := \mathrm{diag}(Z(n_1, a_1), \ldots, Z(n_k, a_k))$$

for some integers n_i and rth roots of unity a_i. If we arrange the n_i in increasing order, we obtain a partition of n which we call the *shape* of the matrix M. Note that two block matrices of the above form are conjugate in $G_{n,r}$ if and only if they can be transformed

into each other by permuting the blocks. Also,

$$\text{char.pol}(M) = \det(X \cdot \mathrm{id} - M) = \prod_{i=1}^{k} (X^{n_i} - a_i).$$

Note that the conjugacy class of M is *not* determined by its characteristic polynomial and its shape.

We shall write $\mathrm{AutCT}(G)$ for the group of automorphisms of the character table $\mathrm{CT}(G)$ of a finite group G (following [14, Definition 2.6]).

Recall that we assume that $G_{n,r} \neq G_{2,2}$.

9.2 Theorem. *Each character table automorphism of $G_{n,r}$ which fixes a natural reflection character is trivial, and the sequence*

$$1 \longrightarrow \mathrm{Inn}(G_{n,r}) \longrightarrow \mathrm{Aut}(G_{n,r}) \longrightarrow \mathrm{AutCT}(G_{n,r}) \longrightarrow 1$$

is exact.

Proof. Let $\chi^{\epsilon}_{u,v}$ be the character afforded by $\rho^{\epsilon}_{u,v}$ ($\epsilon = \pm 1$). Let $\tau \in \mathrm{AutCT}(G_{n,r})$. For each $g \in G_{n,r}$ we choose some $\tau(g) \in G_{n,r}$ such that τ maps the class of g to the class of $\tau(g)$. Assume that $n \geq 3$ and that τ maps $\chi^{+}_{1,0}$ to some $\chi^{-}_{u,v}$. Then $\chi^{+}_{1,0}(\tau(s_1)) = \tau(\chi^{+}_{1,0})(s_1) = \chi^{-}_{u,v}(s_1) = -(n-2)$. Thus $\tau(s_1)$ must be conjugate in $G_{n,r}$ to an element of the form $\mathrm{diag}(\xi^i, \xi^{-i}, -1, \ldots, -1) \cdot s_1$. This can only happen if r is even, so we can define a duality automorphism δ of $G_{n,r}$ as in Proposition 9.1, which maps $\chi^{-}_{u,v}$ to $\chi^{+}_{u,v}$. If $n = 2$, then $\chi^{-}_{u,v} = \chi^{+}_{u,v}$. Since we have already seen that $\mathrm{Aut}(G_{n,r})$ acts transitive on the natural reflection characters, we assume from now on that τ fixes the character $\chi := \chi^{+}_{1,0}$ of the representation $\rho := \rho^{+}_{1,0}$, and then have to show that τ is trivial.

By [14, Corollary 2.5], we have $\text{char.pol}(\rho(\tau(g))) = \text{char.pol}(\rho(g))$ for all $g \in G_{n,r}$.

Let N be the normal subgroup of $G_{n,r}$ consisting of the diagonal matrices. We will show that τ fixes N.

Let $1 \neq g \in \langle t \rangle$. Since g has eigenvalue 1 with multiplicity $n-1$, the class of g is either fixed by τ or sent to the class of s_1. But g has exactly n conjugates in $G_{n,r}$, whereas s_1 has more than n conjugates (this is the reason why we do not consider $G_{2,2}$ here). Thus τ fixes the class of g.

We remark that by the same reasoning, it follows that the class of s_1 is fixed by τ: Since τ preserves the orders of the elements of $G_{n,r}$ and fixes ρ, it follows that $\tau(s_1)$ is either conjugate to $\mathrm{diag}(-1, 1, \ldots, 1)$ (which turns out to be impossible by comparing the conjugacy lengths) or to an element of the form $\mathrm{diag}(\xi^i, \xi^{-i}, 1, \ldots, 1) \cdot s_1$ (i.e., to s_1).

Since N is generated by the conjugates of t, it follows from [14, Corollary 2.5] (and an easy induction) that $\tau(N) = N$. Hence τ permutes the characters of $G_{n,r}$ having N in their kernel, and we obtain an induced character table automorphism $\bar{\tau}$ of the quotient

$G_{n,r}/N \cong S_n$. By Peterson's result [101] (see also [14, Subsection 2.7]), $\bar{\tau}$ must be trivial. This is obvious for $n \neq 6$; for $n = 6$, note that the class of s_1 is fixed by $\bar{\tau}$. In other words, τ preserves the shape of each element of $G_{n,r}$.

Assume that a permutation matrix $P = \mathrm{diag}(Z(n_1, 1), \ldots, Z(n_k, 1)) \in G_{n,r}$ has the same characteristic polynomial as a matrix $M = \mathrm{diag}(Z(n_1, a_1), \ldots, Z(n_k, a_k))$ for some rth roots of unity a_i. We will show by induction on $n = n_1 + \ldots + n_k$ that P and M are conjugate in $G_{n,r}$. Therefore we may assume that $n_1 = \ldots = n_l < n_{l+1} \leq n_{l+2} \leq \ldots$. In the quotient field of the ring of formal power series,

$$1 = \frac{\prod_{i=1}^{k}(X^{n_i} - a_i)}{\prod_{i=1}^{k}(X^{n_i} - 1)} = \prod_{i=1}^{k}\left(a_i + (a_i - 1)\sum_{j=1}^{\infty} X^{n_i j}\right) =: f(X).$$

Thus $\prod_{i=1}^{k} a_i = 1$, and the lowest non-constant term of f has coefficient

$$c := \sum_{i=1}^{l}\left((a_i - 1)\prod_{j \neq i} a_j\right) = \sum_{i=1}^{l}(1 - a_i^{-1}).$$

Since $c = 0$, we get $a_1 = \ldots = a_l = 1$ by the triangle equality. If $k = l$ we are done, and otherwise $\mathrm{diag}(Z(n_{l+1}, 1), \ldots, Z(n_k, 1))$ and $\mathrm{diag}(Z(n_{l+1}, a_{l+1}), \ldots, Z(n_k, a_k))$ have the same characteristic polynomials, and the proof is completed by induction.

Now let $M = \mathrm{diag}(Z(n_1, a_1), \ldots, Z(n_k, a_k)) \in G_{n,r}$. We will show that τ fixes the class of M. This will be done by induction on the number of the a_i's which are different from one. The case when M is a permutation matrix already being settled, we can assume that $a_1 \neq 1$. Then M is the product of $\mathrm{diag}(Z(n_1, 1), Z(n_2, a_2), \ldots, Z(n_k, a_k))$ and a diagonal matrix D with one main diagonal entry equal to a_1, and all others equal to 1. We know that $\tau(D)$ is conjugate to D, so by [14, Corollary 2.3(a)] and the induction hypothesis, we may assume that $\tau(M) = \mathrm{diag}(Z(n_1, 1), Z(n_2, a_1 a_2), \ldots, Z(n_k, a_k))$ (the reader should notice that nothing can happen if M consists of a single block only). It follows that the matrices $\mathrm{diag}(Z(n_1, a_1), Z(n_2, a_2))$ and $\mathrm{diag}(Z(n_1, 1), Z(n_2, a_1 a_2))$ have the same characteristic polynomials, i.e., that $a_1 X^{n_2} + a_2 X^{n_1} = X^{n_2} + a_1 a_2 X^{n_1}$. Since $a_1 \neq 1$, it follows that $n_1 = n_2$. Thus if $a_2 = 1$, then $\tau(M)$ is obtained from M by permuting the first two blocks. Otherwise $\tau(M)$ and $\tau^2(M)$ are conjugate by induction hypothesis, and we may apply τ^{-1} to obtain the desired result.

We have shown that τ is trivial. Thus to prove exactness of the short sequence, we only need to observe that class-preserving automorphisms of $G_{n,r}$ are inner automorphisms. □

To conclude this chapter, we describe a particular situation when a character table automorphism of a factor group of G can be extended to an automorphism of the whole character table of G. This situation is given, for example, for the complex reflection group G of order $3^6 \cdot 2$, which will lead to a character table automorphism which is not induced by a group automorphism of G.

9.3 Remark. Let G be a finite group, with normal subgroup N. We will write $\bar{G} = G/N$ etc. Note that for $g \in G$, we have $\mathrm{C}_{\bar{G}}(\bar{g}) = \frac{l}{|N|}\mathrm{C}_G(g)$, where l is the number of conjugates of g lying in the coset Ng. In particular, if $\mathrm{C}_{\bar{G}}(\bar{g}) = \mathrm{C}_G(g)$ for some $g \in G$, and C denotes the column of the character table $\mathrm{CT}(G)$ belonging to g, then the following holds.

(i) If a column C' of $\mathrm{CT}(G)$ agrees with C in all entries which correspond to characters having N in their kernel, then $C' = C$;

(ii) All entries of C which correspond to characters having N not in their kernel are zero.

(The second observation follows from the Second Orthogonality Relation, and, of course, implies the first one.)

Now assume that there is $\tau \in \mathrm{AutCT}(\bar{G})$ with the property that τ moves only classes of elements $\bar{g}$ with $\mathrm{C}_{\bar{G}}(\bar{g}) = \mathrm{C}_G(g)$. Then, by the above, τ extends to a character table automorphism of G which fixes the class of g if the class of $\bar{g}$ is fixed by τ, and moves the class of g to the class of h if τ moves the class of $\bar{g}$ to the class of $\bar{h}$ (note that this prescription is well defined).

9.4 Example. We show that the imprimitive complex reflection group G of order $3^6 \cdot 2$ has a character table automorphism which is not induced by a group automorphism.[2] Let ξ be a primitive 9th root of unity, and put

$$t = \begin{pmatrix} \xi & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad s_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad s_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Then $G = \langle t^3, t^{-1}s_1t, s_1, s_2 \rangle$ is a normal subgroup of $G_{3,9} = \langle t, s_1, s_2 \rangle$ of index 3 containing all diagonal matrices whose determinant is a 3th root of unity (often G is denoted by $G(9,3,3)$). Set

$$a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \xi^3 & 0 \\ 0 & 0 & \xi^6 \end{pmatrix}, \quad b = \begin{pmatrix} \xi & 0 & 0 \\ 0 & \xi^4 & 0 \\ 0 & 0 & \xi^4 \end{pmatrix}.$$

Then $a^{s_1} = a^2b^3$, $b^{s_1} = ab^4$, $a^{s_2} = a^2$ and $b^{s_2} = b$, so $N := \langle a, b \rangle$ is a normal subgroup of G of order 3^3. (Also, note that $N = \{[x, s_1s_2] \mid x \in D\}$, where D is the subgroup of diagonal matrices in G.) Finally, set

$$u = t^3 = \begin{pmatrix} \xi^3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad v = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \xi & 0 \\ 0 & 0 & \xi^{-1} \end{pmatrix}.$$

[2] GAP [37] claims that $|\mathrm{AutCT}(G)| = 2|\mathrm{Out}(G)| = 108$.

Then $\langle \bar{u}, \bar{v} \rangle$ is a subgroup of order 9 in $\bar{G} := G/N$, with $\bar{v}^{\bar{s}_1} = \bar{v}^{\bar{s}_2} = \bar{v}^2$ and $[\bar{u}, \bar{G}] = 1$. Thus $\bar{G} = \langle \bar{u} \rangle \times (\langle \bar{v} \rangle \rtimes \langle \bar{s}_1, \bar{s}_2 \rangle) \cong C_3 \times (C_3 \rtimes S_3)$. Let τ be the automorphism of $\bar{G}$ which fixes $\bar{u}$ and $\bar{v}$, and interchanges $\bar{s}_1$ and $\bar{s}_2$. Note that the factor $C_3 \rtimes S_3$ contains a unique class of involutions, so that τ fixes each class of elements of 2-order and each class of elements of composite order. It follows that τ interchanges the classes of $\bar{u}^i\bar{v}(\bar{s}_1\bar{s}_2)$ and $\bar{u}^i\bar{v}^2(\bar{s}_1\bar{s}_2)$ for $i = 0, 1, 2$, and leaves the remaining classes fixed.

Let $g = u^i v s_1 s_2$ for some i. Note that a diagonal matrix which centralizes g is a multiple of the identity matrix. It readily follows that $\mathrm{C}_N(g)$ has order 3. We have $g^v = (b^{s_1 s_2})^2 g \in Ng$. Assume that $g^v = g^x$ for some $x \in N$. Then $x = \lambda \cdot v$ for some $\lambda \in \langle \xi \rangle$. Since $xv^{-1} \in G$, it follows that $\lambda \in \langle \xi^3 \rangle$. But then $x \in \langle a, b^3 \rangle$, and we obtain the contradiction $1 = x^3 = v^3 \neq 1$. We have proved that all elements in the coset Ng are conjugate in G, and therefore $\mathrm{C}_{\bar{G}}(\bar{g}) = \mathrm{C}_G(g)$.

It follows that τ extends to a character table automorphism $\hat{\tau}$ of G (in the sense of Remark 9.3). Clearly, $\hat{\tau}$ is not a field automorphism. Next, we show that $\hat{\tau}$ is not induced by a group automorphism.

Assume that $\hat{\tau}$ is induced by some $\varphi \in \mathrm{Aut}(G)$. Then φ stabilizes N, and fixes the conjugacy class of each diagonal matrix. Note that class-preserving automorphisms of $\bar{G}$ are necessarily inner automorphisms, so that we can assume that φ induces α on $\bar{G}$. Then $s_2\varphi = x s_1$ and $v\varphi = yv$ for some $x, y \in N$, and we obtain $(yv)^{s_1} = (yv)^{x s_1} = (v\varphi)^{s_2\varphi} = v^{-1}\varphi = y^{-1}v^{-1}$, i.e., s_1 inverts $v\varphi$. Thus $v\varphi$ is of the form $\mathrm{diag}(\xi^i, \xi^{-i}, \xi^j)$, and since $v\varphi$ is conjugate to v, it follows that $v\varphi = \mathrm{diag}(\xi^{\pm 1}, \xi^{\mp 1}, 1)$. Finally, $v^{-1}(v\varphi) \in N$ implies that $v\varphi = \mathrm{diag}(\xi, \xi^{-1}, 1)$. Furthermore, $s_1\varphi \in N s_2$, so $(v^{s_1})\varphi = (v\varphi)^{s_1\varphi} = (v\varphi)^{s_2} = \mathrm{diag}(\xi, 1, \xi^{-1}) = v^{s_1}$. Hence $\mathrm{diag}(\xi, \xi, \xi^{-2}) = v \cdot v^{s_1} \overset{\phi}{\longmapsto} v\varphi \cdot v^{s_1}\varphi = \mathrm{diag}(\xi^2, \xi^{-1}, \xi^{-1})$, a contradiction, since by assumption φ fixes the conjugacy class of $v \cdot v^{s_1}$.

III. Automorphisms of integral group rings: local–global considerations

> Le bon sens est la chose du monde la mieux partagée, car chacun pense en être bien pourvu.
>
> *Réne Descartes*
> *Le Discours de la méthode, 1637*

An automorphism α of an integral group ring RG, where G is a finite group, is said to have a Zassenhaus factorization if it is the composition of an automorphism of G (extended to a ring automorphism) and a central automorphism. Blanchard [13] showed that there are three groups of order 96 whose group rings over semilocal coefficient rings R have automorphisms without Zassenhaus factorization. In this chapter, it is shown that over the coefficient ring $\mathbb{Z}$ of rational integers, the same holds for two of these groups, but not for the remaining group.

10. General considerations and the groups of Blanchard

In the last 15 years, counterexamples were found to the Zassenhaus conjecture, the normalizer problem, and the isomorphism problem. These are questions about isomorphisms of integral group rings $\mathbb{Z}G$, where G is a finite group, and the counterexamples were found among the finite solvable groups.

A common point of view was that the main problem was to find the semilocal counterexample, with the global problem over $\mathbb{Z}$ just being a question of hard work. Allowing a sufficiently broad interpretation, this philosophy may be accurate: It may indeed be difficult in a given semilocal case to check if one has a counterexample. However, there is at least a general K-theoretic procedure, outlined by Roggenkamp and Scott [117]. And while it may lead to an obstruction, counterexamples usually come in families, and there should always be a possibility of selecting the appropriate family member or making some other small modification to get rid of the obstruction. The results presented here illustrate this point of view.

A specific counterexample due to Roggenkamp and Zimmermann [122], did not lead to a global example (see [57, Section 8]), in spite of expectations. However, it is conventional

wisdom that existence of the semilocal automorphism is very strong evidence for the existence of a global automorphism.

Recently, Blanchard [13] showed that there are three semilocal counterexamples to the Zassenhaus conjecture, the groups having order 96 (and that there are no smaller groups violating the conjecture). Here, it is shown that two of his groups give rise to global counterexamples, but not the remaining one.[1]

Let G be a finite group, and let S be a *G-adapted ring*, that is, an integral domain of characteristic 0 in which no prime divisor of $|G|$ is invertible. (A basic example is $\mathbb{Z}_{\pi(G)}$, the intersection of the localizations $\mathbb{Z}_{(p)}$ with p in $\pi(G)$, the set of prime divisors of $|G|$.) Following [127, p. 327], we shall say that an automorphism of SG has a *Zassenhaus factorization* if it is the composition of a group automorphism of G (extended to a ring automorphism) and a *central* automorphism (an automorphism of SG fixing the center element-wise). Then, the Zassenhaus conjecture holds for G if each augmentation-preserving automorphism of $\mathbb{Z}G$ has a Zassenhaus factorization. Roggenkamp and Scott [117] constructed for the first time a group G such that $\mathbb{Z}G$ has an augmentation-preserving automorphism which has no Zassenhaus factorization (see also [82]). Further counterexamples are given in [55, 60] (the smallest example having order 144). Blanchard [13, 12] gave semilocal counterexamples. His groups from [13] are the following groups of order $96 = 2^5 \cdot 3$.

$$\begin{aligned}
G_0 &= \langle a,b,c,q \mid a^4 = b^4 = c^2 = q^3 = 1,\ [b,c] = [b,q] = [c,q] = 1,\\
&\qquad b^a = bc, c^a = b^2c, q^a = q^{-1}\rangle,\\
G_1 &= \langle a,b,c,q \mid b^4 = c^2 = q^3 = 1, a^4 = b^2,\ [b,c] = [b,q] = [c,q] = 1,\\
&\qquad b^a = bc, c^a = a^4c, q^a = q^{-1}\rangle,\\
G_2 &= \langle a,b,c,q \mid a^8 = b^2 = c^2 = q^3 = 1,\ [b,c] = [b,q] = [c,q] = 1,\\
&\qquad b^a = bc, c^a = a^4c, q^a = q^{-1}\rangle.
\end{aligned}$$

In this chapter, we attack the global case and prove the following theorem.

10.1 Theorem. *There exists augmentation-preserving automorphisms α_i of SG_i, where $S = \mathbb{Z}_{\pi(G_i)}$, which have no Zassenhaus factorization ($i = 1, 2, 3$). Moreover, the following holds.*

(i) *The semilocal automorphisms α_1 and α_2 are represented by global ones, up to semilocal inner automorphisms: The Zassenhaus conjecture does not hold for the groups G_1 and G_2.*

(ii) *The semilocal automorphism α_0 is not represented by a global one: The Zassenhaus conjecture holds for the group G_0.*

[1] The necessary matrix calculations can be done by hand, but they were also checked using MAPLE [144].

The difficult task is to prove part (ii). There is an invertible bimodule M for $\mathbb{Z}G_0$ such that $S \otimes_{\mathbb{Z}} M \cong {}_1(SG_0)_{\alpha_0}$ as invertible bimodules (cf. Proposition 1.4), and the problem is to show that there is no invertible bimodule for $\mathbb{Z}G_0$ in the same genus as M which is free from one side. This is proved indirectly in Section 12 by showing that the semilocal automorphism α_0 is not represented by a global one.

Gustafson and Roggenkamp [48, (4.10)] raised the question whether there is an example of a $\mathbb{Z}$-order Λ and an invertible bimodule N with a left Λ-module isomorphism $N \oplus \Lambda \cong \Lambda \oplus \Lambda$ with N not left Λ-free. Examples were given by Montgomery and Passman [94], and by Guralnick and Montgomery [46, Proposition 5.7]. The question remains open whether such bimodules exist for integral group rings (see [48]).

We were not able to decide whether M (as above) is stably free as left $\mathbb{Z}G_0$-module or not. Note that $\mathbb{Q}G_0$ does not satisfy the Eichler condition, which is a sufficient, but not necessary, condition for $\mathbb{Z}G_0$ to have locally free cancellation. Thus one has to do some extra work. Since in our proof of Theorem 10.1(ii), the components of $\mathbb{Q}G_0$ which are totally definite quaternion algebras seemingly do not play any role (have a look at the unit v given in Subsection 12.4), we believe that M will not be stably free.

In Subsection 12.5 we briefly comment on this question. Without further work, we obtain from Theorem 10.1(ii):

10.2 Proposition. *There is an invertible bimodule M for $\mathbb{Z}G_0$ such that $S \otimes_{\mathbb{Z}} M \cong {}_1(SG_0)_{\alpha_0}$ as invertible bimodules, with $\alpha_0 \in \mathrm{Aut}_{\mathrm{n}}(SG_0)$ as in Theorem 10.1. The module M is not $\mathbb{Z}G_0$-free from one side, and $M \oplus M \cong \mathbb{Z}G_0 \oplus \mathbb{Z}G_0$ as left $\mathbb{Z}G_0$-modules (but the latter does not hold for all choices of M).*

10.3 Remark. We tried unsuccessfully to find an example showing that there is no local–global principle for *central* group ring automorphisms. Roggenkamp pointed out where the obstruction for getting globally central automorphisms from local data lies (see [121, p. 82]). Let R be a Dedekind ring of characteristic 0, let G be a finite group, and let $\mathrm{Cl}_{RG}(\mathrm{Z}(RG))$ be the subgroup of the locally free class group $\mathrm{Cl}(\mathrm{Z}(RG))$ consisting of those isomorphism classes of invertible ideals $\mathfrak{a}$ in $\mathrm{Z}(RG)$ so that $\mathfrak{a}RG$ is a principal ideal in RG. Then Fröhlich's localization sequence ([36]; cf. also [27, 55.25, 55.26]) can be extended to the following diagram with exact rows.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Cl}(\mathrm{Z}(RG)) & \longrightarrow & \mathrm{Picent}(RG) & \longrightarrow & \prod_{P\in\max(R)} \mathrm{Picent}(R_PG) & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \uparrow\cong & & \\
1 & \longrightarrow & \mathrm{Cl}_{RG}(\mathrm{Z}(RG)) & \longrightarrow & \mathrm{Outcent}(RG) & \xrightarrow{\phi} & \prod_{P\in\max(R)} \mathrm{Outcent}(R_PG) & &
\end{array}$$

The question whether ϕ is surjective, i.e., whether for any M in $\mathrm{Picent}(RG)$ there is an invertible bimodule in the same genus as M which is RG-free from the left (say) has been raised in [121, IX 1.13], [120, Problem 3.7], [116, Problem 12.3]. If R is a semilocal ring, then ϕ is an isomorphism (see [27, 55.26, 55.16]).

First, we review some properties which the group rings $\mathbb{Z}G_i$ have in common.

Structure of the group rings

Set $P = \langle a, b, c\rangle$, a Sylow 2-subgroup of G_i of order 32, and $Q = \langle q\rangle$, the normal Sylow 3-subgroup of G_i of order 3 ($i = 1, 2, 3$). Let M denote the center of G_i, so $M := \langle a^4\rangle$ if considered as a subgroup of G_1 or G_2, and $M := \langle b^2\rangle$ if considered as a subgroup of G_0.

For a group X, write $\hat{X}$ for the sum of its elements. The (two-sided) ideal generated by group ring elements $s, t, \dots$ will be denoted by $(s, t, \dots)$. The quotient

$$\Lambda = \mathbb{Z}G_i/(\hat{M}, \hat{Q})$$

is the projection on a factor of $\mathbb{Q}G_i$ (to which all blocks having neither M nor Q in their kernel belong). The projection of $\mathbb{Z}G_i$ on the complementary factor is the image Γ of $\mathbb{Z}G_i$ under the natural map $\mathbb{Z}G_i \to \mathbb{Z}G_i/M \oplus \mathbb{Z}G_i/Q$. Hence there are pullback diagrams

$$\begin{array}{ccc} \Gamma & \longrightarrow & \mathbb{Z}G_i/M \\ \downarrow & & \downarrow \\ \mathbb{Z}G_i/Q & \longrightarrow & \mathbb{Z}G_i/MQ \end{array} \qquad \text{and} \qquad \begin{array}{ccc} \mathbb{Z}G_i & \longrightarrow & \Gamma \\ \downarrow & & \downarrow \\ \Lambda & \longrightarrow & \bar{\Lambda} \end{array}.$$

Roggenkamp and Scott (see Theorem 7.1) proved that the ring $\bar{\Lambda}$ over which the pullback for $\mathbb{Z}G_i$ is taken has the form

$$(\mathbb{F}_2G_i/M)/(\hat{Q}) \oplus (\mathbb{F}_3G_i/Q)/(\hat{M}).$$

A group automorphism τ of G_i plays an important role. Though τ induces on Γ a non-central automorphism, τ will induce central automorphisms of the quotients $(\mathbb{Z}G/M)/(\hat{Q})$ and $(\mathbb{Z}G/Q)/(\hat{M})$, and even an inner automorphism of $\bar{\Lambda}$.

For $i = 1, 2$, it is shown in Section 11 that there are inner automorphisms $\gamma \in \mathrm{Inn}(\Gamma)$ and $\lambda \in \mathrm{Inn}(\Lambda)$ which differ on the common quotient $\bar{\Lambda}$ by the automorphism induced by τ, say $\bar{\tau}\bar{\lambda} = \bar{\gamma}$. Thus there is an automorphism α of $\mathbb{Z}G_i$ which induces γ on Γ and $\tau\lambda$ on Λ. Note that α is augmented; this is because Γ inherits the structure of an augmented algebra, and α induces on Γ an augmentation-preserving automorphism. In order to show that α has no Zassenhaus factorization, it remains to show that there is no $\sigma \in \mathrm{Aut}(G_i)$ which induces on Λ a central automorphism, and differs on Γ from τ by a central automorphism (this will be called the "group-theoretical obstruction").

In contrast to the $i = 1, 2$ group case, it is shown in Section 12 that in the $i = 0$ case, there are *no* central automorphisms $\gamma \in \mathrm{Autcent}(\Gamma)$ and $\lambda \in \mathrm{Autcent}(\Lambda)$ which differ on the common quotient $\bar{\Lambda}$ by the automorphism induced by τ.

For global considerations, one has to deal with the representations (= matrices) more directly. Note that G_i has a faithful irreducible complex representation θ_i, given by the

following matrices (dots indicate zeros, $\zeta = \exp(2\pi i/3)$):

$$\theta_0(a) = \begin{bmatrix} \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \\ 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \end{bmatrix}, \quad \theta_0(b) = \begin{bmatrix} \cdot & 1 & \cdot & \cdot \\ -1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & -1 \\ \cdot & \cdot & 1 & \cdot \end{bmatrix},$$

$$\theta_1(a) = \begin{bmatrix} \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \\ i & \cdot & \cdot & \cdot \\ \cdot & -i & \cdot & \cdot \end{bmatrix}, \quad \theta_1(b) = \begin{bmatrix} \cdot & 1 & \cdot & \cdot \\ -1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & -1 & \cdot \end{bmatrix},$$

$$\theta_2(a) = \begin{bmatrix} \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \\ \cdot & 1 & \cdot & \cdot \\ -1 & \cdot & \cdot & \cdot \end{bmatrix}, \quad \theta_2(b) = \begin{bmatrix} -1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & -1 & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix},$$

$$\theta_i(c) = \begin{bmatrix} -1 & \cdot & \cdot & \cdot \\ \cdot & -1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix}, \quad \theta_i(q) = \begin{bmatrix} \zeta & \cdot & \cdot & \cdot \\ \cdot & \zeta & \cdot & \cdot \\ \cdot & \cdot & \zeta^2 & \cdot \\ \cdot & \cdot & \cdot & \zeta^2 \end{bmatrix} \quad (i = 0, 1, 2).$$

In fact, $\theta_i|_P$ is an irreducible representation of the Sylow 2-subgroup P of G_i. These representations are distinguished by the following properties. We have $\theta_2(P) \subseteq \mathrm{SL}_4(\mathbb{Z})$. We have $\theta_1(\mathbb{Q}P) \cong \mathrm{Mat}_2(\mathbb{H})$, where $\mathbb{H}$ is the skewfield of rational quaternions, so $\theta_1|_P$ has Schur index 2 relative to $\mathbb{Q}$. Finally, we have $\theta_0(P) \subseteq \mathrm{GL}_4(\mathbb{Z})$, but $\theta_0(a)$ has determinant -1.

Note that $\theta_i(cq)$ has trace $2(-\zeta+\zeta^2)$, so some algebraic conjugate of θ_i affords another character of G_i. Since $\dim(\mathbb{Q}\Lambda) = 96 - 96/2 - 96/3 + 96/6 = 32$, it follows that we may identify Λ with the $\mathbb{Z}$-order generated by $\theta_i(G_i)$.

11. Two groups lead to global counterexamples

In this section, G may be one of the groups G_1, G_2. One verifies immediately that automorphisms τ and τ' of G are defined by setting

$$\tau' : \begin{cases} a \mapsto a^{-1} \\ b \mapsto b \\ c \mapsto a^4 c \\ q \mapsto q^{-1} \end{cases}, \quad \tau : \begin{cases} a \mapsto a^{-1} \\ b \mapsto b \\ c \mapsto a^4 c \\ q \mapsto q \end{cases}.$$

Recall that $M := \mathrm{Z}(G) = \langle a^4 \rangle$. Let bars denote reduction modulo M, so $\bar{G} = G/M$. First, we prove the following group-theoretical obstruction:

There is no $\sigma \in \mathrm{Aut}(G)$ which induces on Λ a central automorphism, and differs on Γ from τ by a central automorphism.

By way of contradiction, assume that there is $\sigma \in \mathrm{Aut}(G)$ having these properties. Modifying σ by an inner automorphism, if necessary, we can assume that $q\sigma = q$ and $P\sigma = P$. We have $\mathrm{Z}(P) = \langle a^4 \rangle$ and $[P,P] = \langle a^4 \rangle \times \langle c \rangle \cong C_2 \times C_2$, so $a^4\sigma = a^4$, and either $c\sigma = c$ or $c\sigma = a^4c$. The class sums $C_1 := cq + a^4cq^{-1}$ and $C_2 := cq^{-1} + a^4cq$ have different images in Λ, as one sees from $0 \not\equiv C_1 \equiv c(q - q^{-1}) \equiv -C_2 \mod (\hat{M}, \hat{Q})$. Since σ would permute these class sums provided that $c\sigma = a^4c$, we have $c\sigma = c$. Furthermore $b\sigma \in b\langle c, a^4 \rangle$ since $V := \langle b, c, a^4 \rangle$ is a characteristic subgroup of P. If $b\sigma \in \{bc, bca^4\}$, then $(bcq)\tau\sigma \in \{ba^4q, bq\}$. But $\bar{b}\bar{c}\bar{q}$ and $\bar{b}\bar{q}$ are not conjugate in $\bar{G}$, contradicting the assumption that $\tau\sigma$ induces a central automorphism of $\mathbb{Z}\bar{G}$ (note that $\bar{a}^4 = 1$). Hence $b\sigma \in b\langle a^4 \rangle$. Since a^4 is central, it now follows from $(b\sigma)^{a\sigma} = (b^a)\sigma = (bc)\sigma = (b\sigma)c$ that $b^{a\sigma} = bc$. Clearly $a\sigma \in a^{\pm 1}V \subseteq a^{\pm 1}\mathrm{C}_G(b)$, so $a\sigma \in aV$ as $b^{a^{-1}} \neq bc$. Thus σ induces on $\tilde{G} := G/VQ = \langle \tilde{a} \rangle \cong C_4$ the identity. As $a\tau = a^{-1}$, it follows that $\tau\sigma$ induces a non-central automorphism of $\mathbb{Z}\tilde{G}$, and we have reached a contradiction.

Let us see how τ acts on the various pieces over which the pullback for $\mathbb{Z}G$ is taken. Set $u = ((1+c)a^{-1} + (1-c)a)b$. Then

$$\theta_1(u) = 2\begin{bmatrix} \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & -1 & \cdot \\ \cdot & 1 & \cdot & \cdot \\ -1 & \cdot & \cdot & \cdot \end{bmatrix}, \quad \theta_2(u) = 2\begin{bmatrix} \cdot & \cdot & -1 & \cdot \\ \cdot & \cdot & \cdot & 1 \\ -1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \end{bmatrix},$$

and one verifies that τ' induces on Λ a central automorphism, given by conjugation with the rational unit $\theta_i(u)$. Note that $\theta_i(u)^2$ is ± 4 times the identity matrix. Since τ' and τ induce the same automorphism on P, it follows that τ induces on $\mathbb{F}_3P/(\hat{M})$ an inner automorphism, given by conjugation with the image of $\theta_i(u)$.

Set

$$w = q + a^2q^{-1}, \quad w' = -q - a^6q^{-1}.$$

Then $ww' = 1 - (1 + q + q^2) - a^2(1 + a^4)$, so $\theta_i(w)$ is a unit in Λ, with inverse $\theta_i(w')$. As $aw = (a^4q + a^2q^{-1})a^{-1}$, we have $\bar{a}\bar{w} = \bar{w}\bar{a}^{-1}$ in $\mathbb{Z}\bar{G}$ $(= \mathbb{Z}G/M)$, and $\bar{w}$ commutes with $\bar{b}$, $\bar{c}$ and $\bar{q}$. It follows that τ induces on $\mathbb{F}_2\bar{G}/(\hat{Q})$ an inner automorphism, given by conjugation with the image of w.

The group G_1

Recall that $\mathbb{Q}P/(\hat{M}) \cong \mathrm{Mat}_2(\mathbb{H})$, the isomorphism given by restriction of θ_1. Explicitly, set $\mathbf{i} = \left[\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right]$ and $\mathbf{j} = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$. Then $a \leftrightarrow \left[\begin{smallmatrix} 0 & 1 \\ \mathbf{i} & 0 \end{smallmatrix}\right]$, $b \leftrightarrow \left[\begin{smallmatrix} \mathbf{j} & 0 \\ 0 & \mathbf{j} \end{smallmatrix}\right]$ and $c \leftrightarrow \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$.

We already know that τ' on Λ is given by conjugation with $\left[\begin{smallmatrix} 0 & \mathbf{j} \\ \mathbf{j} & 0 \end{smallmatrix}\right]$, and that τ on $\mathbb{F}_2\bar{G}/(\hat{Q})$ is conjugation with the image of the unit $\theta_1(w)$ of Λ. Note that $\theta_1(w)$ and

$\theta_1(1+a^2)$ map to the same element in $\mathbb{F}_3P/(\hat{M})$, and that

$$\theta_1(b(a+ca^{-1})) = \left[\begin{smallmatrix} 0 & \mathbf{j} \\ \mathbf{j} & 0 \end{smallmatrix}\right] \cdot \theta_1(1+a^2) = \left[\begin{smallmatrix} 0 & \omega \\ \omega & 0 \end{smallmatrix}\right], \quad \text{where } \omega = \mathbf{j}(1+\mathbf{i}).$$

As $\omega^2 = -2$, the matrix $\left[\begin{smallmatrix} 3 & -8\omega \\ 4\omega & 21 \end{smallmatrix}\right]$ has determinant -1. Now $\theta_1(v) = \left[\begin{smallmatrix} 3 & -8\omega \\ 4\omega & 21 \end{smallmatrix}\right]$, where $v = 12 + 9c + 2(3c-1)b(a+ca^{-1})$, so $\theta_1(v)$ is a unit in Λ (with inverse $\left[\begin{smallmatrix} -21 & -8\omega \\ 4\omega & -3 \end{smallmatrix}\right]$, the image of $-12 + 9c + 2(3c-1)b(a+ca^{-1})$). Let λ be the inner automorphism of Λ given by conjugation with $\theta_1(v)\theta_1(w')$. As $v \equiv c \mod (2)$, $\bar{c}$ is central in $\bar{G}$ and τ has order 2, it follows that λ and τ induce the same automorphism on $\mathbb{F}_2\bar{G}/(\hat{Q})$. Moreover, $2\theta_1(v)\theta_1(w') \equiv 2\theta_1(b(a+ca^{-1}))\theta_1(w') \equiv \theta_1(u) \mod (3, q-1)$, so λ and τ induce also on $\mathbb{F}_3P/(\hat{M})$ the same automorphism. Hence there is an augmentation-preserving automorphism α of $\mathbb{Z}G$ which induces λ on Λ and τ on Γ, and by the group-theoretical obstruction, α has no Zassenhaus factorization.

The group G_2

In this case, we have $\mathbb{Q}P/(\hat{M}) \cong \mathrm{Mat}_4(\mathbb{Q})$ and $\mathbb{F}_3P/(\hat{M}) \cong \mathrm{Mat}_4(\mathbb{F}_3)$. Note that $\det(\theta_2(u)) = 16 \equiv 1 \mod (3)$. By [60, Lemma 2.2] (applied with $H = P$, $N = M$, $m = 3$, $\varphi = \tau$), there is an inner automorphism γ_1 of Γ which induces the identity mapping on $\mathbb{Z}\bar{G}$, and which agrees with τ on $\mathbb{F}_3P/(\hat{M})$. Further on, $\theta_1(w)$ and $\theta_1(1+a^2)$ map to the same element in $\mathbb{F}_3P/(\hat{M})$, and

$$\theta_2(1+a^2) = \begin{bmatrix} 1 & 1 & \cdot & \cdot \\ -1 & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & 1 \\ \cdot & \cdot & -1 & 1 \end{bmatrix}$$

has determinant 4, which is congruent 1 modulo 3. Again by [60, Lemma 2.2], there is an inner automorphism γ_2 of Γ which induces the identity mapping on $\mathbb{Z}\bar{G}$, and which induces on $\mathbb{F}_3P/(\hat{M})$ the same automorphism as conjugation with $\theta_2(w)$ on Λ does. Now conjugation with $\theta_2(w)$ and $\gamma_1\gamma_2$ differ on $\mathbb{F}_2\bar{G}/(\hat{Q}) \oplus \mathbb{F}_3P/(\hat{M})$ by the automorphism induced by τ. By the group-theoretical obstruction, these inner automorphisms give rise to an augmentation-preserving automorphism of $\mathbb{Z}G$ without Zassenhaus factorization.

12. ... but not the third one

In this section, we set $G = G_0$, $M = \langle b^2 \rangle$ and $\bar{G} = G/M$, as well as $\theta = \theta_0$. There are automorphisms τ and τ' of G of order two, defined by setting

$$\tau' : \begin{cases} a \mapsto a^{-1} \\ b \mapsto b \\ c \mapsto b^2c \\ q \mapsto q^{-1} \end{cases}, \quad \tau : \begin{cases} a \mapsto a^{-1} \\ b \mapsto b \\ c \mapsto b^2c \\ q \mapsto q \end{cases}.$$

Again, we have the following group-theoretical obstruction:

There is no $\sigma \in \mathrm{Aut}(G)$ which induces on Λ a central automorphism, and differs on Γ from τ by a central automorphism.

To that, the proof of the corresponding result in Section 11 can be copied word by word, except that each time a^4 occurs it has to replaced by b^2.

Let us see how τ acts on the various pieces over which the pullback for $\mathbb{Z}G$ is taken. Set $u = ((1+a^2)+(1-a^2)c)a^{-1}$. Then

$$\theta(u) = 2 \begin{bmatrix} \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot \end{bmatrix},$$

and one verifies that τ' induces on Λ a central automorphism, given by conjugation with the rational unit $\theta(u)$. Note that $\theta(u)^2$ is 4 times the identity matrix. Since τ' and τ induce the same automorphism on P, it follows that τ induces on $\mathbb{F}_3P/(\hat{M}) \cong \mathrm{Mat}_4(\mathbb{F}_3)$ an inner automorphism, given by conjugation with the image of $\theta(u)$, a matrix having determinant 1. Set $w = q + a^2q^{-1}$. Here, the image of w in Λ is not a unit, but the image of w in $\mathbb{F}_2\bar{G}/(\hat{Q})$ is again a unit, as one sees from $w^2 = -1 + 2a^2 + \hat{Q}$ and $(-1+2a^2)(1+2a^2) = 3$. And we have $aw = wa^{-1}$, $[w,c] = [w,q] = 1$ and $[\bar{w},\bar{b}] = 1$ (since $[b,a^2] = b^2$), so τ induces on $\mathbb{F}_2\bar{G}/(\hat{Q})$ an inner automorphism, given by conjugation with the image of w.

Since in the semilocal situation, "units lift to units", it readily follows that there is an augmentation-preserving automorphism of $\mathbb{Z}_{\pi(G)}G$, which permutes only the two faithful irreducible characters, therefore having no Zassenhaus factorization. (Of course, one may stick to the character-theoretic viewpoint introduced in [12,13], see also [127].)

Since the Zassenhaus conjecture holds for $\mathbb{Z}P$ and $\mathbb{Z}\bar{P}Q$, and $\mathrm{Out}_c(\bar{P}) = 1$, it follows from the description of Γ as a pullback that each augmentation-preserving automorphism of $\mathbb{Z}G$ acts on the irreducible characters of Γ in the same way as some group automorphism of G.

Thus we have shown that the Zassenhaus conjecture holds for $\mathbb{Z}G$ once we have proved that there is no augmentation-preserving automorphism of $\mathbb{Z}G$ which permutes only the two faithful irreducible characters.

12.1. Idea of the proof

By the normal subgroup correspondence, each automorphism of $\mathbb{Z}G$ induces automorphisms of Γ, Λ and $\bar{\Lambda}$. We assume that there are $\gamma \in \mathrm{Autcent}(\Gamma)$ and $\lambda \in \mathrm{Autcent}(\Lambda)$ which induce automorphisms of $\bar{\Lambda}$ and differ on this quotient by the inner automorphism induced by τ, and then we finally have to reach a contradiction. Recall that $\mathbb{Z}G$ is the

pullback

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \Gamma \\ \downarrow & & \downarrow \\ \Lambda & \longrightarrow & \bar{\Lambda} = \Lambda_2 \oplus \Lambda_3 \end{array}, \quad \text{where } \Lambda_2 = \mathbb{F}_2\bar{G}/(\hat{Q}),\ \Lambda_3 = \mathbb{F}_3P/(\hat{M}),$$

and that we may identify Λ with $\theta(\mathbb{Z}G)$, and Λ_3 with $\mathrm{Mat}_4(\mathbb{F}_3)$.

The pullback diagram for Γ fits into a larger diagram:

$$\begin{array}{ccccccc} \Gamma & \longrightarrow & \mathbb{Z}P & \longrightarrow & \mathbb{Z}P/(\hat{M}) & \xrightarrow{\text{mod } 3} & \Lambda_3 = \mathbb{F}_3P/(\hat{M}) \cong \mathrm{Mat}_4(\mathbb{F}_3) \\ \downarrow & & \downarrow & & \downarrow & & \\ \mathbb{Z}\bar{P}Q & \longrightarrow & \mathbb{Z}\bar{P} & \longrightarrow & \mathbb{F}_2\bar{P} & & \\ \downarrow & & \downarrow & & & & \\ \mathbb{Z}\bar{P}Q/(\hat{Q}) & \longrightarrow & \mathbb{F}_3\bar{P} & & & & \\ \text{mod } 2 \downarrow & & & & & & \\ \Lambda_2 = \mathbb{F}_2\bar{P}Q/(\hat{Q}) & & & & & & \end{array}$$

Note that a central automorphism of Γ induces central automorphisms on all quotients displayed in the diagram.

The automorphisms γ and λ induce automorphisms of Λ_2 and Λ_3. (For example, the kernel of the projection of Λ onto Λ_3 consists of those $x \in \Lambda$ for which $2x$ is contained in the kernel of the map $\Lambda \to \bar{\Lambda}$, which is stabilized by λ. Hence λ induces an automorphism of Λ_2.)

By the Skolem–Noether Theorem, γ and λ induce inner automorphisms of Λ_3. These automorphisms differ by conjugation with the image of $\theta(u)$, a matrix with determinant 1. Since the image of $\theta(a)$ in Λ_3 has determinant -1, we can assume that both γ and λ induce on Λ_3 conjugations with matrices of determinant 1.

Look at the following part of the above diagram:

$$\begin{array}{ccc} \mathbb{Z}P & \longrightarrow & \mathrm{Mat}_4(\mathbb{F}_3) \\ \downarrow & & \\ \mathbb{F}_3\bar{P} & & \end{array} .$$

We have $\mathbb{F}_3\bar{P} \cong \mathbb{F}_3\bar{P}/\bar{P}' \oplus \mathrm{Mat}_2(\mathbb{F}_3) \oplus \mathrm{Mat}_2(\mathbb{F}_3)$. For any automorphism β of $\mathbb{F}_3\bar{P}$ which fixes the two 2×2-matrix rings (and which is therefore conjugation with matrices M_1 and M_2 on these blocks) we define a norm by setting

$$\mathrm{N}_1(\beta) = \det(M_1) \cdot \det(M_2) \in \{\pm 1\}$$

(which is apparently well defined).

At this point, it should be remarked that instead of G, one could have defined more generally a family of groups, by letting G_p be the semidirect product where the Sylow 2-subgroup P acts on a cyclic group of odd prime order p in the same way as P acts on Q (so that $G = G_3$). Then the discussion below essentially shows that, for example, G_5 does *not* satisfy the Zassenhaus conjecture (which illustrates the remarks made at the beginning of Section 10).

Given any $\alpha \in \mathrm{Autcent}(\mathbb{Z}P)$, we define a norm $\mathrm{N}(\alpha)$ as follows: α induces a central automorphism $\bar{\beta}$ of $\mathbb{F}_3\bar{P}$ and a central automorphism of $\mathrm{Mat}_4(\mathbb{F}_3)$, say conjugation with the matrix T, and we set

$$\mathrm{N}(\alpha) = \mathrm{N}_1(\bar{\beta}) \cdot \det(T) \in \{\pm 1\}.$$

In Subsection 12.2, we show that $\mathrm{N}(\alpha) = 1$ for any $\alpha \in \mathrm{Autcent}(\mathbb{Z}P)$.

Now consider the following diagram:

$$\begin{array}{ccc} \Omega := \mathbb{Z}\bar{P}Q/(\hat{Q}) & \longrightarrow & \mathbb{F}_3\bar{P} \\ \downarrow & & \\ \Lambda \longrightarrow \Lambda_2 = \mathbb{F}_2\bar{P}Q/(\hat{Q}) & & \end{array}$$

Let H be the subgroup of $\mathrm{Autcent}(\Lambda)$ consisting of those α which induce a central automorphism of Λ_2, which, furthermore, can be lifted to a central automorphism of Ω. (We remark that τ' induces a central automorphism of Λ, but a non-central automorphism of Λ_2.) Note that any automorphism β of Ω induces an automorphism of $\mathbb{F}_3\bar{P}$ (If we start with Ω, factor out (3) and then the radical, we arrive at $\mathbb{F}_3\bar{P}$.) If $\beta \in \mathrm{Autcent}(\Omega)$ induces $\bar{\beta}$ on $\mathbb{F}_3\bar{P}$, then $\mathrm{N}_1(\bar{\beta})$ is defined.

If $\alpha \in \mathrm{Autcent}(\Lambda)$ and $\beta \in \mathrm{Autcent}(\Omega)$ induce the same automorphism of Λ_2, set $d(\alpha) = \mathrm{N}_1(\bar{\beta})$. If α is an inner automorphism, say conjugation with $s \in \Lambda^\times$, set $d(s) = d(\alpha)$. In Subsection 12.3, we show that this yields a well defined homomorphism $d : H \to \{\pm 1\}$. We shall see that $H \leq \mathrm{Inn}(\Lambda)$. The author would very much like to know whether there is same general argument showing that d is induced by the determinantal map.

In Subsection 12.3, we show that if $s \in \Lambda^\times$, and there is $\alpha \in \mathrm{Autcent}(\mathbb{Z}\bar{P}Q)$ which induces on Λ_2 the inner automorphism given by conjugation with the image of s, then $\det(s) = \pm 1$, and $\det(s) = 1$ if and only if $d(s) = 1$. This is done by carefully modifying s and α until the claim will be obvious.

In Subsection 12.4, we show that there is $\alpha \in \mathrm{Autcent}(\mathbb{Z}\bar{P}Q)$ which induces on Λ_2 the same automorphism as τ, and induces on $\mathbb{F}_3\bar{P}$ an automorphism β with $\mathrm{N}_1(\beta) = -1$. This will provide the final contradiction.

12.2. Norms of units in $\mathbb{Z}P$

The commutator subgroup of P is $P' = \langle b^2, c\rangle$, and $\tilde{P} = P/P' = \langle \tilde{a}\rangle \times \langle \tilde{b}\rangle \cong C_4 \times C_2$. Let ε be the idempotent $\frac{1}{4}\widehat{P'}$, and set $\eta = 1-\varepsilon$. There are two 2-dimensional irreducible representations ρ_+ and ρ_- of P:

$$\rho_\pm(a) = \begin{bmatrix} 0 & 1 \\ \pm 1 & 0 \end{bmatrix}, \quad \rho_\pm(b) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \rho_\pm(c) = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

We have $\eta\mathbb{Q}P \cong \mathrm{Mat}_2(\mathbb{Q}) \times \mathrm{Mat}_2(\mathbb{Q}) \times \mathrm{Mat}_4(\mathbb{Q})$, which we treat as an identification via $\eta x = (\rho_+(x), \rho_-(x), \theta(x))$, $x \in \mathbb{Q}P$. We define a norm $\mathrm{N}(x)$ for $x \in \mathbb{Z}P$ (or, more generally, for $x \in \mathbb{Q}P$) by setting

$$\mathrm{N}(x) = \det(\rho_+(x)) \cdot \det(\rho_-(x)) \cdot \det(\theta(x)).$$

Note that the group automorphism τ induces on $\eta\mathbb{Z}P$ a central automorphism, given by conjugation with the rational unit

$$x = \left(\begin{bmatrix} 1 & \cdot \\ \cdot & 1 \end{bmatrix}, \begin{bmatrix} -1 & \cdot \\ \cdot & 1 \end{bmatrix}, \begin{bmatrix} \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot \end{bmatrix} \right)$$

satisfying $\mathrm{N}(x) = -1$.

Our goal is to show that the restriction of any $\alpha \in \mathrm{Autcent}(\mathbb{Z}P)$ to $\eta\mathbb{Z}P$ is given by conjugation with a unit x of $\eta\mathbb{Z}P$ satisfying $\mathrm{N}(x) = 1$.

First of all, we consider inner automorphisms of $\mathbb{Z}P$. Note that the number of non-isomorphic simple $\mathbb{R}P$-modules coincides with the corresponding number of $\mathbb{Q}P$-modules. By a theorem of Bass (see [27, 45.21]) it follows that the Whitehead group $\mathrm{K}_1(\mathbb{Z}P)$ is a torsion group. Then, it follows from Wall's theorem (see [27, 46.4]) that $\mathrm{K}_1(\mathbb{Z}P) = \{\pm 1\} \times \tilde{P} \times \mathrm{SK}_1(\mathbb{Z}P)$. Note that the composition $(\mathbb{Z}P)^\times \hookrightarrow \mathrm{K}_1(\mathbb{Z}P) \xrightarrow{\phi} \mathrm{K}_1(\mathbb{Q}P) \xrightarrow{\det\circ\mathrm{N}} \mathbb{Q}$ (of the obvious maps) is just the norm map. Since $\mathrm{N}(\pm P) = 1$, and $\mathrm{SK}_1(\mathbb{Z}P)$ is by definition the kernel of ϕ, it follows that all units in $\mathbb{Z}P$ have norm 1.

Next, note that $\mathrm{Picent}(\mathbb{Z}_r P) = 1$ for an odd prime r (cf. [27, 55.48]), and that $\mathrm{Picent}(\mathbb{Z}_2 P) = 1$ by a famous result of Roggenkamp and Scott [119] (note that $\mathrm{Out}_c(P) = 1$). Thus we have to focus on the subgroup $\mathrm{Cl}_{\mathbb{Z}P}(\mathrm{Z}(\mathbb{Z}P))$ of the locally free class group $\mathrm{Cl}(\mathrm{Z}(\mathbb{Z}P))$ consisting of those isomorphism classes of invertible ideals $\mathfrak{a}$ in $\mathrm{Z}(\mathbb{Z}P)$ so that $\mathfrak{a}\mathbb{Z}P$ is a principal ideal in $\mathbb{Z}P$ (see Remark 10.3). The locally free class group can be studied using Mayer-Vietoris sequences.

Set $\Delta = \mathrm{Z}(\mathbb{Z}P)$. Note that $\Delta^\times = \{\pm 1\} \times C_2$ by a classical result of Higman, since $\mathbb{Z}[i]$ has only units of finite order.

We shall show that $(\eta\Delta)^\times \cong \{\pm 1\} \times C_2$ and $\mathrm{Cl}(\eta\Delta) = 0$. Computing the values $|P : \mathrm{C}_P(g)|\chi(g)/\chi(1)$ for the three relevant characters, one sees that $\eta\Delta$ is generated as $\mathbb{Z}$-module by the columns of the matrix

$$\begin{bmatrix} 1 & -2 & -2 & 2 & 1 \\ 1 & 2 & -2 & -2 & 1 \\ 1 & 0 & 0 & 0 & -1 \end{bmatrix}$$

(and multiplication of two columns is performed entry by entry). We shall write $\eta\Delta = \left\{ \begin{smallmatrix} 1 & \cdots \\ 1 & \cdots \\ 1 & \cdots \end{smallmatrix} \right\}$. Elementary transformations show that

$$\eta\Delta = \left\{ \begin{matrix} 1 & 0 & 0 \\ 1 & 4 & 0 \\ 1 & 0 & 2 \end{matrix} \right\}.$$

This shows that $(\eta\Delta)^\times \cong \{\pm 1\} \times C_2$. There are ideals

$$I = \left\{ \begin{matrix} 0 \\ 0 \\ 2 \end{matrix} \right\} \quad \text{and} \quad J = \left\{ \begin{matrix} 2 & 0 \\ 2 & 4 \\ 0 & 0 \end{matrix} \right\}$$

of $\eta\Delta$ with $I \cap J = 0$. Obviously $\eta\Delta/I \cong \left\{ \begin{smallmatrix} 1 & 0 \\ 1 & 4 \end{smallmatrix} \right\}$ and $\eta\Delta/J \cong \left\{ \begin{smallmatrix} 1 \\ 1 \\ 1 \end{smallmatrix} \right\} \cong \mathbb{Z}$. We have a pullback diagram

$$\begin{array}{ccc} \left\{ \begin{smallmatrix} 1 & 0 \\ 1 & 4 \end{smallmatrix} \right\} & \xrightarrow{\mathrm{mod} \left\{ \begin{smallmatrix} 0 \\ 4 \end{smallmatrix} \right\}} & \mathbb{Z} \\ {\scriptstyle \mathrm{mod} \left\{ \begin{smallmatrix} 4 \\ 0 \end{smallmatrix} \right\}} \downarrow & & \downarrow \\ \mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} \end{array}$$

giving rise to an exact Mayer-Vietoris sequence (see [27, 49.28])

$$1 \longrightarrow \{\pm 1\} \longrightarrow \{\pm 1\} \times \{\pm 1\} \longrightarrow \{\pm 1\} \longrightarrow \mathrm{Cl}(\eta\Delta/I) \longrightarrow 0.$$

This shows that $\mathrm{Cl}(\eta\Delta/I) = 0$. The Mayer-Vietoris sequence associated to the pullback diagram

$$\begin{array}{ccc} \eta\Delta & \xrightarrow{\mathrm{mod}\ J} & \left\{ \begin{smallmatrix} 1 \\ 1 \\ 1 \end{smallmatrix} \right\} \\ {\scriptstyle \mathrm{mod}\ I} \downarrow & & \downarrow \\ \left\{ \begin{smallmatrix} 1 & 0 \\ 1 & 4 \end{smallmatrix} \right\} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \end{array}$$

now reads

$$1 \longrightarrow \{\pm 1\} \times C_2 \longrightarrow \{\pm 1\} \times \{\pm 1\} \longrightarrow 1 \longrightarrow \mathrm{Cl}(\eta\Delta) \longrightarrow 0.$$

Thus $\mathrm{Cl}(\eta\Delta) = 0$ as claimed.

Next we describe $\varepsilon\Delta$. The class length of a^2 is 2, and the elements a, a^3, b, ab, a^2b and a^3b all have class length 4. Consequently

$$\varepsilon\Delta = \mathbb{Z} + 2\mathbb{Z}\langle\tilde{a}^2\rangle + 4\mathbb{Z}\langle\tilde{a}, \tilde{b}\rangle.$$

Note that $(\varepsilon\Delta)^\times = \{\pm 1\}$ by a classical result of Higman. We shall have no need to calculate $\mathrm{Cl}(\varepsilon\Delta)$, but we will demonstrate that $\mathrm{Cl}(\varepsilon\Delta)$ contains elements of order 4. This will be used in Subsection 12.5 to illustrate how subtle things are.

We have $O = \mathbb{Z} + 2\mathbb{Z}\langle\tilde{a}^2\rangle + 4\mathbb{Z}\langle\tilde{a}\rangle \cong \varepsilon\Delta/(4(\tilde{b}-1)) \cong \varepsilon\Delta/(4(\tilde{b}+1))$, so there is a pullback diagram

$$\begin{array}{ccc} \varepsilon\Delta & \longrightarrow & O \\ \downarrow & & \downarrow \\ O & \longrightarrow & O/8O \end{array}$$

which gives rise to the Mayer-Vietoris sequence

$$1 \longrightarrow (\varepsilon\Delta)^\times \longrightarrow O^\times \times O^\times \longrightarrow (O/8O)^\times \longrightarrow \mathrm{Cl}(\varepsilon\Delta) \longrightarrow \mathrm{Cl}(O) \oplus \mathrm{Cl}(O) \longrightarrow 0.$$

It is routine to verify that $(O/8O)^\times$ has order 64, exponent 4, and exactly 8 elements of order ≤ 2. Hence $(O/8O)^\times \cong C_4^{(3)}$, the exact sequence reads

$$1 \longrightarrow C_2 \longrightarrow C_2 \times C_2 \longrightarrow C_4^{(3)} \longrightarrow \mathrm{Cl}(\varepsilon\Delta) \longrightarrow \mathrm{Cl}(O) \oplus \mathrm{Cl}(O) \longrightarrow 0,$$

and it follows that $\mathrm{Cl}(\varepsilon\Delta)$ has a subgroup isomorphic to $C_4 \times C_4 \times C_2$.

The well known pullback diagram

$$\begin{array}{ccc} \mathbb{Z}P & \xrightarrow{f_1} & \mathbb{Z}P/P' \\ {\scriptstyle f_2}\downarrow & & \downarrow{\scriptstyle g_1} \\ \mathbb{Z}P/(\widehat{P'}) & \xrightarrow[g_2]{} & (\mathbb{Z}/4\mathbb{Z})\,(P/P') \end{array}$$

also describes Δ as a pullback: Setting $\Delta_1 = \Delta f_1 \cong \varepsilon\Delta$, $\Delta_2 = \Delta f_2 \cong \eta\Delta$ and $\bar{\Delta} = \Delta f_1 g_1$, we get a pullback diagram

$$\begin{array}{ccc} \Delta & \longrightarrow & \Delta_1 \\ \downarrow & & \downarrow \\ \Delta_2 & \longrightarrow & \bar{\Delta} \end{array}$$

From the description of $\varepsilon\Delta$ it follows that $\bar{\Delta}^\times = \{\pm 1\} \times \langle 1 + 2\tilde{a}^2 \rangle \cong C_2 \times C_2$. Putting everything together, we get an exact Mayer-Vietoris sequence

$$1 \longrightarrow C_2 \times C_2 \longrightarrow C_2 \times C_2 \times C_2 \longrightarrow C_2 \times C_2 \xrightarrow{\partial} \mathrm{Cl}(\Delta) \xrightarrow{f} \mathrm{Cl}(\Delta_1) \longrightarrow 0.$$

Now let $\mathfrak{a}$ be an invertible ideal in Δ such that $\mathfrak{a}\mathbb{Z}P = u\mathbb{Z}P$ for some $u \in \mathbb{Z}P$, that is, $[\mathfrak{a}] \in \mathrm{Cl}_{\mathbb{Z}P}(\Delta)$. Then $[\mathfrak{a}]f = [\tilde{\mathfrak{a}}]$ where $\tilde{\mathfrak{a}} := \mathfrak{a}f_1$ is an invertible ideal in Δ_1 such that $\tilde{\mathfrak{a}}\mathbb{Z}\tilde{P} = \tilde{u}\mathbb{Z}\tilde{P}$. Note that $u \in (\mathbb{Q}P)^\times$, so $\tilde{u}^{-1}x \cdot y = 1$ for some $x \in \tilde{\mathfrak{a}}$ and $y \in \mathbb{Z}\tilde{P}$. As $\tilde{u}^{-1}x \in \mathbb{Z}\tilde{P}$, it follows that $\tilde{u}^{-1}x \in (\mathbb{Z}\tilde{P})^\times$. Hence we may assume that $x = \tilde{u}$. Then $1 \in x^{-1}\tilde{\mathfrak{a}} \subset \mathbb{Z}\tilde{P}$, and $x^{-1}\tilde{\mathfrak{a}} \cong \tilde{\mathfrak{a}}$ as Δ_1-lattices. In particular, $\mathbb{Z}_2 \otimes_{\mathbb{Z}} x^{-1}\tilde{\mathfrak{a}} \cong \mathbb{Z}_2\Delta_1$ as $\mathbb{Z}_2\Delta_1$-lattices. Thus, if we set $X_n = \mathbb{Z}/2^n\mathbb{Z} \otimes_{\mathbb{Z}} x^{-1}\tilde{\mathfrak{a}}$ and $Y_n = \mathbb{Z}/2^n\mathbb{Z} \otimes_{\mathbb{Z}} \Delta_1$ for $n \in \mathbb{N}$, we have $X_n \cong Y_n$. Note that $Y_n \subseteq X_n$, so we have in fact equality, and it follows that $x^{-1}\tilde{\mathfrak{a}} \subset \Delta_1$. Thus $x^{-1}\tilde{\mathfrak{a}} = \Delta_1$, $[\mathfrak{a}]f = [\tilde{\mathfrak{a}}] = 0$, and consequently $[\mathfrak{a}] \in \mathrm{im}(\partial)$.

Assume that $[\mathfrak{a}] \neq 0$. Then, by the description of $\bar{\Delta}^\times$ and the map ∂, we have $[\mathfrak{a}] = v\partial = [M(v)]$, where $v = 1 + 2\tilde{a}^2$ and

$$M(v) = \{(x_1, x_2) \in \Delta_1 \oplus \Delta_2 \mid v\bar{x}_1 = \bar{x}_2 \text{ in } \bar{\Delta}\}.$$

By assumption, the $\mathbb{Z}P$-module

$$X := M(v)\mathbb{Z}P = \{(x_1, x_2) \in \mathbb{Z}\tilde{P} \oplus \mathbb{Z}P/(\widehat{P'}) \mid v\bar{x}_1 = \bar{x}_2 \text{ in } (\mathbb{Z}/4\mathbb{Z})\,(P/P')\}$$

gives rise to the zero element in $\mathrm{Cl}(\mathbb{Z}P)$. Since $\mathbb{Q}P = \text{Eichler}/\mathbb{Z}$, we have (see [27, 49.30])

$$v = (x_1 g_1)(x_2 g_2) \quad \text{for some } x_1 \in (\mathbb{Z}\tilde{P})^\times,\ x_2 \in (\mathbb{Z}P/(\widehat{P'}))^\times. \tag{$*$}$$

We have seen that $\mathrm{Outcent}(\mathbb{Z}P)$ is either trivial or cyclic of order 2, corresponding to whether $(*)$ holds or not. Assume that $(*)$ is satisfied. Since $\mathbb{Z}\tilde{P}$ has only trivial units, we then have $v = xg_1$ for some $x \in (\mathbb{Z}P/(\widehat{P'}))^\times$. We wish to show that $\mathrm{N}(x) = 1$. Note that $\eta(1 + a^2 + b^{-1}a^2b) = (-\mathrm{id}, 3 \cdot \mathrm{id}, \mathrm{id})$. This element differs from x by some element of $\eta \mathrm{I}_{\mathbb{Z}}(P')P$, where $\mathrm{I}_{\mathbb{Z}}(P')$ denotes the augmentation ideal of P'. Note that $\eta(1 - b^2) = (0, 0, 2 \cdot \mathrm{id})$, and that the elements $\eta(1 - c)$ and $\eta(1 - b^2c)$ are given by

$$\left(\begin{bmatrix} 2 & \cdot \\ \cdot & 2 \end{bmatrix}, \begin{bmatrix} 2 & \cdot \\ \cdot & 2 \end{bmatrix}, \begin{bmatrix} 2 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 2 & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix} \right), \quad \left(\begin{bmatrix} 2 & \cdot \\ \cdot & 2 \end{bmatrix}, \begin{bmatrix} 2 & \cdot \\ \cdot & 2 \end{bmatrix}, \begin{bmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & 2 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 2 \end{bmatrix} \right)$$

respectively. It can be checked that the image of $\eta\mathbb{Z}P$ in $\mathrm{Mat}_2(\mathbb{F}_2) \times \mathrm{Mat}_2(\mathbb{F}_2) \times \mathrm{Mat}_4(\mathbb{F}_2)$ consists of elements of the form

$$\left(\begin{bmatrix} a_1 + a_3 & a_2 + a_4 \\ a_2 + a_4 & a_1 + a_3 \end{bmatrix}, \begin{bmatrix} a_1 + a_3 & a_2 + a_4 \\ a_2 + a_4 & a_1 + a_3 \end{bmatrix}, \begin{bmatrix} a_3 & a_2 & a_1 & a_4 \\ a_2 & a_3 & a_4 & a_1 \\ a_1 & a_4 & a_3 & a_2 \\ a_4 & a_1 & a_2 & a_3 \end{bmatrix} \right)$$

with $a_1, \ldots, a_4 \in \mathbb{F}_2$. This allows us to compute the norm $\mathrm{N}(x)$ modulo 4. For example, consider the projection x_3 of x on the 4×4-matrix ring. Modulo 4, the diagonal entries of x_3 are of the form $\overline{1+2s}$, $\overline{1+2t}$, $\overline{1+2s}$, $\overline{1+2t}$, and the off-diagonal entries of x_3 are even. This shows that $\det(x_3) \equiv 1 \mod 4$. As x is a unit in $\eta\mathbb{Z}P$, it follows that $\det(x_3) = 1$. We can argue similarly for the projections of x on the other components. Hence we obtain $\mathrm{N}(x) = 1$, as desired.

12.3. Norms of units in Λ and Ω

We consider the following diagram:

$$\begin{array}{ccccc} \mathbb{Z}G/(\hat{Q}) & \longrightarrow & \Omega := \mathbb{Z}\bar{P}Q/(\hat{Q}) & \longrightarrow & \mathbb{F}_3\bar{P} \\ \downarrow & & \downarrow & & \\ \Lambda & \longrightarrow & \Lambda_2 = \mathbb{F}_2\bar{P}Q/(\hat{Q}) & & \end{array}$$

In the next subsection, we will see that $\lambda \in \mathrm{Autcent}(\Lambda)$ (the automorphism which differs from $\gamma \in \mathrm{Autcent}(\Gamma)$ on the quotient $\bar{\Lambda} = \Lambda_2 \oplus \Lambda_3$ by the inner automorphism induced by τ) induces on Λ_2 an automorphism which can be lifted to a central automorphism of $\mathbb{Z}\bar{P}Q$ (so we will lift the inner automorphism of Λ_2 induced by τ). Such automorphisms will be analyzed in this subsection.

First, we give the irreducible representations of $\mathbb{C}\Omega$. We have $\dim_{\mathbb{C}}(\mathbb{C}\Omega) = 32$, and it easily follows that $\mathbb{C}\Omega$ is isomorphic to the direct sum of eight copies of $\mathrm{Mat}_2(\mathbb{C})$. We treat this isomorphism as identification, the images of the group elements corresponding to:

$$\begin{aligned}
a &\leftrightarrow \left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right), \\
b &\leftrightarrow \left(\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right), \\
c &\leftrightarrow \left(\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right), \\
q &\leftrightarrow \left(\begin{bmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{bmatrix}, \begin{bmatrix} \zeta^2 & 0 \\ 0 & \zeta \end{bmatrix}, \begin{bmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{bmatrix}, \begin{bmatrix} \zeta^2 & 0 \\ 0 & \zeta \end{bmatrix}, \begin{bmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{bmatrix}, \begin{bmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{bmatrix}, \begin{bmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{bmatrix}, \begin{bmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{bmatrix} \right).
\end{aligned}$$

Recall that any $\beta \in \mathrm{Autcent}(\Omega)$ induces an automorphism $\bar{\beta}$ of $\mathbb{F}_3\bar{P}$, for which we have defined a norm $\mathrm{N}_1(\bar{\beta})$. We show how to compute this norm in $\mathbb{C}\Omega$. Note that the first component of $\mathbb{C}\Omega$ corresponds to a representation with kernel $\langle a^2 \rangle$, and that the third component corresponds to a faithful representation. It follows that we may identify the group ring $\mathbb{F}_3\bar{P}$ with $\mathbb{F}_3\bar{P}/\bar{P}' \oplus \mathrm{Mat}_2(\mathbb{F}_3) \oplus \mathrm{Mat}_2(\mathbb{F}_3)$, and that an element $(M_1, \ldots, M_8)$ of Ω maps to an element of the form $(*, \tilde{M}_1, \tilde{M}_3)$, where $\tilde{}$ indicates "reduction mod $1-\zeta$". Let $\beta \in \mathrm{Autcent}(\Omega)$, inducing $\bar{\beta}$ on $\mathbb{F}_3\bar{P}$. Then β is conjugation with a rational unit $(T_1, \ldots, T_8)$. We will show that T_1 and T_3 can be chosen to lie in $\mathrm{GL}_2(\mathbb{Z}[\zeta])$, and having determinant ± 1. Clearly $\bar{\beta}$ on the 2×2-matrix blocks is conjugation with $(\tilde{T}_1, \tilde{T}_3)$, so

that $\mathrm{N}_1(\bar{\beta}) = \det(T_1) \cdot \det(T_3)$. Let φ_+ and φ_- be the projection of $\mathbb{C}G$ onto the first and third component of $\mathbb{C}\Omega$, respectively. We treat both projections simultaneously. There is $T \in \mathrm{GL}_2(\mathbb{Q}(\zeta))$ such that $T^{-1}(g\varphi_\pm)T = g\varphi_\pm\beta$ for all $g \in G$. If $T = \left[\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right]$, and $d = \det(T)$, then

$$
\begin{aligned}
a\varphi_\pm\beta &= \frac{1}{d}\begin{bmatrix} \mp st + uv & \mp t^2 + v^2 \\ \pm s^2 - u^2 & \pm st - uv \end{bmatrix}, \\
b\varphi_\pm\beta &= \frac{1}{d}\begin{bmatrix} -tu - sv & -2tv \\ 2su & sv + tu \end{bmatrix}, \\
q\varphi_\pm\beta &= \frac{1}{d}\begin{bmatrix} tu + (tu + sv)\zeta & tv + 2tv\zeta \\ -su - 2su\zeta & -sv - (sv + tu)\zeta \end{bmatrix}.
\end{aligned}
$$

Note that $\mathbb{Z}[\zeta]$ is a principal ideal domain, with group of units $\{\pm 1\} \times \langle\zeta\rangle$. We may assume that all entries of T lie in $\mathbb{Z}[\zeta]$ and are relatively prime. The entries of the above displayed matrices all lie in $\mathbb{Z}[\zeta]$. From the entries of the first matrix we read off $d \mid \pm s^2 - u^2$ and $d \mid \mp t^2 + v^2$. From the entries of the two other matrices we read off $d \mid su$ and $d \mid tv$. Altogether, it follows that $d \mid s, t, u, v$, so d is a unit by assumption, and we clearly can assume that $d = \pm 1$.

Note that any $\alpha \in \mathrm{Autcent}(\Lambda)$ and $\beta \in \mathrm{Autcent}(\Omega)$ which induce the same automorphism of Λ_2 give rise to a central automorphism of $\mathbb{Z}G/(\hat{Q})$. Using Fröhlich's localization sequence, we will show that any central automorphism of $\mathbb{Z}G/(\hat{Q})$ induces an inner automorphism of Λ. In particular, λ is an inner automorphism. For any prime p, let R_p be the ring of algebraic integers in $\mathbb{Q}_p(\zeta)$.

If $p \neq 2, 3$ then $R_p\Lambda := R_p \otimes_{\mathbb{Z}} \Lambda \cong \mathrm{Mat}_4(R_p) \oplus \mathrm{Mat}_4(R_p)$, so $\mathrm{Outcent}(R_p\Lambda) = 1$ since R_p is a local ring.

Since the restriction of θ to the Sylow subgroup P is irreducible, and $R_3\Lambda = \mathbb{Z}_3[\zeta] \otimes_{\mathbb{Z}} \Lambda$ does not contain the central primitive idempotent belonging to θ, it follows from Schur relations that $\mathbb{Z}_3[\zeta]\Lambda$ is a pullback

$$
\begin{array}{ccc}
\mathbb{Z}_3[\zeta]\Lambda & \longrightarrow & \mathrm{Mat}_4(\mathbb{Z}_3[\zeta]) \\
\downarrow & & \downarrow \\
\mathrm{Mat}_4(\mathbb{Z}_3[\zeta]) & \longrightarrow & \mathrm{Mat}_4(\mathbb{F}_3)
\end{array}
$$

Again, it follows that $\mathrm{Outcent}(R_3\Lambda) = 1$. (We have $\mathrm{Outcent}(R_2\Lambda) \neq 1$, for τ' induces an outer central automorphism of Λ.)

Calculating the norm and the trace of an element of $\mathbb{Q}_2(\zeta)$, one sees that $R_2 = \mathbb{Z}_2[\zeta]$,

with residue class field $\mathbb{Z}_2[\zeta]/2\mathbb{Z}_2[\zeta] = \mathbb{F}_4$. Thus we have a pullback diagram

$$\begin{array}{ccc} \mathbb{Z}_2[\zeta]G/(\hat{Q}) & \longrightarrow & \mathbb{Z}_2[\zeta]\bar{G}/(\hat{Q}) \\ \downarrow & & \downarrow \\ \mathbb{Z}_2[\zeta]\Lambda & \longrightarrow & \mathbb{F}_4\bar{G}/(\hat{Q}) \end{array}$$

The idempotent $e = (1 + \zeta^2 q + \zeta q^2)/3$ of R_2Q has inertia group $T = \langle a^2, b, c\rangle \times \langle q\rangle$ in G. Clearly $eR_2T \cong R_2H$, where $H = \langle a^2, b, c\rangle$. Thus by Clifford theory,

$$R_2G/(\hat{Q}) \cong \mathrm{Mat}_2(R_2H), \quad R_2\bar{G}/(\hat{Q}) \cong \mathrm{Mat}_2(R_2\bar{H}), \quad \mathbb{F}_4\bar{G}/(\hat{Q}) \cong \mathrm{Mat}_2(\mathbb{F}_4\bar{H}).$$

We have $\mathrm{Outcent}(\mathrm{Mat}_2(R_2H)) \hookrightarrow \mathrm{Picent}(\mathrm{Mat}_2(R_2H)) \cong \mathrm{Picent}(R_2H)$ by [27, 55.11, 55.9]. Since $\mathrm{Out_c}(H) = 1$, it follows from [119] that $\mathrm{Picent}(R_2H) = 1$. Hence

$$\mathrm{Outcent}(R_2G/(\hat{Q})) = 1,$$

and any central automorphism of $\mathbb{Z}G/(\hat{Q})$ induces an inner automorphism of $R_2\Lambda$.

From the interpretation of an automorphism as an invertible bimodule and a result due to Reiner and Zassenhaus (see [28, §35 exercise 13, (30.25)]), it follows that any central automorphism of $\mathbb{Z}G/(\hat{Q})$ induces an inner automorphism of $\mathbb{Z}_p\Lambda$ for all primes p.

For later use, we remark that $\mathrm{Outcent}(\mathbb{Z}_2\bar{G}/(\hat{Q})) = 1$, which is proved in the very same way.

Note that the center of Λ is $\mathbb{Z}[\sqrt{-3}]$ (the scalar $\sqrt{-3}$ corresponds to the class sum of cq), and $\mathrm{Cl}(\mathbb{Z}[\sqrt{-3}]) = 0$. By Fröhlich's localization sequence (see Remark 10.3), it follows that any central automorphism of $\mathbb{Z}G/(\hat{Q})$ induces an inner automorphism of Λ.

Let $\psi \in \mathrm{Autcent}(\mathbb{Z}G/(\hat{Q}))$. Then ψ induces an automorphism $\bar{\psi}$ of $\mathbb{F}_3\bar{P}$ for which the norm $\mathrm{N}_1(\bar{\psi})$ is defined. Assume that ψ induces the identity on Λ_2; we will show that $\mathrm{N}_1(\bar{\psi}) = 1$. The automorphism ψ induces a central automorphism of $\mathbb{Z}_2\Omega$ which is modulo 2 the identity. It follows that ψ induces an inner automorphism of $\mathbb{Z}_2\Omega$, given by conjugation with a unit from $1 + 2 \cdot \mathbb{Z}_2\Omega$ (see [62, Theorem 3.9, Remark 3.10]). Let M_1 and M_3 be their projection on the first and third component of $\mathbb{Q}_2(\zeta)\Omega$, respectively. We already know that on these components, ψ is given by conjugation with matrices $T_1, T_3 \in \mathrm{GL}_2(\mathbb{Z}[\zeta])$ of determinant ± 1. Since M_i and T_i differ by a scalar, there are $s, t \in \mathbb{Z}_2[\zeta] \setminus \{0\}$ such that $s^2\det(M_1)\det(M_3) = t^2\det(T_1)\det(T_3) = \pm t^2$. We may assume that s is a unit in $\mathbb{Z}_2[\zeta]$, and then t is a unit, too. Note that s^2 and t^2 are congruent to a power of ζ modulo 4. We compute $\det(M_1)\det(M_3)$ modulo 4. The projection of $\mathbb{Z}_2[\zeta]\Omega$ on the first and third component is

$$\left\{ \left(\begin{bmatrix} x_1 & x_2 + 2x_3 \\ \bar{x}_2 & \bar{x}_1 + 2\bar{x}_4 \end{bmatrix}, \begin{bmatrix} x_1 + 2x_5 & x_2 + 2x_3 + 2x_6 + 4x_7 \\ -\bar{x}_2 - 2\bar{x}_6 & \bar{x}_1 + 2\bar{x}_4 + 2\bar{x}_5 + 4\bar{x}_8 \end{bmatrix} \right) : x_i \in \mathbb{Z}_2[\zeta] \right\}.$$

(We only need to know that corresponding entries in the diagonals differ by a multiple of 2, which is easily checked.) Thus for some x_1, x_2, we have

$$\det(M_1)\det(M_3) \equiv \det\left(\begin{bmatrix} 1+2x_1 & 2x_2 \\ 2\bar{x}_2 & 1+2\bar{x}_1 \end{bmatrix}\right)^2 \equiv 1 \mod (4),$$

and it follows that $\mathrm{N}_1(\bar{\psi}) = \det(T_1)\det(T_3) = 1$, as we wished to show.

This observation has the following consequence. Let $U \leq \Lambda^\times$ consist of those units u such that there is a central automorphism β_u of Ω which induces on Λ_2 the inner automorphism given by conjugation with the image of u. Then, the assignment $u \mapsto \mathrm{N}_1(\bar{\beta}_u)$ yields a well defined homomorphism $d : U \to \{\pm 1\}$. Does this homomorphism arise from the determinantal map?

The following obvious approach to this question seemingly doesn't lead to something concrete. Recall that $R_2G/(\hat{Q}) \cong \mathrm{Mat}_2(R_2H)$, where $H = \langle a^2, b, c\rangle$. Explicitly,

$$a \leftrightarrow \begin{bmatrix} 0 & a^2 \\ 1 & 0 \end{bmatrix}, \quad b \leftrightarrow \begin{bmatrix} b & 0 \\ 0 & bc \end{bmatrix}, \quad c \leftrightarrow \begin{bmatrix} c & 0 \\ 0 & b^2c \end{bmatrix}, \quad q \leftrightarrow \begin{bmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{bmatrix}.$$

Then, with the following representation of $\left(\frac{1-b^2}{2}\right)\left(\frac{1-c}{2}\right)R_2H$:

$$\rho(a^2) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \rho(b) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \rho(c) = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},$$

we recover the representation θ, that is, ρ induces a homomorphism from $\mathrm{Mat}_2(R_2H)$ to the projection $(R_2\Lambda)_{\mathrm{pr}}$ of $R_2\Lambda$ to a block of $\mathbb{Q}_2(\zeta)\Lambda$. Now one would like to apply the K_1-functor to

$$\begin{array}{ccc} R_2H & \longrightarrow & R_2\bar{H} \\ \downarrow & & \\ \left(\frac{1-b^2}{2}\right)\left(\frac{1-c}{2}\right)R_2H & & \end{array}$$

to get information about how norms of units in Λ and Ω are related. But, for example, the unit $\left[\begin{smallmatrix} a^2-b+c & 0 \\ 0 & 1 \end{smallmatrix}\right]$ in $\mathrm{Mat}_2(R_2H)$ maps to a matrix of determinant 1 in $(R_2\Lambda)_{\mathrm{pr}}$ (we have $\rho(a^2 - b + c) = \left[\begin{smallmatrix} -1 & 0 \\ 2 & -1 \end{smallmatrix}\right]$), whereas its image in $\mathrm{Mat}_2(R_2\bar{H}) \cong R_2\bar{G}/(\hat{Q})$ is $\left(\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \dots\right)$.

What we will show is that if $s \in \Lambda^\times$, and there is $\alpha \in \mathrm{Autcent}(\mathbb{Z}\bar{P}Q)$ which induces on Λ_2 the inner automorphism given by conjugation with the image of s, then $\det(s) = \pm 1$, and $\det(s) = 1$ if and only if $d(s) = 1$.

First, note that $\bar{P}Q$ has $S := \langle a, q\rangle$ ($\cong C_3 \rtimes C_4$) as homomorphic image. The nonlinear irreducible complex representations of S can be read off from the seventh and eighth component of $\mathbb{C}\Omega$; let us denote them by φ_7 and φ_8. The unit groups $(\varphi_i(\mathbb{Z}S))^\times$ are

known. The block $\varphi_8(\mathbb{Q}S)$ of the rational group algebra $\mathbb{Q}S$ belongs to the faithful representation and is a totally definite quaternion algebra, and $(\varphi_8(\mathbb{Z}S))^\times = \varphi_8(S)$ (see Proposition 29.2). Hence α agrees on $\varphi_8(\mathbb{Z}S)$ with a group automorphism of S. There is no central automorphism of $\mathbb{Z}S$ which agrees on $\varphi_8(\mathbb{Z}S)$ with a non-inner group automorphism of S (cf. [60, Example 2.1]). Any automorphism of $\mathbb{Z}S$ induces an inner automorphism of $\mathbb{Z}S/\langle a^2\rangle$, the integral group ring of the symmetric group S_3 of order 6 (see [64]). According to a description of the normalized unit group $\mathrm{V}(\mathbb{Z}S_3)$ due to Jespers and Parmenter (see [73]), S_3 has a normal complement in $\mathrm{V}(\mathbb{Z}S_3)$ generated by three bicyclic units.[2]

The following elements are 'modifications' of these units:

$$\begin{aligned} b_1 &= 1 + (1-a)q(1+a) - (1-a^2)qa, \\ b_2 &= 1 + (1-aq)q(1+aq) - (1-a^2)a, \\ b_3 &= 1 + (1-aq^2)q(1+aq^2) + (1-a^2)a. \end{aligned}$$

Thus $(\varphi_7(\mathbb{Z}S))^\times = \langle \varphi_7(b_1), \varphi_7(b_2), \varphi_7(b_3)\rangle \rtimes \varphi_7(S)$. Moreover, the images of b_1, b_2 and b_3 in Ω and Λ are units, having determinant 1 in each irreducible representation belonging to these components: Set $\omega = \zeta - \zeta^2 = i\sqrt{3}$. Then

$$S_1 = \begin{bmatrix} -2\zeta^2 & \omega \\ -\omega & -2\zeta \end{bmatrix}, \quad S_2 = \begin{bmatrix} -2\zeta^2 & \omega\zeta^2 \\ -\omega\zeta & -2\zeta \end{bmatrix}, \quad S_3 = \begin{bmatrix} -2\zeta & -\omega\zeta \\ \omega\zeta^2 & -2\zeta^2 \end{bmatrix},$$

$$T_1 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \qquad T_2 = \begin{bmatrix} 0 & \zeta^2 \\ -\zeta & 0 \end{bmatrix}, \qquad T_3 = \begin{bmatrix} 0 & \zeta \\ -\zeta^2 & 0 \end{bmatrix}$$

are matrices of determinant 1, and the elements b_1, b_2 and b_3 map to

$$\begin{aligned} &\left(S_1, S_1^{-1}, T_1, T_1, S_1, T_1, S_1, T_1\right), \\ &\left(S_2, S_3, T_2, T_3, S_2, T_2, S_2, T_2\right), \\ &\left(S_3^{-1}, S_2^{-1}, -T_3, -T_2, S_3^{-1}, -T_3, S_3^{-1}, -T_3\right) \end{aligned}$$

in Ω, respectively. From this it follows that their images in Λ have determinant 1, for $\theta|_S$ is equivalent to $\varphi_7|_S \oplus \varphi_8|_S$: A representation equivalent to θ is given by

$$a \mapsto \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}, \quad b \mapsto \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix},$$

$$c \mapsto \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad q \mapsto \begin{bmatrix} \zeta & 0 & 0 & 0 \\ 0 & \zeta^2 & 0 & 0 \\ 0 & 0 & \zeta & 0 \\ 0 & 0 & 0 & \zeta^2 \end{bmatrix}.$$

[2] The complement is torsion-free. However, see Section 13 for bicyclic units in $\mathbb{Z}S_4$.

Since $d(g) = \det(\varphi_+(g)) \cdot \det(\varphi_-(g)) = \det(\theta(g)) = \pm 1$ for all $g \in G$, this allows us to modify u and α such that α induces the identity on $\varphi_7(\mathbb{Z}S)$. Let $\tilde{\alpha}$ be the automorphism of $\mathbb{Z}S$ induced by α; we show that $\tilde{\alpha}$ is the identity. Let B be the block of $\mathbb{Q}S$ corresponding to the faithful irreducible representation, and denote the complementary component by C. Then $\tilde{\alpha}$ induces the identity on C, and agrees with an inner group automorphism on B. Thus if $g \in S$, then $g^{-1}(g\tilde{\alpha})$ is a unit of finite order. Therefore, $g^{-1}(g\tilde{\alpha})$ is rationally conjugate to a group element h. Then h maps to the unity in C, so $h = 1$, and we are done.

For $1 \leq i \leq j \leq 8$, let $\Omega_{i\text{-}j}$ denote the projection of Ω to the sum of the blocks $i, \ldots, j$ of $\mathbb{C}\Omega$. We have just shown that α induces the identity on $\Omega_{7\text{-}8}$. Associated with the idempotents $\frac{1+c}{2}$ and $\frac{1+b}{2}$ there are pullback diagrams

$$\begin{array}{ccc} \mathbb{Z}_2\Omega & \longrightarrow & \mathbb{Z}_2\Omega_{1\text{-}4} \\ \downarrow & & \downarrow \\ \mathbb{Z}_2\Omega_{5\text{-}8} & \longrightarrow & \mathbb{Z}_2\Omega_{1\text{-}4}/2\mathbb{Z}_2\Omega_{1\text{-}4} \end{array} \quad \text{and} \quad \begin{array}{ccc} \mathbb{Z}_2\Omega_{5\text{-}8} & \longrightarrow & \mathbb{Z}_2\Omega_{5\text{-}6} \\ \downarrow & & \downarrow \\ \mathbb{Z}_2\Omega_{7\text{-}8} & \longrightarrow & \mathbb{Z}_2\Omega_{5\text{-}6}/2\mathbb{Z}_2\Omega_{5\text{-}6} \end{array} .$$

Recall that α induces an inner automorphism of $\mathbb{Z}_2\Omega$, and therewith of the above pullbacks as well. We will show that there are units $v = (V_1, \ldots, V_8)$ and $w = (W_1, \ldots, W_8)$ of $\mathbb{Z}_2\Omega$ such that α is conjugation with vw, and $\det(V_1) \cdot \det(V_3) \equiv \det(W_1) \cdot \det(W_3) \equiv 1 \mod 4\mathbb{Z}_2[\zeta]$. We already know that there is $s \in \mathbb{Z}_2[\zeta]^\times$ such that $\mathrm{N}_1(\bar{\alpha}) = s^2 \det(V_1) \cdot \det(V_3) \cdot \det(W_1) \cdot \det(W_3) \equiv s^2 \mod 4\mathbb{Z}_2[\zeta]$, and it follows that $\mathrm{N}_1(\bar{\alpha}) = 1$.

Let $M = \mathbb{Z}_2\Omega_{5\text{-}6}$, considered as a $\mathbb{Z}_2$-representation of $S = \langle a, q \rangle$, the action given by $m \cdot g = g^{-1}m(g\alpha)$ for all $g \in S$ and $m \in M$. A 1-coboundary $\delta \in \mathrm{B}^1(S, M)$ is given by $\delta(g) = 1 \cdot (1 - g) = 1 - g^{-1}(g\alpha)$ for all $g \in S$. Since α induces the identity on $M/2M$, there is $\delta' \in \mathrm{Z}^1(S, M)$ with $\delta = 2 \cdot \delta'$.

Note that M is isomorphic to $\mathbb{Z}_2\Omega_{5\text{-}6}$, considered as S-module via usual conjugation, since α induces an inner automorphism of $\mathbb{Z}_2\Omega_{5\text{-}6}$, and that the image of $\{a^i q^j \mid 0 \leq i \leq 3, 1 \leq i \leq 2\}$ in $\mathbb{Z}_2\Omega_{5\text{-}6}$ is a $\mathbb{Z}_2$-basis of M which is permuted by the conjugation action of $\langle a \rangle$. Thus M is a direct summand of a permutation lattice for S over $\mathbb{Z}_2$. By Shapiro's lemma, $\mathrm{H}^1(S, M) = 0$, so δ' is a coboundary, and there is $m \in M$ with $1 - g^{-1}(g\alpha) = 2(m - g^{-1}m(g\alpha))$ for all $g \in S$. This means $g(1 - 2m) = (1 - 2m)(g\alpha)$ for all $g \in S$, and $1 - 2m$ is a unit in M, so α induces on M the inner automorphism given by conjugation with $1 - 2m$. There is $x \in \mathbb{Z}_2S$ which maps to $-m$ in M. Then α on $\Omega_{5\text{-}8}$ is given by conjugation with the image $v = (V_1, \ldots, V_8)$ of $\frac{1+b}{2} + \frac{1-b}{2}(1 + 2x) = 1 + (1 - b)x$ in $\mathbb{Z}_2\Omega$. The element v is of the form

$$\left(\begin{bmatrix} 1 + 2x_1 & 2\bar{x}_2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 + 2\bar{x}_1 & 2x_2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 + 2x_1 + 4x_3 & 2\bar{x}_2 + 4\bar{x}_4 \\ 0 & 1 \end{bmatrix}, \right.$$
$$\left. \begin{bmatrix} 1 + 2\bar{x}_1 + 4\bar{x}_3 & 2x_2 + 4x_4 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 + 2x_1 & 2\bar{x}_2 \\ 2x_2 & 1 + 2\bar{x}_1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \right.$$

$$\left.\begin{bmatrix} 1+2x_1+4x_3 & 2\bar{x}_2+4\bar{x}_4 \\ -2x_2-4x_4 & 1+2\bar{x}_1+4\bar{x}_3 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right)$$

for some $x_i \in \mathbb{Z}_2[\zeta]$. Apparently, v is a unit in $\mathbb{Z}_2\Omega$, with $\det(V_1)\cdot\det(V_3) \equiv 1 \mod 4\mathbb{Z}_2[\zeta]$.

Let $\mathrm{conj}(v)$ be conjugation with v, and consider the automorphism $\beta := \mathrm{conj}(v)^{-1}\alpha$ of $\mathbb{Z}_2\Omega$. Since β induces the identity on $\mathbb{Z}_2\Omega_{5\text{-}8}$, this automorphism induces an inner automorphism of $M := \mathbb{Z}_2\Omega_{1\text{-}4}$, and the identity on $M/2M$. Note that M is only a monomial lattice for the permutation action of $\langle a, b\rangle$, so the previous argument cannot be applied. But it is easy to see that the group of central units in M maps onto the group of central units in $M/2M$, so there is $m \in M$ such that β on M is given by conjugation with $1+2m$. If $y \in \mathbb{Z}_2G$ maps to m in M, then the image $w = (W_1, \ldots, W_8)$ of $\frac{1+c}{2} + \frac{1-c}{2}(1+2y) = 1 + (1-c)y$ in $\mathbb{Z}_2\Omega$ is clearly a unit, and $\det(W_1)\cdot\det(W_3) \equiv 1 \mod 4\mathbb{Z}_2[\zeta]$ (by the same argument which proved that the map d is well defined).

Since $\alpha = \mathrm{conj}(vw)$, it follows that $\mathrm{N}_1(\bar{\alpha}) = 1$, as claimed. Thus it remains to show that $\det(u) = 1$.

We have a look at the image v' of $1+(1-b)x$ and the image w' of $1+(1-c)y$ in $\mathbb{Z}_2\Lambda$. We have

$$v' = \begin{bmatrix} 1+x_1 & -x_1 & \bar{x}_2 & -\bar{x}_2 \\ x_1 & 1+x_1 & \bar{x}_2 & \bar{x}_2 \\ x_2 & x_2 & 1+\bar{x}_1 & \bar{x}_1 \\ x_2 & -x_2 & -\bar{x}_1 & 1+\bar{x}_1 \end{bmatrix}$$

for some $x_i \in \mathbb{Z}_2[\zeta]$. Writing $x_1 = s + t\zeta$ with $s, t \in \mathbb{Z}_2$, we get $\det(v') = 1 + 2(t+t^2)$. Therefore $\det(v') \equiv 1 \mod 4\mathbb{Z}_2[\zeta]$, and v' is a unit in $\mathbb{Z}_2\Lambda$.

The first two diagonal entries of an element of $\mathbb{Z}_2\Lambda$ are congruent modulo 2. It easily follows that $\det(w') \equiv 1 \mod 4\mathbb{Z}_2[\zeta]$, and w' is a unit in $\mathbb{Z}_2\Lambda$.

Note that $u = v'w'z$ for some unit z in $\mathbb{Z}_2\Lambda$ which maps to a central unit in Λ_2.

Let $g_1 = 1$, $g_2 = a^2$, $g_3 = c$, $g_4 = a^2c$, $g_5 = b$, $g_6 = bq$, $g_7 = bq^2$, $g_8 = acq$, $g_9 = ab$, $g_{10} = abq$, $g_{11} = abq^2$, $g_{12} = abc$. Then each central element of Λ_2 can be lifted to an element of the form

$$s = \sum_{i=1}^{4} c_i g_i + \sum_{i=5}^{12} c_i (g_i + a^{-1} g_i a) \quad (c_i \in \mathbb{Z}).$$

Note that the image of s in $\mathbb{Z}_2\Lambda$ is a unit if its image in Λ_2 is a unit. Thus z can be written as the product of some $\theta(s)$ and a unit of $\mathbb{Z}_2\Lambda$ mapping to the identity in Λ_2.

We have $\theta(s) = \left[\begin{smallmatrix} B_1 & 0 \\ 0 & B_2 \end{smallmatrix}\right]$, where (recall that $\omega = \zeta - \zeta^2$)

$$B_1 = \begin{bmatrix} c_1 - c_3 - c_{10}\omega + c_{11}\omega + 2c_{12} & c_2 - c_4 + c_6\omega - c_7\omega - c_8\omega \\ c_2 - c_4 - c_6\omega + c_7\omega - c_8\omega & c_1 - c_3 + c_{10}\omega - c_{11}\omega - 2c_{12} \end{bmatrix},$$

$$B_2 = \begin{bmatrix} c_1 + c_3 + 2c_9 - c_{10} - c_{11} & c_2 + c_4 - 2c_5 + c_6 + c_7 - c_8\omega \\ c_2 + c_4 + 2c_5 - c_6 - c_7 - c_8\omega & c_1 + c_3 - 2c_9 + c_{10} + c_{11} \end{bmatrix}$$

satisfy $\det(B_1) \equiv \det(B_2) \mod 4\mathbb{Z}[\zeta]$.

We have

$$\mathbb{Z}_2\Lambda = \left\{ \begin{bmatrix} a_1 & a_3 + 2a_9 & \bar{a}_7 + 2a_8 & \bar{a}_5 + 2a_6 - 2\bar{a}_{15} - 4a_{16} \\ -a_3 & a_1 + 2a_{11} & \bar{a}_5 + 2a_6 & -\bar{a}_7 - 2a_8 + 2\bar{a}_{13} + 4a_{14} \\ a_5 & a_7 + 2a_{13} & \bar{a}_1 + 2a_2 & -\bar{a}_3 - 2a_4 + 2\bar{a}_9 + 4a_{10} \\ -a_7 & a_5 + 2a_{15} & \bar{a}_3 + 2a_4 & \bar{a}_1 + 2a_2 - 2\bar{a}_{11} - 4a_{12} \end{bmatrix} : a_i \in \mathbb{Z}_2[\zeta] \right\}$$

(only the congruences in the diagonal are of interest for us). Thus $\det(1 + 2m) \equiv 1 \mod 4\mathbb{Z}_2[\zeta]$ for all $m \in \mathbb{Z}_2\Lambda$. Note that the kernel of the map $\mathbb{Z}_2\Lambda \to \Lambda_2$ consists precisely of the elements of the form $1 + 2m$ ($m \in \mathbb{Z}_2\Lambda$).

Thus we have shown that $\det(u) \equiv \det(B_1)^2 \mod 4\mathbb{Z}_2[\zeta]$. Since $u \in \Lambda^\times$, we obtain $\det(u) = 1$, as desired.

12.4. Final contradiction

First, we show that the inner automorphism of Λ_2 induced by τ lifts to a central automorphism α of $\mathbb{Z}\bar{P}Q$. We have a pullback diagram

$$\begin{array}{ccc} \mathbb{Z}\bar{P}Q & \longrightarrow & \mathbb{Z}\bar{P} \\ \downarrow & & \downarrow \\ \mathbb{Z}\bar{P}Q/(\hat{Q}) & \longrightarrow & \mathbb{F}_3\bar{P} \end{array}.$$

Let

$$v = 2(1 - a^2) + 4(a + a^{-1}) - 3(q - a^2q^{-1} + 2).$$

Then the image of v in $\Omega = \mathbb{Z}\bar{P}Q/(\hat{Q})$ is

$$\left(\left[\begin{smallmatrix} \kappa & 8 \\ 8 & \bar{\kappa} \end{smallmatrix}\right], \left[\begin{smallmatrix} \bar{\kappa} & 8 \\ 8 & \kappa \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} \kappa & 8 \\ 8 & \bar{\kappa} \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} \kappa & 8 \\ 8 & \bar{\kappa} \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]\right), \quad \text{where } \kappa = -6 - 3(\zeta - \zeta^2).$$

Since $\kappa\bar{\kappa} - 8^2 = 63 - 64 = -1$, it follows that the image of v in Ω is a unit. Let α_1 denote the inner automorphism of Ω given by conjugation with the image of v. We have $v \equiv q + a^2q^{-1} = w \mod 2$, so α_1 and τ induce the same automorphism of Λ_2. Note that the projections of v and a to any block of $\mathbb{C}\Omega$ are matrices of the same determinant. It follows from [60, Lemma 2.2] that there is an inner automorphism α_2 of $\mathbb{Z}\bar{P}$ which agrees with α_1 on $\mathbb{F}_3\bar{P}$ (for example, conjugation with the image of $a + ((1 - j(1 + b)a)(1 - j(1 - b)a)(1 - j(1 + b)a))$, where $j = (1 - c)(1 - a^2)$), thus giving rise to a central automorphism of α of $\mathbb{Z}\bar{P}Q$ which agrees with τ on Λ_2.

We are in a position to finish the proof of Theorem 10.1. Recall that there are $\gamma \in \mathrm{Autcent}(\Gamma)$ and $\lambda \in \mathrm{Autcent}(\Lambda)$, inducing automorphisms of $\bar{\Lambda}$ and differing on this quotient by the inner automorphism induced by τ. Besides, the automorphisms γ and λ induce automorphisms of Λ_2, and inner automorphisms of Λ_3 given by conjugation with matrices of determinant 1. The automorphism γ induces central automorphisms on the various pieces of the 'large' diagram the pullback Γ fits in (see Subsection 12.1), which shall be denoted by γ too, for short.

According to our assumptions, we can assume that λ and $\gamma\alpha \in \mathrm{Autcent}(\mathbb{Z}\bar{P}Q)$ induce the same automorphism of $\bar{\Lambda}$. Applying the results from Subsection 12.3, we get that λ is an inner automorphism, say conjugation with $u \in \Lambda^\times$. Then $\det(u) \neq -1$ since λ induce an inner automorphism of Λ_3 given by conjugation with a matrix of determinant 1. Therefore $\det(u) = 1$, and consequently $\mathrm{N}_1(\gamma\bar{\alpha}_1) = 1$. Since $\mathrm{N}_1(\bar{\alpha}_1) = -1$, it follows that $\mathrm{N}_1(\gamma) = -1$. But γ induces an inner automorphism of Λ_3 given by conjugation with a matrix of determinant 1, so γ, considered as a central automorphism of $\mathbb{Z}P$, satisfies $\mathrm{N}(\gamma) = -1$, in contradiction to the result from Subsection 12.2.

Theorem 10.1 is proved.

12.5. Final remarks

Let α be an augmentation-preserving automorphism of SG, where $S = \mathbb{Z}_{\pi(G)}$, which has no Zassenhaus factorization. Then there is an invertible bimodule M for $\mathbb{Z}G$ such that $S \otimes_{\mathbb{Z}} M \cong {}_1(SG)_\alpha$ as invertible bimodules (see Proposition 1.4). We now know that there is no invertible bimodule for $\mathbb{Z}G$ in the same genus as M which is free from one side. However, it might be possible to prove this more directly, by examination of the bimodule M. This might also help to answer the question whether M as left $\mathbb{Z}G$-module may be stably free or not.

We have essentially two different descriptions of the bimodule M.

The idele-theoretic description

Firstly, there is the idele-theoretic description from Proposition 1.4. Then, M is a locally free left $\mathbb{Z}G$-ideal in $\mathbb{Q}G$,

$$M = (\mathbb{Z}G)\nu = \bigcap_p \mathbb{Z}_{(p)}G \cdot \nu_p$$

for some idele $\nu = (\nu_p)$ with $\nu_p \in (\mathbb{Q}G)^\times$. Note that we can give such a ν explicitly.

We may view ν as an element of the idele group

$$J(\mathbb{Q}G) = \left\{ (\mu_p) \in \prod_p (\mathbb{Q}_pG)^\times \;\middle|\; \mu_p \in (\mathbb{Z}_pG)^\times \text{ a.e.} \right\}$$

(for this and the following remarks, see [27, § 49]). There are three relevant subgroups

of $J(\mathbb{Q}G)$:

$$\begin{aligned} U(\mathbb{Z}G) &= \text{group of unit ideles} = \textstyle\prod_p (\mathbb{Z}_pG)^\times, \\ u(\mathbb{Q}G) &= \text{group of principal ideles} = \text{image of } (\mathbb{Q}G)^\times \text{ in } J(\mathbb{Q}G), \\ J_0(\mathbb{Q}G) &= \text{kernel of the reduced norm nr acting on } J(\mathbb{Q}G) \\ &= \{\mu \in J(\mathbb{Q}G) \mid \mathrm{nr}(\mu) = 1\}. \end{aligned}$$

($J_0(\mathbb{Q}G)$ is a closed normal subgroup, in the idele topology, and $[J(\mathbb{Q}G), J(\mathbb{Q}G)] \subseteq J_0(\mathbb{Q}G)$.)

Let $\mathrm{Cl}(\mathbb{Z}G)$ be the locally free class group of $\mathbb{Z}G$, consisting of stable isomorphism classes of locally free left $\mathbb{Z}G$-ideals in $\mathbb{Q}G$. Then there is a natural isomorphism

$$\mathrm{Cl}(\mathbb{Z}G) \cong \frac{J(\mathbb{Q}G)}{J_0(\mathbb{Q}G)U(\mathbb{Z}G)u(\mathbb{Q}G)}.$$

Of course, we also have $\mathrm{Cl}(\mathrm{Z}(\mathbb{Z}G)) = J(\mathrm{Z}(\mathbb{Q}G))/U(\mathrm{Z}(\mathbb{Z}G))u(\mathrm{Z}(\mathbb{Q}G))$. As noted before, the isomorphism class of the bimodule M is not uniquely determined: By [28, 31.18]), there are exactly $|\mathrm{Cl}(\mathrm{Z}(\mathbb{Z}G))|$ isomorphism classes of bimodules in the genus of M, and the bimodule corresponding to an idele $\gamma = (\gamma_p) \in J(\mathrm{Z}(\mathbb{Q}G))$ is given by

$$(\mathbb{Z}G)\nu\gamma = \mathbb{Q}G \cap \bigcap_p \mathbb{Z}_pG \cdot \nu_p\gamma_p.$$

Recall from Subsection 12.2 that we have shown $\mathrm{Cl}(\varepsilon\Delta) \neq 0$, for a homomorphic image $\varepsilon\Delta$ of $\Delta = \mathrm{Z}(\mathbb{Z}P)$. Since the surjections $\mathrm{Z}(\mathbb{Z}G) \twoheadrightarrow \Delta \twoheadrightarrow \varepsilon\Delta$ induce surjections between the corresponding class groups, it follows that $\mathrm{Cl}(\mathrm{Z}(\mathbb{Z}G)) \neq 0$. (We have also shown that $\mathrm{Cl}(\mathrm{Z}(\mathbb{Z}G))$ contains elements of order 4.)

Since the bimodule M is not free from one side, we have

$$\nu \notin U(\mathbb{Z}G)u(\mathbb{Q}G).$$

It is easy to see that we can choose ν such that $\nu^2 \in J_0(\mathbb{Q}G)$. Then $M \oplus M$ is, as left module, stably isomorphic to $\mathbb{Z}G$, and from the Bass Cancellation Theorem [27, 41.20] it follows that $M \oplus M \cong \mathbb{Z}G \oplus \mathbb{Z}G$ as left modules. However, this does not hold for all bimodules in the genus of M since $\mathrm{Cl}(\mathrm{Z}(\mathbb{Z}G))$ contains elements of order 4. This proves Proposition 10.2.

The module M is stably free as left $\mathbb{Z}G$-module if and only if $[M] = [\mathbb{Z}G] = 0$ in $\mathrm{Cl}(\mathbb{Z}G)$, that is, if $\nu \in J_0(\mathbb{Q}G)U(\mathbb{Z}G)u(\mathbb{Q}G)$. If we could show that in this case, already $\nu \in U(\mathbb{Z}G)u(\mathbb{Q}G)$, we would have a contradiction and proved that M is *not* stably free. This seems reasonable since ν can be chosen such that $e\nu_p = e$ for all primes p, where e denotes the rational idempotent belonging to the sum of the two blocks of $\mathbb{Q}G$ which are totally definite quaternion algebras.

Milnor's description

A theorem of Milnor (see [27, 42.11]) shows how the projective $\mathbb{Z}G$-modules are built from the projective modules of the pieces Λ and Γ of the pullback diagram

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \Gamma \\ \downarrow & & \downarrow \\ \Lambda & \longrightarrow & \bar{\Lambda} \end{array}.$$

We shall give such a description for M, which is a projective left $\mathbb{Z}G$-module, in a moment.

Given the above pullback diagram, we have Milnor's "Mayer-Vietoris" sequence, which is an exact sequence of groups (see [27, 49.27]):

$$K_1(\Gamma) \times K_1(\Lambda) \longrightarrow K_1(\bar{\Lambda}) \xrightarrow{\partial'} \mathrm{Cl}(\mathbb{Z}G) \longrightarrow \mathrm{Cl}(\Gamma) \oplus \mathrm{Cl}(\Lambda) \longrightarrow 0. \qquad (*)$$

Here, $\bar{\Lambda}$ is a finite ring, so each element of the Whitehead group $K_1(\bar{\Lambda})$ may be represented by a unit of $\bar{\Lambda}$, and the connecting homomorphism ∂' can be described quite simply: for $u \in \bar{\Lambda}^\times$, the left $\mathbb{Z}G$-module

$$M(u) = \{(\gamma, \lambda) \in \Gamma \oplus \Lambda \mid \bar{\gamma}u = \bar{\lambda} \text{ in } \bar{\Lambda}\}$$

is in the same genus as $\mathbb{Z}G$, and $\partial'(u) = [M(u)] \in \mathrm{Cl}(\mathbb{Z}G)$.

As we have seen at the beginning of this section, the image u of the group ring element $2((1+a^2)+(1-a^2)c)a^{-1} + 3(q + a^2q^{-1})$ in $\bar{\Lambda}$ is a unit, and the group automorphism τ of G induces an inner automorphism of $\bar{\Lambda}$, given by conjugation with u. We claim that we can choose

$$M = M(u).$$

Indeed, M is also a right $\mathbb{Z}G$-module, the action given by

$$(\gamma, \lambda) \cdot g = (\gamma(g\tau), \lambda g) \quad \text{for all } (\gamma, \lambda) \in M,\ g \in G.$$

Tensoring with $\mathbb{Q}$ gives $\mathbb{Q}M = {}_1(\mathbb{Q}\Gamma)_\tau \oplus {}_1(\mathbb{Q}\Lambda)_1$, so M yields the 'expected' semilocal isomorphism.

Now M is not free from one side if and only if $u \neq \bar{\gamma}\bar{\lambda}$ in $\bar{\Lambda}$ for all $\gamma \in \Gamma^\times$, $\lambda \in \Lambda^\times$ (see [27, 42.11]). We have shown even more, but note that when one has shown that M is not free, there is no reason why this should also be the case for all the other bimodules in the genus of M.

We remark that, since $[M]$ lies in the kernel of the map $\mathrm{Cl}(\mathbb{Z}G) \to \mathrm{Cl}(\Gamma) \oplus \mathrm{Cl}(\Lambda)$, we have an isomorphism of left $\mathbb{Z}G$-modules

$$M \oplus (\Gamma \oplus \Lambda)^{(k)} \cong \mathbb{Z}G \oplus (\Gamma \oplus \Lambda)^{(k)} \quad \text{for some } k \in \mathbb{N}$$

(cf. the proof of [27, 49.34]).

Furthermore, since $u^2 = 1$ in $\bar{\Lambda}$, we obtain, as before, that $M \oplus M \cong \mathbb{Z}G \oplus \mathbb{Z}G$.

Finally, the module M is stably free as left $\mathbb{Z}G$-module if and only if $[M] = [\mathbb{Z}G] = 0$ in $\mathrm{Cl}(\mathbb{Z}G)$, that is, if u is contained in the image of the map $K_1(\Gamma) \times K_1(\Lambda) \to K_1(\bar{\Lambda})$. Since Γ and Λ have stable range 2 (see [27, 41.23]) this is equivalent to say that there are matrices $X \in \mathrm{GL}_2(\Gamma)$ and $Y \in \mathrm{GL}_2(\Lambda)$ such that $\left[\begin{smallmatrix} u & 0 \\ 0 & 1 \end{smallmatrix}\right] = \bar{X}\bar{Y}$ in $\mathrm{GL}_2(\bar{\Lambda})$.

13. Bicyclic units and torsion

The bicyclic units in an integral group ring $\mathbb{Z}G$, where G is a finite group, have proved to be useful for the explicit construction of subgroups of finite index in the normalized unit group $\mathrm{V}(\mathbb{Z}G)$ of $\mathbb{Z}G$. To describe them, let $x, y \in G$ and write $\hat{x} = 1 + x + \ldots + x^{n-1}$, where n denotes the order of x. Then $\mathbf{b}(x, y) := 1 + (1 - x)y\hat{x}$ defines a typical bicyclic unit of $\mathbb{Z}G$.

Let S_n be the symmetric group on n letters. Ritter and Sehgal proved that the Bass cyclic and the bicyclic units generate a subgroup of finite index in $\mathrm{V}(\mathbb{Z}S_n)$ (see [129, (27.8)]). Set

$$\mathcal{B}_n = \langle \mathbf{b}(x, y) \mid x, y \in S_n \rangle.$$

Jespers and Parmenter [73] showed that $\mathcal{B}_3$ is a torsion-free normal complement of rank 3 to S_3 in $\mathrm{V}(\mathbb{Z}S_3)$. Using a theoretic description of the units in $\mathbb{Z}S_4$ given by Allen and Hobby, Olivieri and del Río proved in [97] the following theorem.

13.1 Theorem. *The intersection $\mathcal{B}_n \cap S_n$ is the normal four-group of S_4 for $n = 4$, and the alternating group of S_n for $n \geq 5$.*

Thus the description of $\mathcal{B}_n \cap S_n$ for $n \in \mathbb{N}$ is complete. The theorem shows in particular that the group generated by the bicyclic units may have torsion; this answers Problem 19 from [129].

To prove the theorem, it suffices to show that $\mathcal{B}_4 \cap S_4$ is nontrivial. For assume that there is a nontrivial g contained in $\mathcal{B}_4 \cap S_4$, and let K be the normal four-group of S_4. Then g has to be contained in K since $\mathcal{B}_3$ is torsion-free (and S_4 maps to S_3 with kernel K, which gives rise to a map $\mathbb{Z}S_4 \to \mathbb{Z}S_3$ which maps bicyclic units to bicyclic units). This implies that $\mathcal{B}_4 \cap S_4 = K$, since it is easily seen that $\mathcal{B}_n \cap S_n$ is a normal subgroup of S_n. Let $n \geq 5$. Since S_4 is embedded in S_n, it follows that $\mathcal{B}_n \cap S_n$ is a nontrivial normal subgroup of S_n, i.e., $\mathcal{B}_n \cap S_n$ is either the alternating group of degree n or all of S_n. But the latter is impossible since any bicyclic unit maps to 1 under the sign representation of S_n. (The latter fact was missed in the submitted version of [97].)

Here, we show how to write a nontrivial element of S_4 explicitly as a product of bicyclic units.[3]

[3] We performed the calculations using MAPLE [144].

Let $S_4 = \langle a, b\rangle \rtimes \langle c, d\rangle$, where $\langle a, b\rangle$ is the normal four-group of S_4 and $\langle c, d\rangle \cong S_3$. Recall that we may identify $\mathbb{Q}S_4$ with $\mathbb{Q}\oplus\mathbb{Q}\oplus\mathrm{Mat}_2(\mathbb{Q})\oplus\mathrm{Mat}_3(\mathbb{Q})\oplus\mathrm{Mat}_3(\mathbb{Q})$ by setting

$$a := \left(\begin{bmatrix} 1 \end{bmatrix}, \begin{bmatrix} 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}\right)$$

$$b := \left(\begin{bmatrix} 1 \end{bmatrix}, \begin{bmatrix} 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}\right)$$

$$c := \left(\begin{bmatrix} 1 \end{bmatrix}, \begin{bmatrix} 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}\right)$$

$$d := \left(\begin{bmatrix} 1 \end{bmatrix}, \begin{bmatrix} -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{bmatrix}\right)$$

Maple tells us that $\mathbb{Z}S_4$ contains 156 (nontrivial) bicyclic units.[4] We can write $b \in S_4$ as a product of seven bicyclic units,

$$b = b_1b_2b_3b_4b_5b_6b_7,$$

where

$$b_1 := \mathbf{b}(b, c^2) = \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\right)$$

$$b_2 := \mathbf{b}(ab, bc) = \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{bmatrix}\right)$$

$$b_3 := \mathbf{b}(d, abc^2) = \left(\begin{bmatrix} -2 & -3 \\ 3 & 4 \end{bmatrix}, \begin{bmatrix} 0 & -2 & -1 \\ 0 & 1 & 0 \\ 1 & 2 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 & -1 \\ -2 & 1 & 2 \\ 1 & 0 & 0 \end{bmatrix}\right)$$

$$b_4 := \mathbf{b}(d, bc^2) = \left(\begin{bmatrix} -2 & -3 \\ 3 & 4 \end{bmatrix}, \begin{bmatrix} 2 & 2 & 1 \\ 0 & 1 & 0 \\ -1 & -2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ -2 & 1 & 2 \\ -1 & 0 & 2 \end{bmatrix}\right)$$

$$b_5 := \mathbf{b}(abd, c) = \left(\begin{bmatrix} 7 & 6 \\ -6 & -5 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 4 & 0 \\ 0 & 1 & 0 \\ 0 & 4 & 1 \end{bmatrix}\right)$$

[4] Thanks to Ángel del Río who informed me that a previous calculation of mine went wrong, cf. below.

$$b_6 := \mathbf{b}(bc^2d, c^2) = \left(\begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 2 & 2 & -1 \\ 2 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 2 \\ 0 & 0 & -1 \\ 0 & 1 & 2 \end{bmatrix} \right)$$

$$b_7 := \mathbf{b}(c^2d, abc) = \left(\begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ -2 & 0 & -1 \\ 2 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & -2 & 2 \\ 0 & 2 & -1 \\ 0 & 1 & 0 \end{bmatrix} \right)$$

(Here we omitted the projections on the first two components, which are all equal to 1). In fact, we observed that

$$b_6 b_7 = \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ -4 & -1 & -4 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 4 & 0 \\ 0 & -1 & 0 \\ 0 & 4 & -1 \end{bmatrix} \right)$$

is 'congruent modulo 4' to b, and then we tried to write bb_6b_7 as a product of bicyclic units.

13.2 Remark. On the 7th December, 2002 Ángel del Río informed the author that $\mathbb{Z}S_4$ contains 156 nontrivial bicyclic units. (Due to a bug in a Maple Worksheet, we originally obtained only 102 nontrivial bicyclic units.)

Motivated by the calculation above, Aurora Olivieri and Ángel del Río performed an exhaustive search, using Mathematica, in order to write the group element a as a product of as few as possible bicyclic units, and obtained

$$a = a_1 a_2 a_3 a_4,$$

where

$$a_1 := \mathbf{b}(cd, ca) = \left(\begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 & 2 \\ -1 & 0 & -2 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ -1 & 2 & 0 \\ -2 & 2 & 1 \end{bmatrix} \right)$$

$$a_2 := \mathbf{b}(c^2d, cab) = \left(\begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 2 & 2 & 1 \\ -2 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & -2 & 2 \\ 0 & 0 & 1 \\ 0 & -1 & 2 \end{bmatrix} \right)$$

$$a_3 := \mathbf{b}(bc^2d, c^2ab) = \left(\begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ -2 & 0 & 1 \\ -2 & -1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 2 \\ 0 & 2 & 1 \\ 0 & -1 & 0 \end{bmatrix} \right)$$

$$a_4 := \mathbf{b}(cd, c^2) = \left(\begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 2 \\ 1 & 2 & -2 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & -1 & 0 \\ 1 & 0 & 0 \\ -2 & 2 & 1 \end{bmatrix} \right)$$

IV. Some results on specific automorphism groups

> ... the source of all great mathematics is the special case, the concrete example. It is frequent in mathematics that every instance of a concept of seemingly great generality is in essence the same as a small and concrete special case.
>
> *Paul R. Halmos*
> *I Want to be a Mathematician, 1985*

This chapter contains a loose variety of results concerning specific automorphism groups which showed up in connection with the Zassenhaus conjecture and the isomorphism problem. We shall deal with class-preserving automorphisms and Coleman automorphisms of finite groups, and (twisted) projective limits of finite groups.

14. Class-preserving automorphisms

Recently, a new motivation to study class-preserving automorphisms of finite groups came from work of Roggenkamp and Kimmerle [80], which related them to the Zassenhaus conjecture (research in this direction began in [117]). Also, Mazur's observation [91, 92] linked the isomorphism problem for integral group rings with the existence of certain non-inner class-preserving automorphisms (see Section 2).

A short survey on class-preserving automorphisms is given in [54, Kapitel 3]; more recent results can be found in [56, 59, 137].

We would like to remark that nilpotent groups are the most natural candidates for groups with non-inner, class-preserving automorphisms. Examples might arise via linear algebra as follows (recently, Szechtman [137] investigated similar examples in detail).

14.1 Example. For any rational prime p, we construct a group G of order p^6 which possesses a non-inner, class-preserving automorphism σ.

Let

$$B = \begin{bmatrix} 1 & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix}, \; C = \begin{bmatrix} 1 & \cdot & \cdot & 1 \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \end{bmatrix} \in \mathrm{GL}(4, p).$$

Then B and C are two commuting matrices of order p. Take the underlying vector space

$$V = \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p \oplus \mathbb{F}_p$$

and form the semidirect product

$$G = V \rtimes (\langle b : b^2 \rangle \times \langle c : c^2 \rangle),$$

the operation given by $v^b = vB$ and $v^c = vC$ for all $v \in V$. Let

$$v = (0, 0, 0, 1) \in V \cap \mathrm{Z}(G)$$

and define the automorphism $\sigma \in \mathrm{Aut}(G)$ by $c\sigma = cz$, $b\sigma = b$ and $v\sigma = v$ for all $v \in V$. Then σ is a class-preserving automorphism if and only if for all $g = b^i c^k$, $i, k \in \mathbb{N}$, there is $v \in V$ with

$$g \cdot v(B^i C^k - E) = vgv^{-1} = g\sigma = gz^k \quad (E = \text{identity matrix}),$$

i.e., if and only if the matrix equation

$$(0, 0, 0, k) = v \begin{bmatrix} \cdot & \cdot & i & k \\ \cdot & \cdot & \cdot & i \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}$$

has a solution for every pair i, k. This is obvious, but there is no simultaneous solution for all i, k. Hence σ is a non-inner, class-preserving automorphism.

Here, we show that class-preserving automorphisms of abelian by cyclic groups are inner automorphisms. (For the class of metacyclic groups, this is obvious and was noticed by Kimmerle (see proof of [81, Folgerung 5.15]).)

The proof is based on the following lemma.

14.2 Lemma. *Let G be an abelian p-group, and let α and β be automorphisms of G of p-power order. Assume that $\alpha\beta = \beta\alpha$ and that for each $g \in G$, there is $n \in \mathbb{N}$ such that $g\beta = g\alpha^n$. Then β is a power of α.*

Proof. Assume that G is a counterexample, with the order of the semidirect product $G\langle\alpha\rangle$ being minimal. Let Z be a central subgroup of order p in $G\langle\alpha\rangle$ which is contained in G. Then β centralizes Z. Thus α and β induce automorphisms $\bar\alpha$ and $\bar\beta$ of $\bar G = G/Z$, and $\bar\beta$ is a power of $\bar\alpha$ by minimality of $G\langle\alpha\rangle$. Hence we can assume that $\bar\beta$ is the identity. Then $G \to Z$, $g \mapsto g^{-1}(g\beta)$ is a surjective homomorphism, with kernel K of index p. For all $g \in G$, there is $n(g) \in \mathbb{N}$ such that $g\beta = g\alpha^{n(g)}$. Choose $h \in G \setminus K$ such that $\alpha^{n(h)}$ is of maximal order among the $\alpha^{n(g)}$, $g \in G \setminus K$. By minimality of $G\langle\alpha\rangle$, we have $\langle\alpha\rangle = \langle\alpha^{n(h)}\rangle$. Thus we can assume that $G = \langle K, h\rangle$ and $h\beta = h\alpha$. Note that $h\beta = zh$ for an element z of order p in $Z \le \mathrm{Z}(G)$. For all $k \in K$, we have $kzh = (k\beta)(h\beta) = (kh)\beta = (kh)\alpha^{n(kh)} = k\alpha^{n(kh)}z^{n(kh)}h$, so $\alpha^{n(kh)}$ is not the identity, and $k\alpha^{n(kh)} \in kZ$. Thus if α^q is a power of α having order p, then α^q induces the identity on G/Z. As above, it follows that $H := \mathrm{C}_G(\alpha^q)$ is a normal α-invariant subgroup of G of index p. Also, H is fixed by β since β commutes with α. Thus by minimality of $G\langle\alpha\rangle$, the automorphism β agrees on H with some power α^l of α. If $h \notin H$, then $h \ne h\alpha^q = z^q h$, so $p \nmid q$ and α has order p. Consequently $H = \mathrm{C}_G(\alpha) \subseteq \mathrm{C}_G(\beta)$ and $\beta = \alpha$ (since $h \notin H$), contradicting our assumption that G is a counterexample. Thus $h \in H$ and $h\alpha = h\beta = h\alpha^l$, so that $\langle\alpha^l\rangle = \langle\alpha\rangle$ since $h\alpha \ne h$. Since β induces the identity on K, it follows that α induces the identity on $H \cap K$. Take any $k \in K \setminus H$; then $G = \langle h, k, H \cap K\rangle$ as $H \cap K$ is of index p^2 in G. Since α induces the identity on G/H, we have $k\alpha = xk$ for some $x \in H \cap K$, and $x \ne 1$ since $\alpha \ne \beta$. Let x^m be a power of x having order p. Assume that $\langle x^m\rangle \ne \langle z\rangle$. Since $x\alpha = x = x\beta$, the automorphisms α and β induce automorphisms of $G/\langle x^m\rangle$, and by minimality of $G\langle\alpha\rangle$, the automorphism induced by β equals the automorphism induced by some power α^j of α. Since $h\alpha^j(h\beta)^{-1} = z^{j-1}$, it follows that $j = 1 + ps$ for some $s \in \mathbb{Z}$. Furthermore $k\alpha^j(k\beta)^{-1} = x^j k k^{-1} = x^j$, and therefore $\langle x\rangle = \langle x^j\rangle \le \langle x^m\rangle$. It follows that $(hk)\alpha^i = z^i h x^i k = (zx)^i hk \ne zhk = (hk)\beta$ for all $i \in \mathbb{Z}$ (this is the place where we use that G is abelian!), and we have reached a final contradiction. □

14.3 Remark. The group G which is the direct product of a cyclic group C_2 of order 2 and the dihedral group D_8 of order 8 may serve as an example showing that the hypothesis that G is abelian cannot be removed. This observation also shows that there is a semidirect product $(\mathrm{C}_2 \times \mathrm{D}_8) \rtimes \mathrm{C}_4$ having a non-inner class-preserving automorphism of order 2.

We now have the following proposition.

14.4 Proposition. *Let G be a finite group having an abelian normal subgroup A with cyclic quotient G/A. Then class-preserving automorphisms of G are inner automorphisms.*

Proof. Let σ be a class-preserving automorphism of G of p-power order, for some prime p dividing the order of G; we have to show that σ is an inner automorphism. By [56,

Corollary 5] we can assume that G/A is a p-group. Let P be a Sylow p-subgroup of G, and choose $x \in P$ such that $G = \langle x, A\rangle$. By Sylow's theorem, we can assume that $P\sigma = P$. Set $S = P \cap A = \mathrm{O}_p(A)$ and $T = \mathrm{O}_{p'}(A)$, so that $P = \langle x, S\rangle$ and $A = S \times T$.

Let $\gamma \in \mathrm{Aut}(G)$ be the inner automorphism given by conjugation with x, and set $H = \langle \sigma|_T, \gamma|_T\rangle \leq \mathrm{Aut}(T)$. It is well known that $\mathrm{C}_H(t_0) = \mathrm{C}_H(T)$ for some $t_0 \in T$. Thus after modifying σ such that $t_0\sigma = t_0$, we have $t\sigma = t$ for all $t \in T$.

Let y be a generator of $\mathrm{C}_{\langle x\rangle}(t_0)$, and let δ be the inner automorphism given by conjugation with y. For each $s \in S$ there is $n(s) \in \mathbb{N}$ such that $s\sigma t_0 = (st_0)\sigma = (st_0)\gamma^{n(s)} = (s\gamma^{n(s)})(t_0\gamma^{n(s)})$, meaning that $s\sigma = s\delta^{m(s)}$ for some $m(s) \in \mathbb{N}$. Clearly $\sigma|_S$ commutes with δ. Thus the lemma tells us that $\sigma|_S$ is a power of δ, and we can modify σ such that the new σ fixes A element-wise. Clearly $x\sigma = x^s$ for some $s \in S$, and then σ is the inner automorphism given by conjugation with s. □

The proof actually shows:

14.5 Proposition. *Let G be a finite metabelian group having an abelian normal subgroup B such that the quotient $\bar{G} = G/B$ is abelian with cyclic Sylow p-group, for some prime p. Then each class-preserving automorphism of G of p-power order is an inner automorphism.* □

15. Coleman automorphisms

A *Coleman automorphism* of a finite group G is an automorphism of G whose restriction to any Sylow subgroup of G equals the restriction of some inner automorphism of G (this notion was introduced in [56, 61]). We write $\mathrm{Aut}_{\mathrm{Col}}(G)$ for the group of Coleman automorphisms of G, and put $\mathrm{Out}_{\mathrm{Col}}(G) = \mathrm{Aut}_{\mathrm{Col}}(G)/\mathrm{Inn}(G)$.

Coleman automorphisms occur naturally in the study of the normalizer of a finite group G in the units of its integral group ring $\mathbb{Z}G$ (see the Ward–Coleman Lemma on page 138). Kimmerle and the author [61] studied Coleman automorphisms in their own right. Here, we shall deal with some problems which were left open in [61].

Groups with non-cyclic chief factors

In [61], it was shown that the size of $\mathrm{Out}_{\mathrm{Col}}(G)$ can be limited if one imposes restrictions on the dimensions of the abelian composition factors of G. More precisely, it was shown (among other things):

- If G is quasinilpotent, then $\mathrm{Out}_{\mathrm{Col}}(G) = 1$;
- If G has no composition factor of order p, then $\mathrm{Out}_{\mathrm{Col}}(G)$ is a p'-group;
- If $\mathrm{Z}(\mathrm{F}^*(G))$ is a p'-group, and no chief factor of $G/\mathrm{F}^*(G)$ has order p, then $\mathrm{Out}_{\mathrm{Col}}(G)$ is a p'-group.

Here, we will be concerned about the following questions which remained unanswered in [61] — even though no definite results will be presented.

15.1 Problem. 1. Assume that no chief factor of G is of order p. Is it true that $\mathrm{Out}_{\mathrm{Col}}(G)$ is a p'-group?

2. Assume that $\mathrm{O}_{p'}(G) = 1$ for some prime p. Is it true that $\mathrm{Out}_{\mathrm{Col}}(G) = 1$?

3. Assume that G has a unique minimal normal subgroup. Is it true that $\mathrm{Out}_{\mathrm{Col}}(G) = 1$?

The present discussion has its origin in the following two results from [61]: For any finite group G, we have $\mathrm{Out}_{\mathrm{Col}}(\mathrm{F}^*(G)) = 1$ (see [61, Corollary 16]), and if N is a normal subgroup of G with $\mathrm{Out}_{\mathrm{Col}}(N)$ a p'-group and if p does not divide the order of G/N, then $\mathrm{Out}_{\mathrm{Col}}(G)$ is a p'-group, too (see [61, Corollary 3]).

In an attempt to generalize this result, we are led to consider the structure of a finite group G having the following properties:

- No chief factor of $G/\mathrm{F}^*(G)$ is isomorphic to C_p;
- The group G has a non-inner Coleman automorphism σ of p-power order.

Note that for $N \trianglelefteq G$, we have $\mathrm{F}^*(G)N/N \leq \mathrm{F}^*(G/N)$. Hence the first property pass on to factor groups. Thus, considering a 'minimal' example, we can assume that σ induces inner automorphisms on proper quotients of G.

Assume that $N := \mathrm{O}_{p'}(G) \neq 1$. Then σ induces an inner automorphism on G/N, and we can modify σ such that σ induces the identity on G/N (see [61, Remark 5]). Then σ induces a Coleman automorphism on N by [61, Lemma 19], and is therefore the identity on N by [61, Proposition 1]. But this implies that σ (which is of p-power order) is the identity, a contradiction.

Hence $\mathrm{O}_{p'}(G) = 1$. Since σ restricted to a Sylow p-subgroup coincides with an inner automorphism, it follows that G is not p-constrained (see [44, Corollary 4.2]).

Choosing $N = \mathrm{F}^*(G)$ in [61, Lemma 19], we see that σ induces a Coleman automorphism on $\mathrm{F}^*(G)$. Since $\mathrm{Out}_{\mathrm{Col}}(\mathrm{F}^*(G)) = 1$, we can modify σ such that σ induces the identity on $\mathrm{F}^*(G)$. Then σ induces the identity on the quotient G/M, where $M = \mathrm{O}_p(\mathrm{Z}(\mathrm{F}^*(G)))$ (so σ corresponds to a nontrivial element of $\mathrm{H}^1(G/M, M)$).

Choose a Sylow p-subgroup P of G with $P\sigma = P$ and $x \in P$ with $\sigma|_P = \mathrm{conj}(x)|_P$. Then x centralizes the Sylow p-subgroup $P \cap \mathrm{F}^*(G)$ of $\mathrm{F}^*(G)$. Note that $x \notin \mathrm{O}_p(G)$ by a well known 1-cohomology argument.

Since $\mathrm{F}^*(G)$ contains its own centralizer, it follows from a result of Gross [44, Theorem A(ii)] that $x \in \mathrm{F}^*(G)$ provided that $p > 2$.

It is known that there are groups H with $\mathrm{O}_{2'}(H) = 1$ having non-inner 2-central automorphisms, so the previous argument does not carry over to the $p = 2$ case. We remark that if $p = 2$ and $x \notin \mathrm{F}^*(G)$, then $\langle x^G \rangle / \mathrm{F}^*(G)$ has an abelian Sylow 2-subgroup

and a normal 2-complement by a result of Glauberman [40, Theorem 1], so $G/\mathrm{F}^*(G)$ has at least a composition factor of order 2. Though this case might be interesting, we didn't pursued it any further.

Now *assume* that $x \in \mathrm{F}^*(G)$. Write $x = yx_1 \cdots x_n$ with $y \in \mathrm{O}_p(G)$, and each x_i lying in a component L_i of G. Then $y \in \mathrm{Z}(\mathrm{F}^*(G))$, and we can assume without lost of generality that $y = 1$. Each x_i is p-central in L_i.

Note that there must be a component L_i, and $\phi \in \mathrm{Aut}(L_i)$, such that $x_i\phi = zx_i$ for some $1 \neq z \in \mathrm{Z}(L_i)$ (consider the action of P on the components of G and on the coset $(x_1 \cdots x_n)M$). In particular, ϕ is a non-inner automorphism. Further, note that there may be some $z' \in \mathrm{Z}(L_i)$ such that xz' is a fixed point of ϕ (at least there is no obvious reason why such an element should not exist, see the example below), but the non-existence of such elements proves in retrospect that σ is a non-inner automorphism.

15.2 Example. Let L be the covering group of the unitary group $K = \mathrm{U}_6(2)$, with center isomorphic to $C_2 \times C_2$. Then there is an (outer) automorphism ϕ of K of order 2 which leaves a normal subgroup $Z = \langle z \rangle$ of order 2 invariant, and a 2-central involution $x \in L \setminus \mathrm{Z}(L)$ such that $x\phi = zx$. However, this also holds for some $x \in \mathrm{Z}(L)$. (This has been checked using GAP [37].)

Some situations are easy to analyze. For example:

15.3 Proposition. *Assume that non-abelian composition factors of* $\mathrm{F}^*(G)$ *are alternating groups, and that no chief factor of* $G/\mathrm{F}^*(G)$ *is of prime order. Then* $\mathrm{Out}_{\mathrm{Col}}(G) = 1$. □

As illustration, we continue with an example.

15.4 Example. Let L be a finite group having a normal subgroup $Z = \langle z \rangle$ of order 2, and an automorphism ϕ of order 2 such that $x\phi = zx$ for some 2-central element x, but xz' is not a fixed point of ϕ for all $z' \in \mathrm{Z}(L)$.

Then there is a group G having a non-inner class-preserving Coleman automorphism of order 2 and the following properties: G has a minimal normal subgroup M of order 2^4, contained in the center of a normal subgroup F of G, such that F/M is a direct product of 15 copies of L/Z, and $G/F \cong A_5$, the alternating group of order 60.

Proof. We work with the presentation $A_5 = \langle s, t \,|\, s^2 = t^3 = (st)^5 = 1 \rangle$. A signed permu-

tation representation $\rho : A_5 \to \mathrm{GL}_{15}(\mathbb{Z})$ is given by $s \mapsto S$, $t \mapsto T$, where

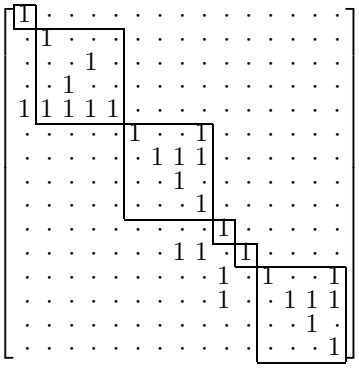
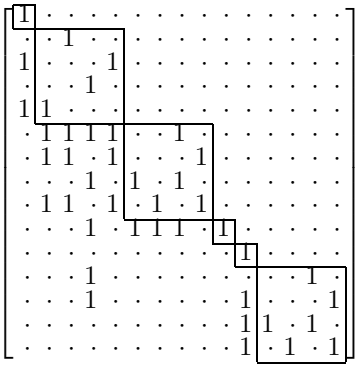
$$S = \begin{bmatrix}
 & 1 & & & & & & & & & & & & & \\
1 & & & & & & & & & & & & & & \\
 & & -1 & & & & & & & & & & & & \\
 & & & & 1 & & & & & & & & & & \\
 & & & & & & 1 & & & & & & & & \\
 & & 1 & & & & & & & & & & & & \\
 & & & & & & & & 1 & & & & & & \\
 & & & 1 & & & & & & & & & & & \\
 & & & & & & & 1 & & & & & & & \\
 & & & & & 1 & & & & & & & & & \\
 & & & & & & & & & & -1 & & & & \\
 & & & & & & & & & & & & 1 & & \\
 & & & & & & & & & -1 & & & & & \\
 & & & & & & & & -1 & & & & & & \\
 & & & & & & & 1 & & & & & & & \\
\end{bmatrix}, \quad T = \begin{bmatrix}
 & & 1 & & & & & & & & & & & & \\
 & & & 1 & & & & & & & & & & & \\
 & & & & 1 & & & & & & & & & & \\
 & & & & & & 1 & & & & & & & & \\
1 & & & & & & & & & & & & & & \\
 & & & & & & & & 1 & & & & & & \\
 & 1 & & & & & & & & & & & & & \\
 & & & & & & & & & & 1 & & & & \\
 & & & & & & & & & & & 1 & & & \\
 & & & & & & & & & & & & 1 & & \\
 & & & & & & & & & & & & & & 1 \\
 & & & & & 1 & & & & & & & & & \\
 & & & & & & & & & & & & & 1 & \\
 & & & & & & & & & & & 1 & & & \\
 & & & & & & & & & 1 & & & & & \\
\end{bmatrix}.$$

Let Π be a direct product of 15 copies of L. Then A_5 acts on Π as follows. The matrix $g\rho$ can be interpreted as an element of $\mathrm{GL}_{15}(\mathrm{Aut}(L))$ when the entries -1 are replaced by the automorphism ϕ. Then g acts on Π by right multiplication with this matrix. We form the corresponding semidirect product $H = \Pi \rtimes A_5$ (This is a "twisted wreath product" in the common sense [65, I.15.10].)

Let $V = Z \times \ldots \times Z \leq \Pi$, and write multiplication in V additively, thus identifying V with a 15-dimensional row space over $\mathbb{F}_2$. We write e_i for the row vector with entry 1 at i-th position and zero elsewhere.

We determined a composition series of the underlying $\mathbb{F}_2 A_5$-module V, together with a transformation matrix A, using the `matrix`-package in GAP [37]:

$$A := \left[\begin{array}{|cccccccccccccc|}
\hline
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
 & & 1 & & & & & & 1 & & & & 1 & \\
 & & & & 1 & & & & & & & & 1 & \\
 & & & & & & & & 1 & & & 1 & & \\
 & 1 & 1 & 1 & 1 & & 1 & 1 & 1 & & 1 & 1 & 1 & 1 \\
 & & & 1 & & & 1 & & 1 & & 1 & & & \\
 & & & & & & & 1 & & 1 & & & & \\
 & & & 1 & & 1 & & & & & & & & \\
 & & & 1 & & 1 & 1 & & & 1 & 1 & & & \\
 & & & & & & & & & & & & & \\
 & & & & & & & & & 1 & & & & \\
\hline
 & & & & & & & & & & 1 & & & \\
 & & & & & & & & & & 1 & & & \\
 & & & & & & & & & & 1 & & & \\
 & & & & & & & & & & 1 & & & \\
\hline
\end{array}\right],$$

$ASA^{-1} \overset{(2)}{\equiv}$  , $ATA^{-1} \overset{(2)}{\equiv}$  .

Set $f_i = e_i A$. Then $N = \langle f_1, \dots, f_{11} \rangle$ is a normal subgroup of H, and we put $G = \bar{H} = H/N$. Then $M = \bar{V}$ is the 4-dimensional faithful irreducible $\mathbb{F}_2 A_5$-module which is reducible over $\mathbb{F}_4$. With respect to the basis $\bar{f}_{12}, \dots, \bar{f}_{15}$, the elements $\bar{s}$, $\bar{t}$ act on M by multiplication with the 4×4-matrices in the lower-right corner in ASA^{-1}, ATA^{-1}. It is easily seen that M comes from the natural representation $A_5 \cong \mathrm{SL}(2,4)$, with $s = \left[\begin{smallmatrix} 1 & \zeta \\ 0 & 1 \end{smallmatrix}\right]$ and $t = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right]$ (ζ a primitive third root of unity). It is well known that $\mathrm{H}^1(A_5, M) \cong C_2 \times C_2$, with pairwise non-equivalent cocycles $\delta_a : s \mapsto (0, a)$, $t \mapsto 0$ ($a \in \mathbb{F}_4^\times$). The corresponding automorphisms of $M \rtimes A_5$ are non-inner, class-preserving automorphisms (see [123]).

Let $c = (x, x, \dots, x) \in \Pi$. Then $t^c = t$ and

$$\begin{aligned} s^c &= (0,0,1,0,0,0,0,0,0,0,1,0,1,1,0) \cdot s \\ &= ((f_2 + f_7 + f_8 + f_9 + f_{10} + f_{11}) + (f_{14} + f_{15})) \cdot s. \end{aligned}$$

Define an automorphism $\sigma \in \mathrm{Aut}(G)$ by $\sigma|_{\bar{\Pi}} = \mathrm{id}|_{\bar{\Pi}}$ and $\sigma|_{\bar{A}_5} = \mathrm{conj}(\bar{c})|_{\bar{A}_5}$.

Then for each $g \in G$, there is $m \in M$ with $g\sigma = g^m$, so σ is a class-preserving automorphism. By assumption, there is a Sylow 2-subgroup P of H such that $c \in \mathrm{Z}(P \cap \Pi)$, and then σ agrees on $\bar{P}$ with $\mathrm{conj}(\bar{c})$. Also, since σ induces the identity on G/M, σ agrees on each Sylow subgroup of odd order with some inner automorphism. Thus σ is a Coleman automorphism. Note that $f_{14} + f_{15} = e_{13}$, so that the extra condition on the group element x ensures that σ is a non-inner automorphism. □

15.5 Remark.

1. We may take for L a group like $S_3 \times C_2$, but then $G/\mathrm{F}^*(G)$ has chief factors of order 2.
2. If there exists a quasisimple group L satisfying the hypotheses of Example 15.4, then all questions posed in Problem 15.1 have a negative answer. (In this context, it might be helpful to understand the concept of splitting and stable involutions, cf. [43].) However, we couldn't find such a group.

The discussion leads us to the following question.

15.6 Problem. Let p be a prime. Is there a finite group L having the following properties:

- No chief factor of $L/\mathrm{O}_p(L)$ has order p;
- There is a central subgroup $\langle z\rangle$ of order p in L, a p-central element x in L and $\phi \in \mathrm{Aut}(L)$ of order p such that $x\phi = zx$, but there is no $z' \in \mathrm{Z}(L)$ such that xz' is a fixed point of ϕ.

If such a group L exists, is L necessarily non-solvable? (not p-constrained?)

1-cohomology

We have seen how 1-cohomology appears in the study of Coleman automorphisms. We briefly recall some general facts which might be helpful in some further discussion.

Let G be a finite group with an abelian normal subgroup A. Let $\mathrm{Aut}(G, A)$ be the group of automorphisms of G which leave A invariant. Thus each $\sigma \in \mathrm{Aut}(G, A)$ induces an automorphism $\bar\sigma$ of $\bar G = G/A$. Then the n-th cohomology group $\mathrm{H}^n(\bar G, A)$ has a natural structure as a right $\mathrm{Aut}(G, A)$-module; the action of $\sigma \in \mathrm{Aut}(G, N)$ is induced by its action $f^\sigma := (\bar\sigma^{-1} \times \ldots \times \bar\sigma^{-1})f\sigma$ on normalized cochains $f : \bar G \times \ldots \times \bar G \to A$. It is easily seen that $\mathrm{Inn}(G)$ acts trivially, so $\mathrm{H}^n(\bar G, A)$ can be viewed as a module for $\mathrm{Aut}(G, A)/\mathrm{Inn}(G)$.

The following has been observed by Dade (in a special case, see [29, 2.5]).

15.7 Proposition. *Let A be an abelian normal subgroup of the finite group G. Then the group $\mathrm{Out}_{\mathrm{Col}}(G)$ acts trivially on $\mathrm{H}^*(G/A, A)$.* □

Let $\mathrm{Aut}^1_1(G, A)$ denote the group of automorphisms $\sigma \in \mathrm{Aut}(G, A)$ with $\sigma|_A = \mathrm{id}$ and $\bar\sigma = \mathrm{id}$. It is well known that $\mathrm{Aut}^1_1(G, A) \cong \mathrm{Z}^1(\bar G, A)$, with $\sigma \in \mathrm{Aut}^1_1(G, A)$ corresponding to $\delta \in \mathrm{Z}^1(\bar G, A)$ defined by $\delta(\bar g) = g^{-1}(g\sigma)$. The inner automorphisms given by conjugation with an element of A correspond to the 1-coboundaries.

Let $\sigma \in \mathrm{Aut}^1_1(G, A)$. If q is a prime not dividing $|A|$, and Q is a Sylow q-subgroup of G, then it follows from Sylow's theorem (or a 1-cohomology argument) that $\sigma|_Q = \mathrm{conj}(a)|_Q$ for some $a \in A$.

From now on, we will assume that A is a p-group. Then $\sigma \in \mathrm{Aut}_{\mathrm{Col}}(G)$ if and only if $\sigma|_P = \mathrm{conj}(x)|_P$ for some Sylow p-subgroup P of G and $x \in G$.

Conversely, given some Sylow p-subgroup P of G and $x \in P$ with $x \in \mathrm{C}_G(A)$ and $\bar x \in \mathrm{Z}(\bar P)$, we might ask whether there is $\sigma \in \mathrm{Aut}^1_1(G, A)$ such that $\sigma|_P = \mathrm{conj}(x)|_P$.

This happens if and only if $[\delta] \in \mathrm{H}^1(\bar P, A)$, defined by $\delta(\bar g) = g^{-1}g^x = [g, x]$, lies in the image of the restriction map $\mathrm{H}^1(\bar G, A) \to \mathrm{H}^1(\bar P, A)$, that is, if $[\delta]$ is stable with respect to G (see [20, III(10.3)]).

So assume that $[\delta]$ is stable with respect to G, which means that $\mathrm{res}_{P,P^g\cap P}([\delta]) = \mathrm{res}_{P^g,P^g\cap P}([\delta^{\mathrm{conj}(g)}])$ for all $g \in G$. So for all $g \in G$ there is $a \in A$ such that for $y \in P^g \cap P$,

we have $[y,x] = \delta(\bar{y}) = \delta^{\mathrm{conj}(g)}(\bar{y})\cdot[y,a] = \delta(\bar{y}^{g^{-1}})^g\cdot[y,a] = [y^{g^{-1}},x]^g\cdot[y,a] = [y,x^g]\cdot[y,a]$. Hence

$$[\delta] \text{ is } G\text{-stable iff } \underset{g\in G}{\forall}\ \underset{a\in A}{\exists}\ \underset{y\in P^g\cap P}{\forall}\ [y,x] = [y,x^g]\cdot[y,a].$$

In particular, we get that $[x^{-1},g]$ centralizes $P^g \cap P \cap \mathrm{C}_G(A)$.

The following technical lemma might help to clarify some specific situations.

15.8 Lemma. *Let $A \le K \le G$ with A a normal p-subgroup of G, and $A \le \mathrm{Z}(K)$. Assume that $K/K^{(1)}A$ is a p'-group, and that there is $S \le K$, a subgroup of index p in a Sylow p-subgroup P of G. Finally, assume that $\mathrm{Z}(P/A) = T/A$ with $[T,A] = 1$ and $\mathrm{Z}(S)\mathrm{Z}(P) \subseteq A$. Then any p-central automorphism of G which is of p-power order is given by conjugation with an element of A.*

Proof. Replacing K, and P, by a suitable conjugate, we may assume that $\sigma|_P = \mathrm{id}|_P$. Let $\bar{G} = G/A$. There is a p-element $g \in G$ such that $\sigma_{\bar{G}} = \mathrm{conj}(\bar{g})$. It follows that $g \in P$ and $\bar{g} \in \mathrm{Z}(\bar{P})$, so $[g,A] = 1$. Hence $\tau = \sigma\cdot\mathrm{conj}(g^{-1})$ induces on both A and $\bar{G}$ the identity. Since $\mathrm{H}^1(\bar{K},A) = \mathrm{Hom}(\bar{K},A)$ consists of the trivial homomorphism only, it follows that $\tau|_K = \mathrm{id}|_K$, and consequently $[g,S] = 1$. If $g \in S$, then $g \in \mathrm{Z}(S)$, and otherwise $g \in \mathrm{Z}(P)$ since $[P:S] = p$. Hence $g \in A$ by assumption, and it follows that σ is given by conjugation with an element of A. □

For any finite simple group S, there is a prime p dividing the order of S such that p-central automorphisms of S are inner automorphisms [61, Theorem 14]. This implies that the same is true for each group G with $S \le G \le \mathrm{Aut}(S)$ [61, Remark 15]. One might ask whether the same is true for each covering group of G. As a concluding example, we consider the symmetric groups:

15.9 Proposition. *The group $\mathrm{Out}_{\mathrm{Col}}(G)$ is trivial for any covering group G of a symmetric group S_n.*

Proof. If $n \le 3$, then all Sylow subgroups of S_n are cyclic, the Schur multiplier of S_n is trivial and the assertion is obvious. So assume that $n \ge 4$, and let G be a covering group of S_n. It is known that G is isomorphic to one of the following groups (see [75, 2.12]):

$$S_n^* = \langle\, g_1,\dots,g_{n-1},z \mid g_i^2 = (g_jg_{j+1})^3 = (g_kg_l)^2 = z,\ z^2 = [z,g_i] = 1 \\ \text{for } 1 \le i \le n-1,\ 1 \le j \le n-2,\ k \le l-2 \,\rangle,$$

$$S_n^{**} = \langle\, g_1,\dots,g_{n-1},z \mid g_i^2 = (g_jg_{j+1})^3 = 1,\ (g_kg_l)^2 = z, \\ z^2 = 1,\ [z,g_i] = 1 \\ \text{for } 1 \le i \le n-1,\ 1 \le j \le n-2,\ k \le l-2 \,\rangle.$$

Note that in both cases, we have $g_k g_l = g_l g_k z$ for $k \leq l-2$ and $g_j g_{j+1} g_j = g_{j+1} g_j g_{j+1}$ for $1 \leq j \leq n-2$.

Let $\bar{G} = G/\langle z \rangle \cong S_n$; an isomorphism is given by letting $\bar{g}_i$ correspond to the cycle $(i, i+1)$.

Let $\sigma \in \mathrm{Aut}_{\mathrm{Col}}(G)$. Since the induced automorphism $\bar{\sigma}$ of $\bar{G}$ is a Coleman automorphism, it follows that $\bar{\sigma}$ is an inner automorphism (here, only the case $n = 6$ has to be considered, see [65, II.5.5]). Hence we may assume that $\bar{\sigma} = \mathrm{id}$, so σ is of 2-power order, σ fixes a Sylow 2-subgroup P of G, and there is $c \in P$ with $\sigma|_P = \mathrm{conj}(c)|_P$.

Note that σ restricted to the commutator subgroup $G^{(1)}$ is the identity. This is easily seen in the case $n = 4$, and if $n > 4$, this follows from the fact that $G^{(1)}/\langle z \rangle \cong A_n$ is perfect. Hence if $\sigma \neq \mathrm{id}$, that is, $\sigma|_P \neq \mathrm{id}|_P$, then $c \in G^{(1)}$.

Recall the following description of a Sylow 2-subgroup of S_n. If $n = \sum_{i=0}^{\infty} a_i 2^i$ with $a_i \in \{0, 1\}$ is the 2-adic expansion, then $\prod_{a_i \neq 0} 2^{2^i - 1}$ is the 2-part of $n!$, and a Sylow 2-subgroup of S_n is the direct product of Sylow 2-subgroups of the S_{2^i} with $a_i \neq 0$. These Sylow 2-subgroups can be described as iterated wreath products (see [65, III.15.3]).

Now assume that $\sigma \neq \mathrm{id}$. Then it follows from the description of the Sylow 2-subgroups that $\bar{c} \in \mathrm{Z}(\bar{P})$ is an involution, that we may assume $c = g_1 g_3 \cdots g_{2n+1}$ for some $n \geq 1$ (since $c \in G^{(1)}$) and that P contains the element $d = g_2 g_1 g_3 g_2$. We calculate

$$\begin{aligned} g_1 g_3 \cdot g_2 g_1 g_3 g_2 &= g_3 (g_1 g_2 g_1) g_3 g_2 \cdot z = g_3 g_2 g_1 (g_2 g_3 g_2) \cdot z \\ &= g_3 g_2 (g_1 g_3) g_2 g_3 \cdot z = (g_3 g_2 g_3) g_1 g_2 g_3 = g_2 g_3 (g_2 g_1 g_2) g_3 \\ &= g_2 (g_3 g_1) g_2 g_1 g_3 = g_2 g_1 g_3 g_2 \cdot g_1 g_3 \cdot z. \end{aligned}$$

It follows that $cd = dcz$, and $d\sigma = d^c = dz$. On the other hand, $d \in G^{(1)}$, so $d\sigma = d$. This contradiction shows that $\sigma = \mathrm{id}$, and the lemma is proven. □

16. Subdirect products of finite groups

In this section, we will touch upon the following problems in group theory, guided by possible applications to the Zassenhaus conjecture and the isomorphism problem.

- Given a finite group G, what are the possibilities to represent G as a subgroup of a direct product?
- Describe the structure of the subgroups of a direct product in terms of the subgroups of the direct factors.

Known results

Let $G_1, \ldots, G_n$ be finite groups. A subgroup of the direct product $D = G_1 \times \ldots \times G_n$ is called a *subdirect product* (of the G_i's). (We remark that many of the following definitions also make sense for infinite groups and infinitely many factors.)

Remak was the first who investigated in a series of papers [108, 107, 109, 110] how a finite group G can be written as a subdirect product, and introduced the following terminology. The finite group G is *subdirectly indecomposable* if is not a subgroup of the direct product of two groups of smaller order. Let G be a subgroup of $D = G_1 \times \ldots \times G_n$. The projection of G to G_i is the i-th *subdirect factor*. Assume that these projections are surjective. The kernel of the projection of G to $G_i^\wedge = G_1 \times \ldots \times G_{i-1} \times G_{i+1} \times \ldots \times G_n$ (i-th factor omitted) is the i-th *block component*. The i-th subdirect factor is *supernumerary* if the i-th block component is trivial; then G is a subdirect product of $G_i^\wedge$. The embedding $G \hookrightarrow D$ is an *economic subdirect decomposition* if each G_i is subdirectly indecomposable and not supernumerary.

Remak [107] studied subdirect products of two factors and showed that these are what is nowadays known as a pullback. A group G is subdirectly indecomposable if and only if G has exactly one nontrivial minimal normal subgroup. In an economic subdirect decomposition of G, the socle of G is the direct product of the minimal normal subgroups of the factors. Based on his work [108], Remak proved further results on subdirect products, depending on the properties of the socle of a group. In [109], Remak described a method of how to obtain an economic subdirect decomposition for a given group, and showed that all such decompositions are obtained in that way. In [110], Remak related certain subgroups of a subdirect product with three factors. As an application, he gave the following proposition.

16.1 Proposition ([110, Satz VII]). *Let G be a group with normal subgroups A, B and C. Then*

$$\frac{AB \cap C}{(A \cap C)(B \cap C)} \cong \frac{BC \cap A}{(B \cap A)(C \cap A)} \cong \frac{CA \cap B}{(C \cap B)(A \cap B)}$$

and each factor group is an abelian group.

We can, however, give a short and elementary proof of this proposition:

Proof. There is a well defined surjective map $AB \cap C \to BC \cap A/B \cap A$ which maps an element $c \in C$ which is of the form ab ($a \in A$, $b \in B$) to the coset $a(B \cap A)$. Indeed, $a = cb^{-1} \in BC \cap A$, and if $c = a_1b_1 = a_2b_2$ with $c \in C$, $a_1, a_2 \in A$ and $b_1, b_2 \in B$, then $a_1a_2^{-1} = c(b_1^{-1}b_2)c^{-1} \in B \cap A$. By definition, the kernel of this map is $B \cap C$. Hence there is an isomorphism $AB \cap C/B \cap C \to BC \cap A/B \cap A$ which carries $(A \cap C)(B \cap C)/B \cap C$ to $(A \cap C)(B \cap A)/B \cap A$, and the induced isomorphism on the factor groups gives the first isomorphism. The second isomorphism is obtained by interchanging B and C.

In order to prove that the first factor group is abelian, put $N = (A \cap C)(B \cap C)$ and let $^-$ denote the natural map $G \to G/N$. Then $\bar{A} \cap \bar{C} = 1$ and $\bar{B} \cap \bar{C} = 1$, and we have to show that $\bar{A}\bar{B} \cap \bar{C}$ is abelian. Hence we may assume that $A \cap C = 1$ and $B \cap C = 1$.

Then the group G is a pullback, as shown below,

$$\begin{array}{ccc} G & \longrightarrow & G/A \\ \downarrow & & \downarrow \\ G/C & \longrightarrow & G/AC \end{array}$$

The image of $AB \cap C$ in G/C is trivial, so we have to show that the image of $AB \cap C$ in G/A is abelian. Let $x, y \in (AB \cap C)A/A$. Then there are $b \in B$ and $c \in C$ such that $x = bA$ and $y = cA$, and since $[b, c] \in B \cap C = 1$, it follows that x and y commute, and we are done. □

Using lattice theory, Birkhoff [8, Theorem 26·2], [10, VI.5] proved an extension of this proposition. He also proved a representation theorem in universal algebra: every algebra can be represented as a subdirect union of subdirectly irreducible algebras (see [9], or [10, VI.6 Theorem 10]). It follows, for example, that any abelian group is a subdirect product (possibly infinitely many subdirect factors) of the groups $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ (see [9, Corollary 5]).

Again, let G be a subdirect product of groups G_i, $i \in I$. Loonstra [89] gives a criterion for when there exist a group F and homomorphisms $\alpha_i : G_i \to F$ $(i \in I)$ such that G consists of those tupels $(g_i)_{i \in I}$ with $g_i\alpha_i = g_j\alpha_j$ for all $i, j \in I$.

If $N_1, \ldots, N_n$ are normal subgroups of G whose intersection is trivial, then G is a subdirect product of the groups G/N_i in a natural way. We may also form a projective limit associated with G and the N_i, in which G embeds. Kimmerle and Roggenkamp [80] give a criterion for when G is isomorphic to this projective limit (see Corollary 16.9 below).

Bryce and Cossey [22, 21] investigate Fitting classes which are closed with respect to forming subdirect products.

Vedernikov [140] shows that finite subdirect products can be made by iterating the familar (pullback) construction of subdirect products with two subdirect factors, and uses this construction to describe those formations of finite groups whose subformations are all closed under taking subnormal subgroups.

Vedernikov [141] proves that the class of groups which have Hall π-subgroups, for some nonempty set π of prime numbers, is closed under finite subdirect products provided Schreier's conjecture holds. (Schreier's conjecture holds by the classification of the finite simple groups).

If G is a subdirect product of groups $G_1, \ldots, G_n$ and N is a normal subgroup of G such that each projection $N \to G_i$ is surjective, then G/N is nilpotent of class not exceeding n (see [42, Proposition 4.7]). Khukhro [78] constructs groups G/N of this type (for an infinity of values of n) that have increasing (with n) nilpotency class.

There is a well known description of all subgroups of the direct product of two finite groups (see [136, (4.19)], [138, (1.1)]). Seemingly, it is open whether there is a similar

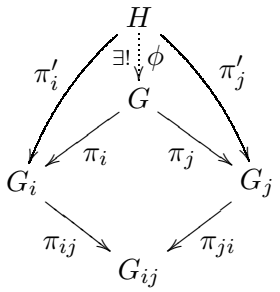
description of the subgroups of direct products of more then two finite groups (see Problem 16.2 below). Thévenaz [138] describes the maximal subgroups of the direct product G^n of n copies of a group G. In particular, if G is perfect then any maximal subgroup of G^n is the inverse image of a maximal subgroup of G^2 for some projection $G^n \to G^2$ onto two factors, and if G is perfect and finite then the number of maximal subgroups of G^n is a quadratic function of n (otherwise this number grows exponentially). Also, he deduces a theorem of Wiegold about the growth behavior of the number of generators of G^n.

Definitions

Let G_i and G_{ij} be finite groups with $G_{ij} = G_{ji}$ and $G_{ii} = G_i$, for all $1 \le i, j \le n$, n a natural number. Let $\pi_{ij} : G_i \to G_{ij}$ be homomorphisms (with π_{ii} the identity mapping). The *projective limit* of the groups G_i with respect to the homomorphisms π_{ij} is the subgroup

$$G = \operatorname*{proj\,lim}_{1\le i,j\le n}(G_i, \pi_{ij}) = \left\{(g_1, \dots, g_n) \in \prod_{i=1}^{n} G_i \;\middle|\; g_i\pi_{ij} = g_j\pi_{ji} \text{ for all } 1 \le i, j \le n\right\}$$

of the direct product of the G_i, i.e., a special subdirect product (cf. Problem 16.2 below). The projection $\pi_i : G \to G_i$ into the i-th component is clearly a homomorphism, and $\pi_i\pi_{ij} = \pi_j\pi_{ji}$ for all i, j. The projective limit G has the following universal property: whenever there is a group H and homomorphisms $\pi'_i : H \to G_i$ such that $\pi'_i\pi_{ij} = \pi'_j\pi_{ji}$ for all i, j, then there is a unique homomorphism $\phi : H \to G$ making the following diagrams commutative.



It does no harm to replace the G_i by the subdirect factors of G, i.e., to assume that the projections $\pi_i : G \to G_i$ are surjective. Then π_{ij} and π_{ji} have the same image in $G_{ij} = G_{ji}$, for all i, j, and we may also assume that the π_{ij} are surjective, so that all involved groups are factor groups of G.

Let G be a finite group, and let $N_1, \dots, N_n$ be normal subgroups of G. Put $G_i = G/N_i$, $G_{ij} = G/N_iN_j$, and let $\pi_{ij} : G_i \to G_{ij}$ be the natural maps. Then we write

$$\hat{G} = \operatorname*{proj\,lim}_{1\le i,j\le n}(G_i, \pi_{ij}),$$

and sometimes we omit to mention the π_{ij} in the definition of the projective limit. Note that if $\bigcap_{i=1}^n N_i = 1$, then G has a natural embedding into $\hat{G}$, but this need not be an isomorphism (see [80, Example 2.2]). We ask:

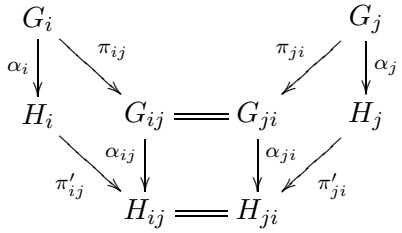
16.2 Problem. Let $D_1, \dots, D_n$ be normal subgroups of G such that $G \hookrightarrow \prod_{i=1}^n G/D_i$ is an economic subdirect decomposition of G. Is then $G \cong \operatorname{proj\,lim}_{1\le i\le n}(G/D_i)$?

A *homomorphism* between projective limits

$$G = \operatorname*{proj\,lim}_{1\le i,j\le n}(G_i, \pi_{ij}) \quad \text{and} \quad H = \operatorname*{proj\,lim}_{1\le i,j\le n}(H_i, \pi'_{ij})$$

(same index set!) is the obvious thing, i.e., a family of homomorphisms $\alpha_i : G_i \to H_i$ such that $\pi_i\alpha_i\pi'_{ij} = \pi_j\alpha_j\pi'_{ji}$ for all i, j. By the universal property, this family determines uniquely a homomorphism $G \to H$.

It would be nice to have a simpler criteria for when the family $(\alpha_i)_{1\le i\le n}$ is a homomorphism of projective limits. If the kernel of π_{ij} is contained in the kernel of $\alpha_i\pi'_{ij}$ for all i, j, then the α_i induce homomorphisms $\alpha_{ij} : G_{ij} \to H_{ij}$, and $(\alpha_i)_{1\le i\le n}$ is a homomorphism if $\alpha_{ij} = \alpha_{ji}$ for all i, j, which is also a necessary condition if all maps π_i, π_{ij} are surjective:



Here, we shall assume that a homomorphism between projective limits is understood in this stricter sense.

16.3 Example. There are two obvious examples of homomorphisms between projective limits. Let G_i, G_{ij} and π_{ij} be as above.

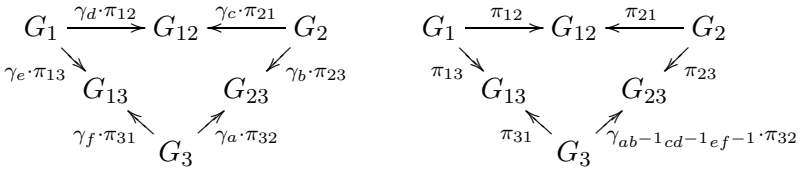
(1) Let $\alpha_1 \in \operatorname{Aut}(G_1)$, and let

$$\pi'_{ij} = \begin{cases} \alpha_1\pi_{12} & \text{if } i = 1,\ j = 2, \\ \pi_{ij} & \text{otherwise.} \end{cases} \qquad \pi''_{ij} = \begin{cases} \alpha_1^{-1}\pi_{1j} & \text{for } j > 2, \\ \pi_{ij} & \text{otherwise.} \end{cases}$$

Then $(\alpha_1, \mathrm{id}, \dots, \mathrm{id}) : \operatorname{proj\,lim}_{1\le i,j\le n}(G_i, \pi'_{ij}) \to \operatorname{proj\,lim}_{1\le i,j\le n}(G_i, \pi''_{ij})$ is an isomorphism of projective limits.

(2) Let $\sigma_{ij} \in \operatorname{Aut}(G_{ij})$ with $\sigma_{ij} = \sigma_{ji}$. Then there is an isomorphism of projective limits: $(\mathrm{id})_{1\le i,j\le n} : \operatorname{proj\,lim}_{1\le i,j\le n}(G_i, \pi_{ij}) \to \operatorname{proj\,lim}_{1\le i,j\le n}(G_i, \pi_{ij}\sigma_{ij})$.

16.4 Example. Let N_1, N_2, N_3 be normal subgroups of a group G, set $G_i = G/N_i$, $G_{ij} = G/N_iN_j$, and let $\pi_i : G \to G_i$, $\pi_{ij} : G_i \to G_{ij}$ be the natural maps. For $g \in G$ we agree that γ_g, when interpreted as an automorphism of G_i, is conjugation with $g\pi_i$. Then the two projective limits associated with the following data are isomorphic ($a, b, c, d, e, f \in G$):



Twisted projective limits

We briefly discuss the concept of twisted projective limits, considered in [117,80] in connection with the Zassenhaus conjecture and the isomorphism problem. Some examples are given at the end of this section.

Let $N_1, \dots, N_n$ be normal subgroups of the finite group G. Set $G_i = G/N_i$, $G_{ij} = G/N_iN_j$, and let $\pi_{ij} : G_i \to G_{ij}$ be the natural maps. Given a family σ of automorphisms $\sigma_{ij} \in \mathrm{Aut}(G_{ij})$, the projective limit

$$\hat{G}(\sigma) = \operatorname*{proj\,lim}_{1\le i,j\le n}(G_i, \pi_{ij}\sigma_{ij})$$

might be called a twisted projective limit (though $G_{ij} = G_{ji}$, we may have $\sigma_{ij} \neq \sigma_{ji}$, cf. Example 16.3(2)).

We remark that interest in these groups arises from the following theorem (see [80, Theorem 1.2]):

16.5 Theorem. *Let G be a finite solvable group, and set $\hat{G} = \operatorname{proj\,lim}_{p\in\pi(G)}(G/\mathrm{O}_{p'}(G))$. If H is a group basis of $\mathbb{Z}G$, then $H \cong \hat{G}(\sigma)$ for a family σ of class-preserving automorphisms.*

The structure of a twisted projective limit $\hat{G}(\sigma)$ may be not at all obvious (compared to that of $\hat{G}$). For example, we may ask:

16.6 Problem. Give necessary and/or sufficient conditions on σ such that $\hat{G}$ and $\hat{G}(\sigma)$ have the same order.

The following lemma can be extracted from the proof of [80, Lemma 2.3], which we will recover as Corollary 16.9.

16.7 Lemma. *Assume that $\hat{G}(\sigma)$ maps surjectively onto some factor G_i, and that N_i is a p'-group, for some prime p. Then Sylow p-subgroups of G and $\hat{G}(\sigma)$ are isomorphic.*

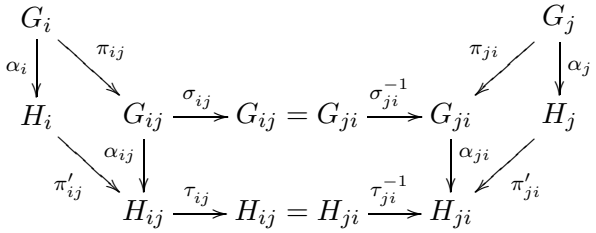
Proof. Let $\pi'_j : \hat{G}(\sigma) \to G_j$ $(1 \le j \le n)$ be the projections to the factors. By assumption, π'_i is surjective, and a Sylow p-subgroup of G_i is isomorphic to a Sylow p-subgroup of G. Hence we have to show that a Sylow p-subgroup P of $\hat{G}(\sigma)$ has trivial intersection with the kernel of π'_i. Take any $x \in P$ with $x\pi'_i = 1$, and let $j \in \{1, \dots, n\}$. Then $x\pi'_j$ is a p-element which lies in the kernel of π_{ji}. But the kernel of π_{ji} is the p'-group N_iN_j/N_j, so $x\pi'_j = 1$, and consequently $x = 1$. □

16.8 Corollary. *Assume that $\hat{G}(\sigma)$ maps surjectively onto all factors G_i, and that for each $p \in \pi(G)$, some N_i is a p'-group. Then $|\hat{G}(\sigma)| = |G|$.* □

16.9 Corollary ([80, Lemma 2.3]). *Let G be a finite group, and let $N_1, \dots, N_n$ be normal subgroups of G such that $\bigcap_{i=1}^n N_i = 1$, and that for each $p \in \pi(G)$, some N_i is a p'-group. Then $G \cong \operatorname{proj\,lim}_{1 \le i \le n}(G/N_i)$.* □

Again, we can discuss homomorphisms, between twisted projective limits. Let H be another finite group, and let $M_1, \dots, M_n$ be normal subgroups of H. Set $H_i = H/M_i$, $H_{ij} = H/M_iM_j$, let $\pi'_{ij} : H_i \to H_{ij}$ be the natural maps, and let τ be a family of automorphisms $\tau_{ij} \in \operatorname{Aut}(H_{ij})$.

If a family α of homomorphisms $\alpha_i : G_i \to H_i$ induce homomorphisms $\alpha_{ij} : G_{ij} \to H_{ij}$ $(1 \le i, j \le n)$ such that the following diagram commutes:



i.e., if $\alpha_{ij}(\tau_{ij}\tau_{ji}^{-1}) = (\sigma_{ij}\sigma_{ji}^{-1})\alpha_{ji}$ for all i, j, then α is a homomorphism of projective limits $\hat{G}(\sigma) \to \hat{H}(\tau)$. (Compare with [80, Definition 3.4].)

For a family of automorphisms $\sigma_{ij} \in \operatorname{Aut}(G_{ij})$, we are thus led to consider the family of automorphisms $\delta_{ij} = \sigma_{ij}\sigma_{ji}^{-1}$. The collection $\delta = (\delta_{ij})_{1 \le i,j \le n}$ is called a *cocycle*. Note that δ really consists of a family of automorphisms of the groups G_{ij}, since $\delta_{ij}^{-1} = \delta_{ji}$ (this condition also could have served for the definition of a cocycle).

The way twisted projective limits appear in the obstruction theory given in [80] suggests the following addition: If there are groups G_{ijk} (not depending on the order of the indices) and homomorphisms $G_{ij} \to G_{ijk}$, then we require in addition that δ_{ij} induce a homomorphism $\delta_{ij,k}$ of G_{ijk} such that $\delta_{ij,k}\delta_{jk,i} = \delta_{ik,j}$, for all $1 \le i, j, k \le n$ (think of $G_{ijk} = G/\mathrm{O}_{p'_i}(G)\mathrm{O}_{p'_j}(G)\mathrm{O}_{p'_k}(G)$).

A cocycle δ is called a *coboundary* if there is a family of automorphisms $\alpha_i \in \operatorname{Aut}(G_i)$ which induce automorphisms α_{ij} of the G_{ij} such that $\alpha_{ij}\delta_{ij} = \alpha_{ji}$ for all i, j, that is,

if and only if there exists an isomorphism (of projective limits) between $\hat{G}$ and $\hat{G}(\tau)$, where $\tau = (\tau_{ij})$ is such that $\tau_{ij} = \delta_{ij}$ if $i < j$ and $\tau_{ij} = \mathrm{id}$ otherwise.

16.10 Remark. If G and H are solvable groups and $\alpha : G \to H$ is a homomorphism (of abstract groups), then α is also a homomorphism between the projective limits $\hat{G} = \operatorname{proj\,lim}_{p\in\pi(G)}(G/\mathrm{O}_{p'}(G))$ and $\hat{H} = \operatorname{proj\,lim}_{p\in\pi(H)}(H/\mathrm{O}_{p'}(H))$ in the above sense. The same holds for homomorphisms of abstract groups between twisted projective limits $\hat{G}(\sigma)$ and $\hat{H}(\tau)$. (This holds in many other cases; the main point here is that the involved normal subgroups are characteristic.)

Automorphisms as projective limits

Let $G = \operatorname{proj\,lim}_{1\le i,j\le n}(G_i, \pi_{ij})$ be a projective limit as above. Let

$$\underline{\mathrm{Aut}}(G_i) = \{\sigma \in \mathrm{Aut}(G_i) \mid \sigma \text{ induces an automorphism of } G_{ij}, \text{ for all } j\}.$$

(Note that this definition does not depend on G_i alone, but this will hopefully cause no confusion.) There are natural maps $\theta_{ij} : \underline{\mathrm{Aut}}(G_i) \to \mathrm{Aut}(G_{ij})$.

Let us assume that the projections $\pi_i : G \to G_i$ are surjective, and that the kernels of the π_i are characteristic subgroups. Then

$$\begin{aligned}\mathrm{Aut}(G) &= \operatorname*{proj\,lim}_{1\le i,j\le n}(\underline{\mathrm{Aut}}(G_i), \theta_{ij}) \\ &= \Big\{(\sigma_1,\dots,\sigma_n) \in \prod_{i=1}^{n} \underline{\mathrm{Aut}}(G_i) \;\Big|\; \sigma_i\theta_{ij} = \sigma_j\theta_{ji} \text{ for all } 1 \le i,j \le n\Big\}.\end{aligned}$$

For solvable groups, we have the following characterization of Coleman automorphisms.

16.11 Lemma. *Let G be finite solvable group. Then $\mathrm{Aut}_{\mathrm{Col}}(G)$ consists of those automorphisms σ of G which induce inner automorphisms of all quotients $G/\mathrm{O}_{p'}(G)$, $p \in \pi(G)$.*

Proof. Let $N = \mathrm{O}_{p'}(G)$ and put $\bar{G} = G/N$, for some $p \in \pi(G)$. Assume that $\sigma \in \mathrm{Aut}(G)$ induces an inner automorphism of $\bar{G}$. Let P be a Sylow p-subgroup of G; we will show that the restriction of σ to P equals the restriction of some inner automorphism of G. Without lost of generality, σ induces the identity on $\bar{G}$. Then σ stabilizes NP, and by Sylow's theorem there is $m \in N$ such that $P\sigma = P^m$. Put $\tau = \sigma \cdot \mathrm{conj}(m^{-1})$. Then τ still induces the identity map of $\bar{G}$, and $P\tau = P$. It follows $x^{-1}(x\tau) \in N \cap P = 1$ for all $x \in P$, so the restriction of σ to P equals the restriction of $\mathrm{conj}(m)$. This proves one inclusion, and the other follows from a result of Gross [44, Corollary 2.4]. □

More generally, for an arbitrary finite group G, the group $\mathrm{Aut}_{\mathrm{Col}}(G)$ consists of those automorphisms σ of G which induce an inner automorphism of the principal block of $\mathbb{Z}_pG$, for all $p \in \pi(G)$ (a proof can be extracted from [126]).

For a solvable group G, the result allows us to describe $\mathrm{Aut}_{\mathrm{Col}}(G)$ as a projective limit. For the rest of this subsection, let G be a solvable group, let $\pi(G) = \{p_1, \ldots, p_n\}$, and put $G_i = G/\mathrm{O}_{p_i'}(G)$, $G_{ij} = G/\mathrm{O}_{p_i'}(G)\mathrm{O}_{p_j'}(G)$. Then $G = \operatorname{proj\,lim}_{1\le i\le n}(G_i)$ by Corollary 16.9. Note that the natural maps $\pi_{ij} : G_i \to G_{ij}$ induce maps $\pi_{ij}^* : G_i/\mathrm{Z}(G_i) \to G_{ij}/\mathrm{Z}(G_{ij})$. Lemma 16.11 shows that

$$\mathrm{Aut}_{\mathrm{Col}}(G) \cong \operatorname*{proj\,lim}_{1\le i\le n}(G_i/\mathrm{Z}(G_i), \pi_{ij}^*) = \operatorname*{proj\,lim}_{1\le i\le n}(\mathrm{Inn}(G_i)),$$

which provides a convenient way to compute $\mathrm{Aut}_{\mathrm{Col}}(G)$.

16.12 Example. Let $G = (C_3 \times C_5) \rtimes C_2$, where the cyclic group of order two acts by inversion (i.e., G is the dihedral group of order 30). Then $G_3 = G/\mathrm{O}_{3'}(G) = C_3 \rtimes C_2$, $G_5 = G/\mathrm{O}_{5'}(G) = C_5 \rtimes C_2$ and $\mathrm{Aut}_{\mathrm{Col}}(G) = \operatorname{proj\,lim}(\mathrm{Inn}(G_3), \mathrm{Inn}(G_5)) = G_3 \times G_5$. In particular, $\mathrm{Out}_{\mathrm{Col}}(G) \cong C_2$.

Also, with respect to the composite maps $\bar\pi_{ij} : G_i \xrightarrow{\pi_{ij}} G_{ij} \to G_{ij}/\mathrm{Z}(G_{ij})$ we can form the projective limit $H = \operatorname{proj\,lim}_{1\le i\le n}(G_i, \bar\pi_{ij})$, and then $\mathrm{Out}_{\mathrm{Col}}(H) = 1$.

Clearly $\underline{\mathrm{Aut}}(G_i)$ contains $\mathrm{Inn}(G_i)$, and we write $\underline{\mathrm{Out}}(G_i)$ for the quotient. The natural maps $\underline{\mathrm{Aut}}(G_i) \to \mathrm{Aut}(G_{ij})$ induce maps $\underline{\mathrm{Out}}(G_i) \to \mathrm{Out}(G_{ij})$. With respect to these maps, we have the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Inn}(G) & \longrightarrow & \mathrm{Aut}(G) & \longrightarrow & \mathrm{Out}(G) & \longrightarrow & 1 \\
 & & \downarrow & & \| & & \downarrow & & \\
1 & \longrightarrow & \mathrm{Aut}_{\mathrm{Col}}(G) & \longrightarrow & \operatorname*{proj\,lim}_{1\le i\le n}(\underline{\mathrm{Aut}}(G_i)) & \xrightarrow{\lambda} & \operatorname*{proj\,lim}_{1\le i\le n}(\underline{\mathrm{Out}}(G_i)) & &
\end{array}$$

The map λ is in general not surjective.

Let $\underline{\mathrm{Aut}}_n(\mathbb{Z}G_i)$ be the group of augmentation-preserving ring automorphisms of $\mathbb{Z}G_i$ which stabilize the relative augmentation ideals of the normal subgroups N_jN_i/N_i, where $N_i = \mathrm{O}_{p_i'}(G)$. Let $\mathcal{I}(\mathbb{Z}G_i)$ be the group of automorphisms of $\mathbb{Z}G_i$ which induce inner automorphisms of $\mathbb{Z}_{p_i}G_i$. Then $\underline{\mathrm{Aut}}_n(\mathbb{Z}G_i)/\mathcal{I}(\mathbb{Z}G_i) \cong \underline{\mathrm{Out}}(G_i)$, by the F*-Theorem (see [128, Theorem]).

Let $\Gamma = \operatorname{proj\,lim}_{1\le i\le n}(\mathbb{Z}G_i)$, a projective limit in the category of rings with respect to the maps $\mathbb{Z}G_i \to \mathbb{Z}G_{ij}$. Setting

$$\underline{\mathrm{Aut}}(\Gamma) = \operatorname*{proj\,lim}_{1\le i\le n}(\underline{\mathrm{Aut}}_n(\mathbb{Z}G_i)) \le \mathrm{Aut}(\Gamma),$$

we have an exact sequence

$$1 \to \operatorname*{proj\,lim}_{1\le i\le n}(\mathcal{I}(\mathbb{Z}G_i)) \to \underline{\mathrm{Aut}}(\Gamma) \xrightarrow{\mu} \operatorname*{proj\,lim}_{1\le i\le n}(\underline{\mathrm{Out}}(G_i)).$$

The quotient $\mathrm{im}(\mu)/\mathrm{im}(\lambda)$ measures to some extent how far Γ is away from satisfying a "simultaneous p-version" of the Zassenhaus conjecture, cf. [80].

Finally, we shall give a short proof of a result of Dade. We will use (for simplicity) the bar convention for all maps $G \to G_i$ (there will be no confusion), and set $N_i = \mathrm{O}_{p_i'}(G)$. Let $\sigma, \tau \in \mathrm{Aut}_{\mathrm{Col}}(G)$. Then $G = \{(\bar{g}, \dots, \bar{g}) \in \prod_{i=1}^n G_i \mid g \in G\}$. By Lemma 16.11, there are $x_i, y_i \in G$ such that σ induces the inner automorphism $\mathrm{conj}(\bar{x}_i)$ of G_i and τ induces the inner automorphism $\mathrm{conj}(\bar{y}_i)$ of G_i. It follows that $g^{x_i} \equiv g^{x_j} \mod N_i N_j$ for all $g \in G$, that is, $x_i x_j^{-1}$ maps to a central element in G/N_iN_j, and likewise $y_i y_j^{-1}$. It follows that $[\bar{x}_i, \bar{y}_i][\bar{x}_j, \bar{y}_j]^{-1} \in N_iN_j$, so $g = ([\bar{x}_1, \bar{y}_1], \dots, [\bar{x}_n, \bar{y}_n])$ is an element of G, and $[\sigma, \tau] = \mathrm{conj}(g) \in \mathrm{Inn}(G)$. Thus we have [29, Proposition 2.2]:

16.13 Proposition. *For a solvable group G, the group $\mathrm{Out}_{\mathrm{Col}}(G)$ is abelian.* □

Using the classification of the finite simple groups, this has been verified for any finite group G in [61, Theorem 11].

Pullbacks

Subgroups of the direct product of two finite groups are well understood: these are just (twisted) pullbacks. As illustration, we briefly describe the group-theoretical obstruction we met in Section 3.

Let G be a finite group, and let $N_1, N_2 \trianglelefteq G$ with $N_1 \cap N_2 = 1$. Set $\bar{G} = G/N_1N_2$. Then we have the following pullback diagram

$$\begin{array}{ccc} G & \xrightarrow{\pi_2} & G/N_2 \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \rho_2} \\ G/N_1 & \xrightarrow{\rho_1} & \bar{G} \end{array}$$

—the maps being the natural ones. Let $\sigma \in \mathrm{Aut}(\bar{G})$. We may form the "twisted" pullback H of the maps $\rho_1\sigma$ and ρ_2,

$$\begin{array}{ccccc} H & & \xrightarrow{\tau_2} & & G/N_2 \\ {\scriptstyle \tau_1}\downarrow & & & & \downarrow{\scriptstyle \rho_2} \\ G/N_1 & \xrightarrow{\rho_1} & \bar{G} & \xrightarrow{\sigma} & \bar{G} \end{array}$$

Then we have the following group-theoretical condition for when G and H are isomorphic.

16.14 Lemma. *With G and H given as above, suppose that each surjective homomorphism $G \to G/N_i$ has kernel N_i ($i = 1, 2$). Then $G \cong H$ if and only if there are $\phi_i \in \mathrm{Aut}(G/N_i)$, inducing automorphisms $\bar{\phi}_i$ of $\bar{G}$, so that $\sigma = \bar{\phi}_1^{-1}\bar{\phi}_2$.*

Proof. Let $\phi : G \to H$ be an isomorphism. By assumption, $\phi\tau_i$ has kernel N_i, so there is $\phi_i \in \mathrm{Aut}(G/N_i)$ with $\phi\tau_i = \pi_i\phi_i$.

Let $K = N_1\pi_2$, which is the kernel of ρ_2. Then $(K\phi_2)\rho_2 = N_1\pi_2\phi_2\rho_2 = N_1\phi\tau_2\rho_2 = N_1\phi\tau_1\rho_1\sigma = (N_1\pi_1)\phi_1\rho_1\sigma = 1$, so ϕ_2 stabilizes the kernel of ρ_2 and there is $\bar\phi_2 \in \mathrm{Aut}(\bar G)$ with $\phi_2\rho_2 = \rho_2\bar\phi_2$. Similarly, we get $\bar\phi_1 \in \mathrm{Aut}(\bar G)$ with $\phi_1\rho_1 = \rho_1\bar\phi_1$. Hence we have the following diagram, in which every square is commutative.

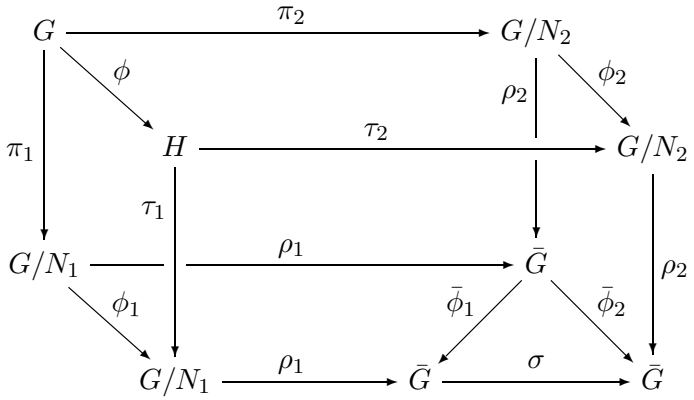


Diagram chasing shows that the "triangle" is commutative, too:

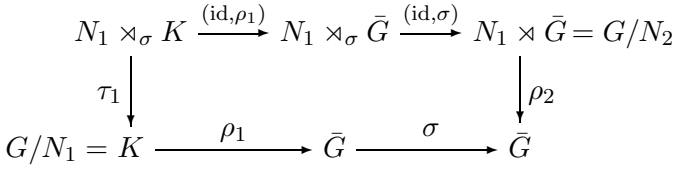
$$\pi_1\rho_1\bar\phi_1\sigma = \pi_1\phi_1\rho_1\sigma = \phi\tau_1\rho_1\sigma = \phi\tau_2\rho_2 = \pi_2\phi_2\rho_2 = \pi_2\rho_2\bar\phi_2 = \pi_1\rho_1\bar\phi_2,$$

so $\bar\phi_1\sigma = \bar\phi_2$ as $\pi_1\rho_1$ is surjective.

Conversely, given ϕ_i as above, $G \cong H$ follows from the universal property of the pullback. □

16.15 Remark. 1. The hypothesis of the Lemma is clearly satisfied if $N_i = \mathrm{O}_{p_i}(G)$ for different primes p_1, p_2.

2. In the special situation when N_1 has a complement K in G containing N_2, the group H has a convenient description: it is the semidirect product $N_1 \rtimes_\sigma K$, the action of K on N_1 being "twisted" by σ, i.e., $n^k = n^{\bar k\sigma}$ for all $n \in N_1$, $k \in K$. Indeed, the following diagram is commutative.



Projective limits with three factors

We shall collect some observations on twisted projective limits with three factors.

Let N_1, N_2, N_3 be normal subgroups of a finite group G such that for all $p \in \pi(G)$, some N_i is a p'-group. Again, let $G_i = G/N_i$, $G_{ij} = G/N_iN_j$, and let $\pi_i : G \to G_i$, $\pi_{ij} : G_i \to G_{ij}$ be the natural maps. Then $G = \operatorname{proj\,lim}_{1\le i\le 3}(G_i, \pi_{ij})$.

In the simplest case, we consider G, and for some $\gamma \in \operatorname{Aut}(G_1)$, the twisted projective limit H, as shown below.

$$G: \quad \begin{array}{ccccc} G_1 & \xrightarrow{\pi_{12}} & G_{12} & \xleftarrow{\pi_{21}} & G_2 \\ & {\scriptstyle\pi_{13}}\searrow & & \swarrow{\scriptstyle\pi_{23}} & \\ & & G_{13} \quad G_{23} & & \\ & {\scriptstyle\pi_{31}}\nwarrow & & \nearrow{\scriptstyle\pi_{32}} & \\ & & G_3 & & \end{array} \qquad H: \quad \begin{array}{ccccc} G_1 & \xrightarrow{\gamma\cdot\pi_{12}} & G_{12} & \xleftarrow{\pi_{21}} & G_2 \\ & {\scriptstyle\pi_{13}}\searrow & & \swarrow{\scriptstyle\pi_{23}} & \\ & & G_{13} \quad G_{23} & & \\ & {\scriptstyle\pi_{31}}\nwarrow & & \nearrow{\scriptstyle\pi_{32}} & \\ & & G_3 & & \end{array}$$

Then $|G| = |H|$ if and only if $[G, \gamma] = \langle g^{-1}(g\gamma) : g \in G\rangle \le N_1N_2N_3$. Indeed, the latter condition is equivalent to say that H maps surjectively onto the factor G_1, and the kernel of this map consists of elements of the form $(g\pi_1, g\pi_2, g\pi_3)$ $(g \in N_1)$, whence is equal to N_1.

Note that if $\gamma = \operatorname{conj}(x\pi_1)$ for some $x \in G$, then $x \in N_1N_2N_3$ implies that $G \cong H$ (this follows from Example 16.4).

Assume that $[G, \gamma] \le N_1N_2N_3$. Then for each $g \in G$, there are $a_g \in N_2$ and $b_g \in N_3$ (not uniquely determined) such that $(g\gamma^{-1}a_g, g, g) = (gb_g, g, g) \in H$. (We agree to write (g_1, g_2, g_3) instead of $(g_1\pi_1, g_2\pi_2, g_3\pi_3)$ for $g_i \in G$). Let $M_1 = N_2 \cap N_3$. The group H is the complex product of $M_1 \times 1 \times 1$ and $\{(gb_g, g, g) \mid g \in G\}$. In particular, we have extensions

$$1 \to M_1 \to G \to G/M_1 \to 1,$$

$$1 \to M_1 \to H \to G/M_1 \to 1,$$

which, however, need not have the same coupling (at least, there seems to be no obvious reason for this).

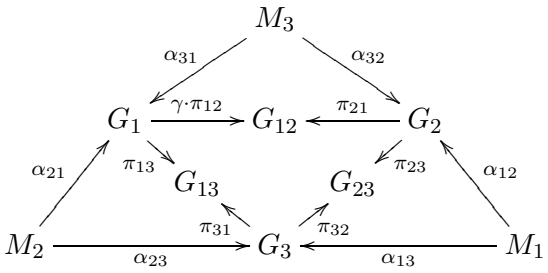
Note that there are surjections $H \to G/N_1 \xrightarrow{\pi} G/N_1M_1$ and $H \to G/M_1 \xrightarrow{\pi} G/N_1M_1$ (the π's are the natural maps) which necessarily have the same kernel. Hence there is $\sigma \in \operatorname{Aut}(G/N_1M_1)$ such that there is a pullback diagram

$$\begin{array}{ccc} H & \longrightarrow & G/N_1 \\ \downarrow & & \downarrow{\scriptstyle\pi\sigma} \\ G/M_1 & \xrightarrow[\pi]{} & G/N_1M_1 \end{array}$$

The next problem may be easy, but we did not elaborate on it.

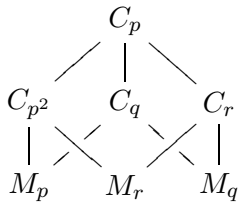
16.16 Problem. Describe the map σ.

Finally, set $M_1 = N_2 \cap N_3$ etc. Then there are homomorphisms $\alpha_{ij} : M_i \to G_j$ such that the following diagram is commutative, and $H \cong \operatorname{proj\,lim}(M_i, \alpha_{ij})$.

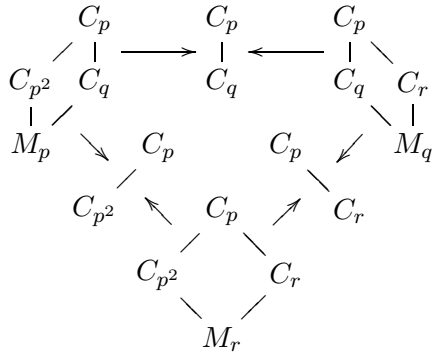


16.17 Example. (Non-isomorphic twisted projective limits.) We give a projective limit G where twisting with an inner automorphism leads to a non-isomorphic group of the same order.

Let p, q and r be different primes such that C_p acts on C_q and C_r. Form an iterated semidirect product G, as shown below (lines indicate faithful operation),



where M_i is a i-group such that only the inner automorphisms of $G/\mathrm{O}_{i'}(G)M_i$ can be lifted to automorphisms of $G_i := G/\mathrm{O}_{i'}(G)$, for $i = p, q, r$. (Note that such M_p, M_q, M_r exist, see [103].) Then $G = \hat{G} = \operatorname{proj\,lim}(G/\mathrm{O}_{p'}(G), G/\mathrm{O}_{q'}(G), G/\mathrm{O}_{r'}(G))$ can be visualized as follows.



Let x be a generator of the cyclic group C_p on the top of G. Then twisting some projection with the inner automorphism $\mathrm{conj}(\bar{x})$ yields a group H which has the same order as G, as we already noted before.

We claim that G and H are non-isomorphic. To demonstrate this, we first fix such a group H: Set $G_{ij} = G/\mathrm{O}_{i'}(G)\mathrm{O}_{j'}(G)$, define $\sigma_{ij} \in \mathrm{Aut}(G_{ij})$ by

$$\sigma_{ij} = \begin{cases} \mathrm{conj}(\bar{x}) & \text{if } (i,j) = (p,q), \\ \mathrm{id} & \text{otherwise} \end{cases}$$

and set $H = \hat{G}(\sigma)$, where $\sigma = (\sigma_{ij})$. The cocycle $\delta = (\delta_{ij})$ assigned to σ is given by

$$\delta_{ij} = \sigma_{ij}\sigma_{ji}^{-1} = \begin{cases} \mathrm{conj}(\bar{x}) & \text{if } (i,j) = (p,q), \\ \mathrm{conj}(\bar{x})^{-1} & \text{if } (i,j) = (q,p), \\ \mathrm{id} & \text{otherwise.} \end{cases}$$

Note that $G \cong H$ if and only if $\hat{G} \cong \hat{G}(\sigma)$ as projective limits, and that the latter holds if and only if δ is a coboundary (by our discussion on homomorphisms between twisted projective limits). Thus assume, by way of contradiction, that there are automorphisms $\alpha_i \in \mathrm{Aut}(G_i)$ which induce automorphisms α_{ij} of the G_{ij} such that $\alpha_{ij}\delta_{ij} = \alpha_{ji}$ for all i, j. Since the automorphisms α_i arise from an isomorphism $G \cong H$, each automorphism α_i induces an automorphism $\bar{\alpha}_i$ of $G/\mathrm{O}_{i'}(G)M_i$, which is, by assumption, an inner automorphism, $\mathrm{conj}(\bar{g}_i)$ (say). Write $g_i = y_i x^{n_i}$ in G, with $y_i \in \mathrm{O}_{p'}(G)\mathrm{O}_{q'}(G)\mathrm{O}_{r'}(G)$ and $1 \leq n_i \leq p$. Note that $\bar{\alpha}_i = \mathrm{conj}(\bar{g}_i)$ induces the automorphisms α_{ij}. Since x acts faithfully on the cyclic groups C_{p^2}, C_q and C_r, it follows from $\alpha_{pr} = \alpha_{pr}\delta_{pr} = \alpha_{rp}$ and $\alpha_{qr} = \alpha_{qr}\delta_{qr} = \alpha_{rq}$ that $n_p = n_r$ and $n_q = n_r$. But then $n_p = n_q$, which is impossible since $\alpha_{pq} \cdot \mathrm{conj}(\bar{x}) = \alpha_{qp}$. This contradiction shows that G and H are non-isomorphic.

It would be interesting to know what properties these groups might have in common.

V. On the normalizer problem for infinite groups

> Things done well, and with a care, exempt themselves from fear;
> things done without example, in their issue are to be fear'd.
>
> *William Shakespeare*
> *King Henry the Eighth, 1612*

Throughout this chapter, G denotes an arbitrary (i.e., possibly infinite) group.

For a group G, and a commutative ring R, the automorphisms of G inducing an inner automorphism of the group ring RG form a group $\mathrm{Aut}_R(G)$. We show that $\mathrm{Aut}_R(G)$ consists of class-preserving automorphisms, and that any automorphism in $\mathrm{Aut}_R(G)$ induces an inner (group) automorphism of G/N for some finite normal subgroup N of G. Thus the group $\mathrm{Out}_R(G) = \mathrm{Aut}_R(G)/\mathrm{Inn}(G)$ is periodic. If R is a G-adapted ring, then any outer automorphism from $\mathrm{Out}_R(G)$ has some representative which is given by conjugation with a unit whose support generates a finite normal subgroup. Extending results given by Jespers, Juriaans, de Miranda and Rogerio [72], it is shown that $\mathrm{Out}_R(G) = 1$ for certain classes of groups (comprising infinite p-groups, nilpotent groups and groups whose finite normal subgroups N are p-constrained with $\mathrm{O}_{p'}(N) = 1$ for some prime p), by reduction to the (known) finite group case.

17. Normalizers of group bases: general coefficients

Recall that G denotes an arbitrary group, and let R be a commutative ring, not necessarily G-adapted. In this section, we show that $\mathrm{Aut}_R(G) \leq \mathrm{Aut}_{\mathrm{c}}(G)$, and that any automorphism of $\mathrm{Aut}_R(G)$, after modification by an inner group automorphism, induces the identity on G/N for some finite normal subgroup N of G.

A *group basis* of RG is a group $H \leq \mathrm{V}(RG)$ which consists of R-linearly independent elements, such that $RG = RH$. Let $*_G$ be the anti-involution of RG associated with the group basis G, that is, $(\sum_{g\in G} r_g g)^{*_G} = \sum_{g\in G} r_g g^{-1}$ (all r_g in R). If $u = u^{*_G}$ for some $u \in RG$, then u might be called *G-symmetric*, or, more customary, simply *symmetric* (having the distinguished basis G explicitly in mind). Note that $*_G$ commutes with taking inverses. For $u \in \mathrm{U}(RG)$, we shall write $u^{-*_G} = (u^{-1})^{*_G}$ for short.

The most basic fact about elements of $\mathrm{N}_{\mathrm{U}(RG)}(G)$ involves the standard anti-involution of RG, and is given in the next lemma. Though it is well known (see [66]), we shall include the (short) proof.

17.1 Lemma. *Let $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$. Then $uu^{*_G} \in \mathrm{Z}(RG)$, so $[u, u^{*_G}] = 1$, and (an observation of Krempa) $(uu^{-*_G})^{*_G}(uu^{-*_G}) = 1$.*

Proof. Let $g \in G$ and write $* = *_G$. Then $u^{-1}gu = (u^{-1}g^{-1}u)^{-1} = (u^{-1}g^{-1}u)^* = u^*gu^{-*}$, so $uu^* \in \mathrm{Z}(RG)$, and $(uu^{-*})^*(uu^{-*}) = u^{-1}(u^*u)u^{-*} = 1$ follows. □

A classical result due to Higman and Berman says that if $uu^{*_G} = 1$ for some $u \in \mathbb{Z}G$, then $u \in \pm G$ (one just has to look at the 1-coefficient of uu^{*_G}). Thus the lemma immediately implies that $\mathrm{Out}_{\mathbb{Z}}(G)$ is of exponent 2, a result due to Krempa. This underlines the special role the coefficient ring $\mathbb{Z}$ plays, and the strength of such "star-arguments". Some of these arguments remain valid if $\mathbb{Z}$ is replaced by a suitable ring of algebraic integers (see [93], and Proposition 6.1).

For $x = \sum_{g\in G} r_g g$ (all r_g in R), the *support* $\mathrm{supp}(x)$ of x is the set $\{g \in G \mid r_g \neq 0\}$, and the *support group* of x is the group generated by $\mathrm{supp}(x)$. Note the little inconsistency: we should have written $\mathrm{supp}_G(x)$ rather than $\mathrm{supp}(x)$, but this will cause no confusion.

When studying $\mathrm{N}_{\mathrm{U}(RG)}(G)$, the first basic observation is that we can work in the group ring of the FC-center of G (see the lemma below). Hence we recall the following definitions and elementary properties (see, for example, [100, PART 2, 4§1]). The set $\Delta(G) = \{g \in G \mid g^G \text{ is finite}\}$ is a characteristic subgroup of G, called the *FC-center* of G. If $G = \Delta(G)$, then G is said to be a finite conjugate group (*FC-group* for short). The set of torsion elements $\Delta^+(G) = \{x \in \Delta(G) \mid x \text{ is of finite order}\}$ is a characteristic subgroup of $\Delta(G)$. If $\Delta(G)$ is finitely generated, then its center is of finite index in $\Delta(G)$, and $\Delta^+(G)$ is a finite group, with $\Delta(G)/\Delta^+(G)$ finitely generated torsion-free abelian.

We begin our investigations with taking a closer look at the support of elements of $\mathrm{N}_{\mathrm{U}(RG)}(G)$. The first statement of the following lemma has already been proved by Mazur [93, Corollary 1].

17.2 Lemma. *If $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ and $1 \in \mathrm{supp}(u)$, then*

$$\{h^{-1}h^u \mid h \in G\} \subseteq \mathrm{supp}(u) \subseteq \Delta(G).$$

Moreover, $\langle h^{-1}h^u : h \in G\rangle$ and $\langle \mathrm{supp}(u)\rangle$ are normal subgroups of G. If furthermore u is G-symmetric, then $\{h^{-1}h^v \mid h \in G, v \in \langle u\rangle\} \subseteq \mathrm{supp}(u)$.

Proof. Let $u = \sum_{g\in G} u_g g$ (all u_g in R), and set $\sigma = \mathrm{conj}(u)$. Comparing coefficients in $hu = u(h\sigma)$ $(h \in G)$ gives

$$u_{hg} = u_{g(h\sigma)} \quad \text{for all } g, h \in G. \tag{$*$}$$

Specializing to $g = h^{-1}$ yields $u_1 = u_{h^{-1}(h\sigma)}$ for all $h \in G$, and as $u_1 \neq 0$, it follows that $D = \{h^{-1}(h\sigma) \mid h \in G\} \subseteq \operatorname{supp}(u)$. Substituting $g = h^{-1}g$ in $(*)$ gives

$$u_g = u_{h^{-1}g(h\sigma)} = u_{g^h \cdot h^{-1}(h\sigma)} \quad \text{for all } g, h \in G.$$

As D is finite, the set $\{g^h \cdot h^{-1}(h\sigma) \mid h \in G\}$ is finite if and only if g^G is finite, and therefore $\operatorname{supp}(u) \subseteq \Delta(G)$. Moreover, if $g \in \operatorname{supp}(u)$ and $h \in G$, then $g^h = h^{-1}g(h\sigma) \cdot (h^{-1}(h\sigma))^{-1} \in \langle \operatorname{supp}(u) \rangle$, so $\langle \operatorname{supp}(u) \rangle \trianglelefteq G$. It follows from $(h^{-1}h^u)^g = [h,u]^g = [hg,u][g,u]^{-1}$ that $\langle D \rangle \trianglelefteq G$.

Assume that u is G-symmetric, and let $g \in G$ and $n, m \in \mathbb{Z}$. Then $u_{g^{-1}(g\sigma^n)} = u_{(g^{-1}\sigma^n)g} \overset{(*)}{=} u_{g(g^{-1}\sigma^{n+1})}$, and it follows inductively that $u_{g^{-1}(g\sigma^n)} = u_{g^{-\epsilon}(g^\epsilon \sigma^m)}$, with $\epsilon = 1$ if $n - m$ is even and $\epsilon = -1$ otherwise. So $u_{g^{-1}(g\sigma^n)} = u_1$ by $(*)$, and the proof is complete. □

We do not know whether the last statement of the lemma is true if u is not G-symmetric. The question arises whether the normal subgroups defined in the lemma are finite. We shall see in this section that this is true for $\langle h^{-1}h^u : h \in G \rangle$ in an important case, and in the next section, that also $\langle \operatorname{supp}(u) \rangle$ is finite under some natural restrictions on R.

However, we shall first show how the fact that $\operatorname{supp}(u) \subseteq \Delta(G)$ for $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ with $1 \in \operatorname{supp}(u)$ can be used to prove that $\operatorname{Aut}_R(G) \leq \operatorname{Aut}_{\mathrm{c}}(G)$. The proof follows the way which has been pursued by Mazur, who obtained partial results in [93] (however, see the remark following the proof!).

We shall repeatedly need the following trivial observation: for any $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$, and $N \trianglelefteq G$, the automorphism $\operatorname{conj}(u) \in \operatorname{Aut}(G)$ induces an automorphism of G/N since the inner automorphism $\operatorname{conj}(u) \in \operatorname{Aut}(RG)$ preserves the kernel of the natural map $RG \to RG/N$.

17.3 Theorem. $\operatorname{Aut}_R(G) \leq \operatorname{Aut}_{\mathrm{c}}(G)$ *for any group* G.

Proof. Let G be a counterexample, with $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ and $g \in G$ such that g and g^u are not conjugate in G. We may assume that $1 \in \operatorname{supp}(u)$; then $\operatorname{supp}(u) \subseteq \Delta(G)$ by Lemma 17.2. The subgroup H generated by $\operatorname{supp}(u)$ and g is also a counterexample (with the same data, i.e., $\sigma = \operatorname{conj}(u) \in \operatorname{Aut}(H)$ and $g \in H$). Note that $H/\Delta(H) = \langle \bar{g} \rangle$ since $\operatorname{supp}(u) \subseteq \Delta(G) \cap H \subseteq \Delta(H)$. As $\Delta(H)$ is a finitely generated FC-group, it follows from the definition of the FC-center that $[H : \mathrm{C}_H(\Delta(H))] < \infty$. In particular, g^n centralizes $\Delta(H)$ for some $n \in \mathbb{N}$. It follows that g^n is central in H, and therefore $g^n \in \Delta(H)$. (This reduction step has been given already by Mazur [93, p. 178].)

Choose a characteristic, central and torsion-free subgroup Z of $\Delta(H)$ with $[H : Z] < \infty$. Note that Z is finitely generated. Put $T = \Delta^+(H)$, a finite characteristic subgroup of $\Delta(H)$, with $\Delta(H)/T$ finitely generated torsion-free abelian.

For any natural number m, H/Z^m is a finite group, so σ induces a class-preserving automorphism σ_m of H/Z^m. In particular $\sigma_1 \in \mathrm{Aut_c}(H/Z)$, and we may assume (after modifying σ by a suitable inner automorphism) that $g\sigma = gz$ for some $z \in Z$.

Let $S = \{k \in \Delta(H) \mid [k, g] \in Z\}$, a subgroup of $\Delta(H)$ with Z as a subgroup of finite index. Since $\sigma_m \in \mathrm{Aut_c}(H/Z^m)$, there is $k_m \in \Delta(H)$ with $[k_m, g]z = g^{-k_m}(g\sigma) \in Z^m$, for all m. It follows that $k_m \in S$. These facts translate into matrix language as follows. Since ST/T is a finitely generated torsion-free abelian group, we may write ST/T as a product of n copies of $\mathbb{Z}$, for some $n \in \mathbb{N}$. Then the action of g on ST/T is given by multiplication with a matrix $A_g \in \mathrm{GL}(n, \mathbb{Z})$, and the system of linear equations $x(A_g - E) = -z$ (E the identity matrix) has modulo $m \in \mathbb{N}$ the solution k_m. Hence there is also a global solution. Translated back, this gives $s \in S$ with $[s, g]z = g^{-s}(g\sigma) \in T \cap Z = 1$, and the contradiction $g\sigma = g^s$. The theorem is proved. □

After having seen this work, I. B. S. Passi pointed out the following easy proof. For $g \in G$, the *partial augmentation* $\varepsilon_{[g]}$ is the R-linear map $\varepsilon_{[g]} : RG \to R$ such that if $h \in G$ is conjugate to g within G, then $\varepsilon_{[g]}(h) = 1$, and $\varepsilon_{[g]}(h) = 0$ otherwise. Note that $\varepsilon_{[g]}(xy) = \varepsilon_{[g]}(x^{-1}(xy)x) = \varepsilon_{[g]}(yx)$ for all $x, y \in G$, and therefore $\varepsilon_{[g]}(ab) = \varepsilon_{[g]}(ba)$ for all $a, b \in RG$ by linearity.

Short proof of Theorem 17.3. Let $\sigma \in \mathrm{Aut}_R(G)$, and take any $g \in G$. There is $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ such that $g\sigma = g^u$, and it follows that $\varepsilon_{[g]}(g\sigma) = \varepsilon_{[g]}(u^{-1}gu) = \varepsilon_{[g]}(g) = 1$. As $g\sigma \in G$, this shows that $g\sigma$ is conjugate to g within G, and the result follows. □

Due to Lemma 17.2, we are led to recall a theorem of Baer [7, Satz 3]. For convenience of the reader, and since we do not need all results established in [7] from which the theorem is deduced, a proof is included at the end of the section.

17.4 Theorem (Baer). *Assume that a group has a normal subgroup G with complement A such that the set $G^{-1+A} = \{[g, a] \mid g \in G, a \in A\}$ is finite. Then $[G, A] = \langle G^{-1+A} \rangle$ is a finite normal subgroup of GA.*

As an immediate consequence of this theorem and Lemma 17.2 we obtain the following corollary.

17.5 Corollary. *If $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ is G-symmetric and $1 \in \mathrm{supp}(u)$, then the normal subgroup of G generated by the elements $h^{-1}h^u$ ($h \in G$), is finite. In particular,* $\mathrm{conj}(u)$*, as an automorphism of RG, has finite order.* □

We like to mention [93, Lemma 6], thereby pointing out an important detail which will be needed for the proof of Theorem 17.8.

17.6 Lemma. *The image of* $\mathrm{Out}_R(G)$ *in* $\mathrm{Out}_R(G/\Delta^+(G))$ *is trivial. More precisely, for any $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ there is $x \in G$ such that* $\mathrm{conj}(ux)$ *induces the identity on $G/\Delta^+(G)$, and $1 \in \mathrm{supp}(ux)$.*

Proof. Let $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$. By Lemma 17.2, there is $g \in G$ such that $\mathrm{supp}(ug) \subseteq \Delta(G)$. Choose a maximal ideal m of R. Since $A = \Delta(G)/\Delta^+(G)$ is a torsion-free abelian group and $F = R/m$ is a field, the group ring FA has only trivial units (see [100, PART 13, §1]). Hence ug maps under the natural map $R\Delta(G) \to FA$ to a trivial unit, say λa ($\lambda \in F^\times$, $a \in A$). It follows that $\mathrm{conj}(ug)$ is given by conjugation with a on $FG/\Delta^+(G)$. Choose $h \in \Delta(G)$ with image a in A. Then $\mathrm{conj}(ugh^{-1})$ induces the identity on $G/\Delta^+(G)$, and as ugh^{-1} maps to λ in FA, there is $t \in \Delta^+(G)$ such that $1 \in \mathrm{supp}(ugh^{-1}t)$. With $x = gh^{-1}t$, we get the desired result. □

The following corollary was proved by Mazur [93, Corollary 9] under the additional assumption that G is finitely generated.

17.7 Corollary. *If $\Delta(G)$ is finitely generated, then $\mathrm{Out}_R(G)$ is a finite group.*

Proof. We begin with a trivial remark. Let G be an arbitrary group, and N a finite normal subgroup of G. Then the subgroup $S \leq \mathrm{Aut}(G)$ generated by the automorphisms $\mathrm{conj}(u)$ with $u \in \mathrm{N}_{\mathrm{U}(RG)}(G) \cap RN$ is finite. Indeed, $\mathrm{C}_G(N)$ is of finite index in G, and if T is a system of coset representatives of $\mathrm{C}_G(N)$ in G, then any $\sigma \in S$ is completely determined by its values on T, which are contained in the finite set TN.

Now assume that $\Delta(G)$ is finitely generated, and choose a central and torsion-free subgroup A of $\Delta(G)$ with $[\Delta(G) : A] < \infty$ which is normal in G. Then G is a pullback, as shown below.

$$\begin{array}{ccc} G & \longrightarrow & G/A \\ \downarrow & & \downarrow \\ G/\Delta^+(G) & \longrightarrow & G/A\Delta^+(G) \end{array} \qquad \text{(P)}$$

Let $S \leq \mathrm{Aut}_R(G)$ be the subgroup generated by the automorphisms $\mathrm{conj}(u)$ with $u \in \mathrm{N}_{\mathrm{U}(RG)}(G) \cap R\Delta(G)$ which induce the identity on $G/\Delta^+(G)$. By Lemma 17.6 and Lemma 17.2, it suffices to show that S is finite. But by the preliminary remark, the group of automorphisms of G/A induced by S is finite, and therefore also the group of automorphisms of the pullback (P) induced by S. The proof is complete. □

Using Theorem 17.4, we now can prove the following final result with respect to an arbitrary commutative coefficient ring R.

17.8 Theorem. *Any element of $\mathrm{Aut}_R(G)$ induces an inner automorphism of G/N for some finite normal subgroup N of G.*

Proof. Let $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$. By Lemma 17.6, there is $x \in G$ such that $\sigma = \mathrm{conj}(ux)$ induces the identity on $G/\Delta^+(G)$, and $1 \in \mathrm{supp}(ux)$. By Lemma 17.2, $H = \langle \mathrm{supp}(ux) \rangle \trianglelefteq G$ is a finitely generated FC-group. Choose a torsion-free normal subgroup A of finite index in H which is normal in G. Then σ induces on $\overline{G} = G/A$ an automorphism $\overline{\sigma}$

given by conjugation with $\overline{ux} \in R\overline{H}$, where $\overline{H} = H/A$ is a finite group. Hence $\overline{\sigma}$ is of finite order. As G is a pullback, as shown in (P), it follows that σ is of finite order. From Lemma 17.2 we know that the set $S = \{g^{-1}(g\sigma) \mid g \in G\}$ is finite. For any $n \in \mathbb{N}$ and $g \in G$,

$$g^{-1}(g\sigma^n) = g^{-1}(g\sigma) \cdot (g\sigma)^{-1}(g\sigma^2) \cdot \ldots \cdot (g\sigma^{n-1})^{-1}(g\sigma^n) \in S^n,$$

and as σ is of finite order, say m, $T = \{g^{-1}(g\tau) \mid g \in G, \tau \in \langle\sigma\rangle\} \subseteq S^m$ is a finite set too. Now it follows from Theorem 17.4 that $N = \langle T\rangle$ is a finite normal subgroup of G, and σ induces the identity on G/N. □

17.9 Corollary. *The group* $\mathrm{Out}_R(G)$ *is periodic.* □

One can also make some statement about the order of an element of this group (see [93, Theorem 1]), which is based on the fact that for a finite group G, prime divisors of the order of $\mathrm{Aut}_c(G)$ are contained in $\pi(G)$ (see [65, Kap. I, § 4, Aufg. 14]). One might ask, for general G, whether a prime dividing the order of an element of $\mathrm{Out}_R(G)$ is contained in $\pi(G)$ (cf. [93, p. 180]), but the next example shows that this is not the case. It also substantiates the necessity of the hypothesis of Theorem 18.4 below.

17.10 Example. The matrices $A = \left[\begin{smallmatrix} 2 & 1 \\ 3 & 2 \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 3 & 0 \\ 0 & 2 \end{smallmatrix}\right]$, viewed as elements of $\mathrm{GL}(2,5)$, have order 3 and 4, respectively, and $A^B = A^2$. Let

$$G = \langle\, v, w, a, b \;:\; v^5 = w^5 = [v,w] = 1,\ a^3 = 1,\ a^b = a^2,$$
$$v^a = v^2w,\ w^a = v^3w^2,\ v^b = v^3,\ w^b = w^2 \,\rangle.$$

Then $N = \langle v, w\rangle$ is an elementary abelian normal subgroup of G of order 25, on which a and b act via the matrices A and B, respectively. It follows that $\mathrm{Z}(G) = \langle b^4\rangle$, and $G/\mathrm{Z}(G)$ is the Frobenius group of order 300. An automorphism $\sigma \in \mathrm{Aut}(G)$ is defined by $v\sigma = v^2$, $w\sigma = w^2$, $a\sigma = a$ and $b\sigma = b$. We shall show that $\sigma \in \mathrm{Aut}_R(G)$, where $R = \mathbb{Z}[\frac{1}{5}]$ (see also [56, 58] for some theoretical background). Note that σ has order 4, whereas $\pi(G) = \{3, 5\}$.

Let $\widehat{X}$ denote the sum of the elements of a set X. Consider the element

$$t = \widehat{\langle v\rangle}b + \widehat{\langle vw^3\rangle}ba^2 + \widehat{\langle vw^2\rangle}ba + \widehat{\langle w\rangle}b^3 + \widehat{\langle vw^4\rangle}b^3a^2 + \widehat{\langle vw\rangle}b^3a.$$

It is easily checked that the summands of t are permuted under the conjugation action of $\langle a, b\rangle$, and that the product of any two distinct summands of t is contained in $\widehat{N}G$. Therefore tt^{*G} is modulo $\widehat{N}(\mathbb{Z}G)$ equivalent to five times the sum of the elements of the six nontrivial cyclic subgroups of N, so $tt^{*G} \equiv 5(5 + \widehat{N}) \mod \widehat{N}(\mathbb{Z}G)$. It follows that $u = \frac{1}{25}\widehat{N} + \left(1 - \frac{1}{25}\widehat{N}\right)\frac{1}{5}t \in \mathrm{V}(RG)$, with $u^{-1} = u^{*G}$. Finally, it is easily seen that $gt = t(g\sigma)$ for all $g \in G$, so $\sigma = \mathrm{conj}(u)$. Also note that there is no $g \in G$ such that $\langle \mathrm{supp}(ug)\rangle$ is a finite group.

We shall give two more illuminating examples. A homomorphism $r : \mathrm{Out}_R(G) \to \mathrm{Out}_R(\Delta(G))$ is defined as follows. Any $\alpha \in \mathrm{Out}_R(G)$ is represented by some $\mathrm{conj}(u) \in \mathrm{Aut}(G)$ with $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ and $1 \in \mathrm{supp}(u)$. Then $u \in R\Delta(G)$ by Lemma 17.2, and r maps α to the outer automorphism defined by $\mathrm{conj}(u)|_{R\Delta(G)}$. To show that r is well defined, let $\mathrm{conj}(u')$ with $u' \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ and $1 \in \mathrm{supp}(u')$ be another representative of α. Then $u^{-1}u' = gz$ for some $g \in G$ and $z \in \mathrm{Z}(RG)$. As $\mathrm{Z}(RG) \subseteq \mathrm{Z}(R\Delta(G))$, it follows that $g \in \Delta(G)$ and therefore $\mathrm{conj}(u)$ and $\mathrm{conj}(u')$ indeed define the same element in $\mathrm{Out}_R(\Delta(G))$. In [93, p. 181], it has been asked whether this map r is necessarily injective. The following simple example shows that this is not true.

17.11 Example. Let G be the group generated by elements v, w, b, c subject to the relations

$$w^8 = b^2 = c^2 = [b, c] = [v, w] = 1, v^b = v,\ v^c = v^{-1},\ w^b = w^{-1},\ w^c = w^5.$$

Then $\langle v\rangle \cong C_\infty$ and $G = \langle v\rangle \rtimes H$ with $H = \langle w, b, c\rangle$ of order 32. Clearly $\Delta(G) = \langle v, w, b\rangle$, and

$$u = \frac{1}{2}(1 + w^4) + \frac{1}{2}(1 - w^4)(w + w^{-1}) \qquad (**)$$

is a unit in the center of $\mathbb{Q}\Delta(G)$ with $1 \in \mathrm{supp}(u)$ which induces a non-inner automorphism of G (cf. [65, I 4.10b]). Hence $r : \mathrm{Out}_{\mathbb{Q}}(G) \to \mathrm{Out}_{\mathbb{Q}}(\Delta(G))$ is not injective.

In [93, p. 188], it has been asked whether for any FC-group G, the locally inner automorphisms in $\mathrm{Aut}_R(G)$ must be inner. We give an example showing that this is not the case. Recall that a *locally inner* automorphism of a group G is an automorphism ϕ of G such that for every finitely generated subgroup U of G, there is $\gamma \in \mathrm{Inn}(G)$ such that $\phi|_U = \gamma|_U$.

17.12 Example. Let G be the iterated semidirect product

$$G = \langle w : w^8\rangle \rtimes \langle b : b^2\rangle \rtimes \operatorname{\overset{\infty}{\mathrm{Dr}}}_{i=1}\langle c_i : c_i^2\rangle \rtimes \operatorname{\overset{\infty}{\mathrm{Dr}}}_{i=1}\langle a_i : a_i^2\rangle,$$

the actions given by $w^b = w^{-1}$, $w^{c_i} = w^5$, $b^{c_i} = b$, $w^{a_i} = w$, $b^{a_i} = b$ and $c_i^{a_i} = w^4 c_i$. (Here Dr denotes the restricted product.) Let u be defined as in $(**)$. Then $\mathrm{conj}(u) \in \mathrm{Aut}_{\mathbb{Q}}(G) \setminus \mathrm{Inn}(G)$ is a locally inner automorphism of the FC-group G.

We finish this section with a reproduction of a proof of the theorem of Baer.

Proof of Theorem 17.4. Let g, h denote elements of G, and a, b elements of A. Set $M = [G, A]$.

Claim. M, $\mathrm{C}_G(M)$ and $\mathrm{C}_G(A) \cap \mathrm{C}_G(M)$ are normal subgroups of GA.

Proof. Clearly, these subgroups of G are A-invariant. It follows from

$$[g,a]^h = [gh,a][h,a]^{-1} \qquad (\dagger)$$

that $M \trianglelefteq GA$. Consequently, $\mathrm{C}_G(M) \trianglelefteq GA$. If $g \in \mathrm{C}_G(A) \cap \mathrm{C}_G(M)$, then $(g^h)^a = h^{-1}[h^{-1},a]gh^a = h^{-1}g[h^{-1},a]h^a = g^h$, showing that $\mathrm{C}_G(A) \cap \mathrm{C}_G(M)$ is G-invariant.

As $F = G^{-1+A}$ is a finite set, we may assume that A is finitely generated. Further, we may assume that $\mathrm{C}_A(G) = 1$.

Claim. $[G : \mathrm{C}_G(M)] < \infty$.

Proof. The automorphism $\mathrm{conj}(h)|_M$ of M is completely determined by its effect on F. It follows from (†) that $\mathrm{conj}(h)|_M$ maps the *finite* set F into the *finite* set FF^{-1}, so $\{\mathrm{conj}(h)|_M \mid h \in G\}$ is a finite group.

Claim. $\nu = [G : \mathrm{C}_G(A)] < \infty$ and A is a finite group.

Proof. The map $[\cdot,a]$ from right cosets of $\mathrm{C}_G(a)$ in G to F given by $\mathrm{C}_G(a) \cdot g \mapsto [g,a]$ is a well defined injective map, so $[G : \mathrm{C}_G(a)] < \infty$. As $\mathrm{C}_G(A)$ is a finite intersection of subgroups $\mathrm{C}_G(a)$, it follows that $[G : \mathrm{C}_G(A)] < \infty$.

Now there is the well defined map $[\cdot,a]$ from the *finite* set of right cosets of $\mathrm{C}_G(A)$ in G to F, given by $\mathrm{C}_G(A) \cdot g \mapsto [g,a]$, and $[\cdot,a] = [\cdot,b]$ implies $a = b$ since $\mathrm{C}_A(G) = 1$. Consequently, A is finite.

Since $[G : \mathrm{C}_G(M)]$ is finite, $\mathrm{Z}(M) = M \cap \mathrm{C}_G(M)$ is of finite index in M. It is well known (see [65, IV 2.3]) that this implies that $[M,M]$ is finite. Let $m \in M$. As $m^\nu \in \mathrm{C}_G(A)$, we have

$$[m,a]^\nu = (m^{-1}m^a)^\nu \equiv m^{-\nu}(m^a)^\nu \equiv m^{-\nu}(m^\nu)^a \equiv 1 \mod [M,M],$$

so $[M,A]^\nu \subseteq [M,M]$. Using the commutator identity $[x,yz] = [x,z][x,y][[x,y],z]$ (see [65, III 1.2]), we get for $i \in \mathbb{N}$

$$\begin{aligned}[g,a^i] &= [g,a^{i-1}a] = [g,a] \cdot [g,a^{i-1}] \cdot [[g,a^{i-1}],a] = \dots \\ &= [g,a]^i \cdot [[g,a],a] \cdots [[g,a^{i-2}],a] \cdot [[g,a^{i-1}],a].\end{aligned}$$

With α being the order of A, we get $1 = [g,a]^\alpha \cdot [[g,a],a] \cdots [[g,a^{\alpha-2}],a] \cdot [[g,a^{\alpha-1}],a]$. Since $[[g,a^i],a] \in [M,A]$ for all i, we get

$$1 = \big([g,a]^\alpha \cdot [[g,a],a] \cdots [[g,a^{\alpha-2}],a] \cdot [[g,a^{\alpha-1}],a]\big)^\nu \equiv [g,a]^{\alpha\nu} \mod [M,M].$$

Since the elements $[g,a]$ form the finite generating set F of M and $[M,M]$ is finite, M is a finite group. □

18. Normalizers of group bases: G-adapted coefficients

It was shown in [74, 72, 70] that some group ring problems can be reduced to the finite group case. We shall give short and unified proofs of these results. The basic observation can be extracted from [74]:

18.1 Lemma. *Let G be a group which has a finite normal subgroup T such that G/T is a finitely generated torsion-free abelian group. Let $u \in \mathrm{U}(\mathbb{Z}G)$, and write $u = \sum_i g_i x_i$ with all $x_i \in \mathbb{Z}T$, and the $g_i \in G$ belonging to different cosets of T in G. Then we have that $u = g_i x_i$ for some index i provided the following holds for each central primitive idempotent e in $\mathbb{Q}T$:*

(i) *$x_i e$ is either zero or a unit in $(\mathbb{Q}T)e$, for all i;*

(ii) *if $x_i e \neq 0$, then $x_i e^g \neq 0$, for all i and $g \in G$.*

Proof. Let $1 = e_1 + e_2 + \ldots + e_n$ be a decomposition of the identity into central primitive idempotents of $\mathbb{Q}T$. Let f be an orbit sum of the conjugacy operation of G on the e_j's. Then uf is a unit in $(\mathbb{Q}G)f$, and since G/T is ordered, it follows by a classical argument (see, for example, [129, (45.3)]) that $uf = g_k x_k f$ (some k). The unit u is the sum of all such (uf)'s. Collecting terms with the same g_k, we get $u = \sum h_l a_l f_l$, where the pairwise different h_l's are contained in the set formed by the g_k's, the f_l's are orthogonal idempotents in $\mathbb{Q}T$, central in $\mathbb{Q}G$ and summing up to one, and each $a_l \in \mathbb{Q}T$ is such that $a_l f_l$ is a unit in $(\mathbb{Q}T)f_l$. Comparing coefficients, we see that each $a_l f_l \in \mathbb{Z}T$. Let $b_l \in (\mathbb{Q}T)f_l$ with $a_l b_l = f_l$, and set $v = \sum b_l h_l^{-1} f_l$. Then $uv = vu = 1$, so $v = u^{-1} \in \mathbb{Z}G$. Comparing coefficients, we see that $b_l f_l \in \mathbb{Z}T$. Hence $f_l = a_l f_l b_l f_l \in \mathbb{Z}T$. As $\mathbb{Z}T$ has no (nontrivial) central idempotents, this proves the lemma. □

The following proposition appears as a "representation theorem" in [72, Theorem 1.4].

18.2 Theorem. *Let G be a group and $u \in \mathrm{N}_{\mathrm{U}(\mathbb{Z}G)}(G)$. Then for any $g \in \mathrm{supp}(u)$, there is a finite normal subgroup T of G such that $g^{-1}u \in \mathbb{Z}T$.*

Proof. Let $u \in \mathrm{N}_{\mathrm{U}(\mathbb{Z}G)}(G)$ such that $1 \in \mathrm{supp}(u)$, and set $H = \langle \mathrm{supp}(u) \rangle$. Then H is a normal subgroup of G contained in $\Delta(G)$ by Lemma 17.2. Consequently, H is a finitely generated FC-group, and $T := \Delta^+(H)$ is a finite normal subgroup of G, with H/T finitely generated torsion-free abelian. We can assume that $G = H$.

Write $u = \sum g_i x_i$ as in Lemma 18.1. Comparing coefficients in $Tu = uT$ shows that $Tx_i = x_i T$ for all i. In particular, $I_i = (\mathbb{Z}T)x_i = x_i(\mathbb{Z}T)$ is a two-sided ideal in $\mathbb{Z}T$. Let e be a central primitive idempotent in $\mathbb{Q}T$. Then $\mathbb{Q}I_i e$ is a two-sided ideal in the block $(\mathbb{Q}T)e$, so $x_i e$ is either zero or a unit in $(\mathbb{Q}T)e$. Take any $g \in G$. Since G/T is abelian, it follows from $\sum g_i[g_i, g]x_i^g = u^g = u[u, g] = \sum g_i x_i [u, g]$ that $(Tx_i T)^g = Tx_i T$. Consequently $Tx_i e^g T = (Tx_i e T)^g$, so if $x_i e \neq 0$, then $x_i e^g \neq 0$. The claim now follows from Lemma 18.1. □

The next proposition appears as a "representation theorem" in [70, Theorem 1.4].

18.3 Theorem. *Let G be a group and $u \in \Delta(\mathrm{U}(\mathbb{Z}G))$. Then for any $g \in \mathrm{supp}(u)$, there is a finite normal subgroup T of G such that $g^{-1}u \in \mathbb{Z}T$.*

Proof. Let $u \in \Delta(\mathrm{U}(\mathbb{Z}G))$ and set $H = \langle x^g \mid x \in \mathrm{supp}(u), g \in G\rangle \trianglelefteq G$. Then H is a finitely generated FC-group, and we can assume that $G = H$. Set $T := \Delta^+(H)$.

Write $u = \sum g_i x_i$ as in Lemma 18.1, and let e be a central primitive idempotent in $\mathbb{Q}T$. If $(\mathbb{Q}T)e$ is a division ring, then it is clear that $x_i e$ is either zero or a unit in $(\mathbb{Q}T)e$. Let M be the sum of the blocks of $\mathbb{Q}T$ that are proper matrix rings. Clearly, there are elements $f_1, \dots, f_n$ of square zero in $\mathbb{Z}T$ which generate M as a $\mathbb{Q}$-algebra. Then $f_j u = u f_j$ implies that $f_j^{g_i} x_i = x_i f_j$, and since M^g for all $g \in G$, it follows that $x_i M = M x_i$. Thus if $e \in M$, then $x_i M e$ is a two-sided ideal in the block Me, meaning that $x_i e$ is either zero or a unit in $(\mathbb{Q}T)e$. Assume there is $g \in G$ with $e^g \neq e$. Then eg is of square zero, so $(eg)u = u(eg)$, that is, $\sum g_i x_i e^{gg_i} = \sum g_i [g_i, g](x_i e)^g$. Since G/T is abelian, it follows that $x_i e^{gg_i} = [g_i, g](x_i e)^g$. Consequently $e^{gg_i} = e^g$ if $x_i e \neq 0$, and then also $x_i e^g \neq 0$. The claim now follows from Lemma 18.1. □

It is obvious that the above results hold more generally for a $\Delta^+(G)$-adapted coefficient ring. In fact, we have the following theorem.

18.4 Theorem. *Let R be a commutative ring such that for each finite normal subgroup T of G, the group ring RT has no (nontrivial) central idempotents, and KT is semisimple for some ring extension $R \subseteq K$. Then for any $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ with $1 \in \mathrm{supp}(u)$, the support group $\langle \mathrm{supp}(u)\rangle$ is a finite normal subgroup of G.* □

We shall apply this theorem in the following form.

18.5 Theorem. *Let R be a $\Delta^+(G)$-adapted ring. Then for any $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ with $1 \in \mathrm{supp}(u)$, the support group $\langle \mathrm{supp}(u)\rangle$ is a finite normal subgroup of G.* □

The next corollary shows in particular that central units of finite order in RG are trivial (see also [76, Theorem 2.13], but note that our condition on R is weaker). A different proof has been given by Mazur [93, Lemma 8]. The reader might convince himself that for $R = \mathbb{Z}$, the corollary follows readily from a "star-argument".

18.6 Corollary. *Let R be a $\Delta^+(G)$-adapted ring, and $u \in \mathrm{N}_{\mathrm{V}(RG)}(G)$ such that $u^n \in G$ for some $n \in \mathbb{N}$. Then $u \in G$. In particular, central units of finite order in $\mathrm{V}(RG)$ are contained in G.*

Proof. Let $g \in \mathrm{supp}(u)$. By Theorem 18.5, $N = \langle \mathrm{supp}(ug^{-1})\rangle$ is a finite normal subgroup of G. Now $(ug^{-1})^n \in G \cap RN = N$, so ug^{-1} has finite order, and $\langle N, ug^{-1}\rangle$ is a finite subgroup of RN. Hence $ug^{-1} \in N$ (see, for example, [76, Proposition 2.15]), and the corollary is proved. □

18.7 Corollary. *If R is a $\Delta^+(G)$-adapted ring, then the order of any element of the periodic group $\mathrm{Out}_R(G)$ is divisible only by primes from $\pi(\Delta^+(G))$.*

Proof. Let $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ with $1 \in \mathrm{supp}(u)$. By Theorem 18.5, $N = \langle \mathrm{supp}(u) \rangle$ is a finite normal subgroup of G. Since $\mathrm{conj}(u)|_N \in \mathrm{Aut}_{\mathrm{c}}(N)$, and prime divisors of the order of $\mathrm{Aut}_{\mathrm{c}}(N)$ are contained in $\pi(N)$ (see [65, Kapitel I, §4, Aufgabe 14]), the result follows. □

19. Groups satisfying the normalizer property

We shall say that a group G has the *normalizer property* if $\mathrm{Out}_R(G) = 1$, or, equivalently, $\mathrm{N}_{\mathrm{V}(RG)}(G) = \mathrm{Z}(\mathrm{V}(RG))G$ for any G-adapted ring R. Using a strong version of the Ward–Coleman Lemma for infinite groups, we prove a lemma which allows us to reduce the question whether $\mathrm{Out}_R(G) = 1$ or not in certain cases to the finite group case, and give examples thereof. In particular, p-groups, nilpotent groups and groups whose finite normal subgroups N are p-constrained with $\mathrm{O}_{p'}(N) = 1$ for some prime p have the normalizer property, and also a well known result of Jackowski and Marciniak extends to infinite groups. These results strongly extend results obtained by Jespers, Juriaans, de Miranda and Rogerio [72, Theorem 2].

First of all, however, we shall clarify the structure of $\mathrm{N}_{\mathrm{V}(RG)}(G)/G$. Using different methods, this has been done in [93, Theorem 8] for G with finitely generated FC-center, and a ring R of algebraic integers, and in [72, Corollary 1.5] for $R = \mathbb{Z}$ (note that the proof given there depends on a "star-argument").

19.1 Proposition. *Let R be a $\Delta^+(G)$-adapted ring. Then $\mathrm{N}_{\mathrm{V}(RG)}(G)/G$ is a torsion-free abelian group. If $\Delta(G)$ is finitely generated, then $\mathrm{N}_{\mathrm{V}(RG)}(G)/G$ has the same rank as $\mathrm{Z}(\mathrm{V}(RG))/\mathrm{Z}(G)$.*

Proof. By Corollary 18.6, $\mathrm{N}_{\mathrm{V}(RG)}(G)/G$ is torsion-free. Let $u, v \in \mathrm{N}_{\mathrm{V}(RG)}(G)$. We have to show that $[u, v] \in G$, and, without lost of generality, we may assume that $1 \in \mathrm{supp}(u)$ and $1 \in \mathrm{supp}(v)$. Then $\langle \mathrm{supp}(u), \mathrm{supp}(v) \rangle$ is a finite normal subgroup of G by Theorem 18.5. Thus we may suppose that G is finite. Embed the quotient field of R into a splitting field K of G. Then KG is a direct sum of full matrix rings over K, and the projection of $[u, v] \in \mathrm{V}(RG)$ to each of these has determinant 1. Since $[u, v]$ has finite order over the center $\mathrm{Z}(\mathrm{V}(RG))$, it follows that $[u, v]$ is of finite order, so $[u, v] \in G$ by Corollary 18.6.

Now let G be again an arbitrary group, and set $\mathcal{C} = \mathrm{Z}(\mathrm{V}(RG))$. If $\Delta(G)$ is finitely generated, then $\mathrm{N}_{\mathrm{V}(RG)}(G)/\mathcal{C}G$ is a finite group by Corollary 17.7, so $\mathrm{N}_{\mathrm{V}(RG)}(G)/G$ has the same rank as $\mathcal{C}G/G$, which is isomorphic to $\mathcal{C}/\mathrm{Z}(G)$. □

If $R = \mathbb{Z}$, we have the following interesting result, which is based on an observation of Jackowski and Marciniak (see the proof of [66, 3.5. Theorem]).

19.2 Proposition. *If $R = \mathbb{Z}$, then $\mathrm{N}_{\mathrm{V}(RG)}(G)/G$ can be generated by symmetric units whose support contains* 1.

Proof. Let $u \in \mathrm{N}_{\mathrm{V}(\mathbb{Z}G)}(G)$; we have to show that $(hu)^* = hu$ for some $h \in G$ and $* = *_G$. By Theorem 18.5, we may assume that G is finite. Let $H = \mathrm{C}_G(u) = \mathrm{C}_G(u^*)$. By Lemma 17.1, $c = uu^*$ is a central element, and $(uu^{-*})^*(uu^{-*}) = 1$, so $uu^{-*} = x$ for some $x \in G$ by a classical result due to Higman and Berman. Note that $x \in \mathrm{Z}(H)$. Write $x = x^s x^{2t}$ $(s, t \in \mathbb{N})$ such that x^s is the 2-part of x, and x^{2t} is the $2'$-part of x. Then $(ux^{-t})^2 = u^2 x^{-2t} = cuu^{-*}x^{-2t} = cx^s$. Hence we may suppose that $u^{2^m} \in \mathrm{Z}(\mathbb{Z}G)$ for some $m \in \mathbb{N}$. Let $u = \sum_{g\in G} a_g g$ (all a_g in $\mathbb{Z}$). Then $a_g = a_{g^u}$ and $a_{g^{-1}} = a_{xg}$ for all $g \in G$. Note that $x \in \mathrm{Z}(H)$ implies that H is a disjoint union of the sets $S(h) = \{h^{-1}, xh\}$. Since the augmentation of u is not divisible by 2, and u acts as a 2-element on $\mathrm{supp}(u)$, there must be $h \in H$ with $S(h) \subseteq \mathrm{supp}(u)$ containing only one element. It follows that $(hu)^* = u^* h^{-1} = u^* xh = uh = hu$, and clearly $1 \in \mathrm{supp}(hu)$. □

We also give the proper generalization of Corollary 1.6 from [72] (note that there, the assumption that $\mathcal{N}_{\mathcal{U}_1}(G)$ is finitely generated is unnecessary).

19.3 Proposition. *Let G be a group so that $\mathcal{Z} := \mathrm{Z}(\mathrm{V}(RG))$ is finitely generated. Then $\mathrm{N}_{\mathrm{V}(RG)}(G)/\mathcal{Z}G$ is a finite abelian group, the rank of a Sylow p-subgroup being at most the torsion-free rank of $\mathcal{Z}$.*

Proof. Set $N = \mathrm{N}_{\mathrm{V}(RG)}(G)$ and $H = \mathcal{Z}G$. Then N/H is a periodic abelian group by Corollary 17.9 and Proposition 19.1. Let $X = \langle x_1, \dots, x_s\rangle \le N$ be such that $\bar{X} = XH/H$ is a p-group of rank s, and let r be the torsion-free rank of $\mathcal{Z}$. Then we have to show that $s \le r$.

First we will show that the natural map $X \to N/G$ is injective. Assume the contrary; then, as N/G is torsion-free abelian by Proposition 19.1, there are natural numbers $m_1, \dots, m_s$ such that

$$x = x_1^{m_1} \cdots x_s^{m_s} \in G. \tag{$*$}$$

In particular, $\bar{x} = 1$, so p divides all m_i. Let q be the highest power of p which divides all m_i, and set $n_i = m_i/q$. Then $y = x_1^{n_1} \cdots x_s^{n_s}$ has the property that $y^q \in G$ (bear in mind that N/G is abelian), so $y \in G$ by Corollary 18.6. But at least one n_i is not divisible by p, which means that $y \notin H$, and we have reached a contradiction.

We may assume that there are natural numbers a_i such that $x_i^{a_i} \in \mathcal{Z}$ for all i (this is clearly the case if the group generated by the support of x_i is a finite normal subgroup, and this can be assumed by Theorem 18.5). By the above, $Y = \langle x_1^{a_1}, \dots, x_s^{a_s}\rangle$ is a torsion-free abelian group of rank s. On the other hand, the rank of Y can not be strictly bigger than r, the torsion-free rank of $\mathcal{Z}$, since otherwise a relation of the form $(*)$ would hold. This proves the proposition. □

By the Ward–Coleman Lemma we will understand the very useful fact that for a finite group G with a p-subgroup P, and any commutative ring R with $pR \neq R$, we have

$$\mathrm{N}_{\mathrm{V}(RG)}(P) = \mathrm{N}_G(P)\mathrm{C}_{\mathrm{V}(RG)}(P).$$

Coleman's contribution [25] is well known, but the first version appears in an article of Ward [142] as a contribution to a seminar run by Richard Brauer at Harvard. In its present form, the lemma appears first in [124, Proposition 1.14], see also [66, 2.6 Theorem].

We shall need a version of the Ward–Coleman Lemma for infinite groups. The idea behind the proof is the same in both cases.

19.4 Lemma. *Let R be commutative ring with $pR \neq R$ for some rational prime p. Then for any $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ there is $g \in \mathrm{supp}(u)$ such that ug^{-1} centralizes a subgroup of G which is of finite p'-index in G.*

Proof. Let $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$. The group G acts on $\mathrm{supp}(u)$ via $x \overset{g}{\mapsto} g^{-1}xg^u$ for $x \in \mathrm{supp}(u)$ and $g \in G$, and elements of an orbit under this operation have the same coefficient in u (viewed as a linear combination of elements of G). Let Q be the kernel of this operation, and choose $Q \leq P \leq G$ such that P/Q is a Sylow p-subgroup of the (finite) group G/Q. Since the augmentation of u is a unit in R, there is a fixed point $x \in \mathrm{supp}(u)$ under the operation of P, that is, ux^{-1} centralizes P. □

This version of the Ward–Coleman Lemma is used to prove the key lemma of this section, which will then be applied to establish that $\mathrm{Out}_R(G) = 1$ for G belonging to certain classes of groups, extending (known) results for finite groups.

19.5 Lemma. *Let*

(i) *R be a commutative ring with $pR \neq R$, for some rational prime p;*

(ii) *N be a finite normal subgroup of a group G such that the center of a Sylow p-subgroup of N is contained in $\mathrm{O}_p(N)$;*

(iii) *$u \in \mathrm{N}_{\mathrm{Z}(\mathrm{U}(RN))}(G)$ be such that $\sigma = \mathrm{conj}(u) \in \mathrm{Aut}_R(G)$ is of p-power order.*

Then there is $g \in \mathrm{Z}(\mathrm{O}_p(N))$ such that $ug \in \mathrm{Z}(RG)$.

Proof. Clearly $[G, u] \leq N$, so $[[G, u], u] = 1$ and $[G, u]^{p^n} = [G, u^{p^n}] = 1$. Moreover, $[[G, u], N] = 1$ by the Three Subgroup Lemma. In particular, it follows that $[G, u] \leq A = \mathrm{Z}(\mathrm{O}_p(N))$. By Lemma 19.4, there is a subgroup P of G which is of finite p'-index in G, and $x \in \mathrm{supp}(u)$, such that $[P, ux^{-1}] = 1$. Since u is of p-power order over the center, and $[u, x] = 1$, there is $y \in \langle x \rangle$ of p-power order with $[P, uy^{-1}] = 1$. Let S be a Sylow p-subgroup of N. Then there is a fixed point under the multiplication action of S on the set of left cosets of P in G, say gP, and it follows that $[S^g, y^{-1}] = [S^g, uy^{-1}] \leq [P, uy^{-1}] = 1$.

Hence $y \in A$ by the hypothesis on N. Now $\sigma = \mathrm{conj}(uy^{-1})$ is an automorphism of G, which is of p-power order, induces the identity on both A and G/A, and fixes P element-wise. Using restriction-corestriction in 1-cohomology [65, I 16.18], it follows that $\sigma = \mathrm{conj}(a)$ for some $a \in A$. (Explicitly, $a = \left(\prod_{i=1}^{n} g_i^{-1}(g_i\tau)\right)^m$, where $g_1, \ldots, g_n$ is a system of right coset representatives of P in G, and $m \in \mathbb{N}$ is such that $nm \equiv 1 \bmod |A|$.) The proof is complete. □

As another application of that kind of reasoning, we prove the following proposition, which extends [93, Corollary 18], and also [72, Corollary 2.7], considerably.

19.6 Proposition. *Let R be a commutative ring with $pR \neq R$ for some rational prime p. If finite quotients of the commutator subgroup G' are p-groups, then $\mathrm{Out}_R(G) = 1$.*

Proof. Let $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$. By Lemma 19.4, there is a subgroup P of finite p'-index in G, and $x \in G$, such that $[P, ux] = 1$. Since G' acts on the set of right cosets of P in G as a finite p-group, it follows that $G' \leq P$. Let $\sigma = \mathrm{conj}(ux) \in \mathrm{Aut}(G)$. Then σ induces the identity on both G' and $G/\mathrm{Z}(G')$, and the same 1-cohomology argument as above shows that $\sigma \in \mathrm{Inn}(G)$. □

Note that there was no need to apply a "representation theorem", so the remark preceding [72, Corollary 2.7] doesn't make sense. We take the opportunity to point out that [72, Proposition 2.6] can also be proved without applying a "representation theorem":

19.7 Proposition. *Let G be a group which has a normal subgroup N so that $N \cap G' = 1$. If G/N has the normalizer property, then G has the normalizer property.*

Proof. Let $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$, and $g \in G$. By hypothesis, there is $x \in G$ such that ux maps to a central element under the natural map $RG \to RG/N$. It follows that $[ux, g]$, which is an element of G, is contained in N. On the other hand, since RG/G' is commutative, $[ux, g]$ maps to 1 under the natural map $RG \to RG/G'$, so $[ux, g] \in G'$. It follows that $[ux, g] \in N \cap G' = 1$, and since g was an arbitrary element of G, the proposition is proved. □

19.8 Proposition. *Let G be a group whose finite normal subgroups N satisfy $N \cap G' = 1$. Then G has the normalizer property.*

Proof. Let $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$. By Theorem 17.8, there is a finite normal subgroup N of G and $x \in G$ such that $[G, ux] \leq N$, and $[G, ux] \leq G'$ by Theorem 17.3. Hence $[G, ux] = 1$ by assumption and the proposition is proved. □

Note that the last proposition holds for any commutative coefficient ring R.

Jackowski and Marciniak proved that $\mathrm{Out}_{\mathbb{Z}}(G) = 1$ for a finite group G with a normal Sylow 2-subgroup [66, Theorem 3.6]. In [61], it is shown that this is a special case of a much more general result. Here, we shall need the following proposition.

19.9 Proposition. *Let G be a finite group which has a normal Sylow p-subgroup, and let R be a commutative ring with $pR \neq R$. If $\sigma \in \mathrm{Aut}_R(G)$ has p-power order, then $\sigma = \mathrm{conj}(g)$ for some $g \in \mathrm{O}_p(G)$.*

Proof. Let $\sigma \in \mathrm{Aut}_R(G)$ be of p-power order, and put $N = \mathrm{O}_p(G)$. As G/N is a p'-group, σ induces the identity on G/N (see [65, Kap. I, § 4, Aufg. 14]). By the Ward–Coleman Lemma, there is $g \in G$ such that $\sigma|_N = \mathrm{conj}(g)|_N$, and clearly g can be chosen to be a p-element. But then $\mathrm{conj}(g^{-1})\sigma$ fixes N element-wise, and is therefore an inner automorphism, given by conjugation with an element from $\mathrm{Z}(N)$. □

19.10 Corollary. *Let p be a rational prime, and let G be a group whose finite normal subgroups have a normal Sylow p-subgroup. Let R be a $\Delta^+(G)$-adapted ring. Then $\mathrm{Out}_R(G)$ has no p-torsion.*

Proof. Let $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ and put $\sigma = \mathrm{conj}(u) \in \mathrm{Aut}_R(G)$. By the way of contradiction, assume that $\sigma \notin \mathrm{Inn}(G)$, but that the image of σ in $\mathrm{Out}_R(G)$ has p-power order. Take $g \in \mathrm{supp}(u)$; then $N = \langle \mathrm{supp}(ug^{-1}) \rangle$ is a finite normal subgroup of G by Theorem 18.5. Consequently, $\tau = \mathrm{conj}(ug^{-1}) \in \mathrm{Aut}(G)$ is of finite order, and there is $n \in \mathbb{N}$, not divisible by p, such that τ^n has p-power order. Note that $p \in \pi(\Delta^+(G))$ by Corollary 18.7, so Proposition 19.9 can be applied to give $h \in \mathrm{O}_p(N)$ with $v = (ug^{-1})^n h \in \mathrm{Z}(RN)$, and $\mathrm{conj}(v) \in \mathrm{Aut}(G)$ has p-power order. Hence $\sigma^n \in \mathrm{Inn}(G)$ by Lemma 19.5, a contradiction. □

Note that the hypothesis of the corollary is particularly satisfied if the set of p-torsion elements of G form a normal subgroup of G.

Since $\mathrm{Out}_{\mathbb{Z}}(G)$ is of exponent 2, it follows that the Jackowski-Marciniak result extends to infinite groups.

19.11 Corollary. *Let G be a group whose finite normal subgroups have a normal Sylow 2-subgroup. Then $\mathrm{Out}_{\mathbb{Z}}(G) = 1$.* □

Now we turn to the obvious class of groups to which Lemma 19.5 applies.

19.12 Corollary. *Let G be a group whose finite normal subgroups are nilpotent, and R a $\Delta^+(G)$-adapted ring. Then $\mathrm{Out}_R(G) = 1$. More precisely, if $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ with $1 \in \mathrm{supp}(u)$, then $N = \langle \mathrm{supp}(u) \rangle$ is a finite normal subgroup of G, and there is $g \in N$ such that $ug \in \mathrm{Z}(RG)$.*

Proof. Let $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ with $1 \in \mathrm{supp}(u)$. Then $N = \langle \mathrm{supp}(u) \rangle$ is a finite normal subgroup of G by Theorem 18.5, and by the Ward–Coleman Lemma, there is $x \in N$ such that $v = ux \in \mathrm{Z}(RN)$. The automorphism $\sigma = \mathrm{conj}(v) \in \mathrm{Aut}(G)$ is of finite order; assume that σ^n ($n \in \mathbb{N}$) is of p-power order, for some rational prime p. Obviously, it suffices to show that there is $h \in N$ such that $v^n h \in \mathrm{Z}(RG)$. But this follows from Lemma 19.5. □

In particular, $\mathrm{Out}_{\mathbb{Z}}(G) = 1$ for p-groups and locally nilpotent groups G, extending the well known finite group case (Ward–Coleman Lemma). Also note that hypercentral groups, that is, groups which coincide with the terminal member of its (transfinite) upper central series, are locally nilpotent (see [77, 1.B.2 Lemma]).

A somewhat weaker version of the next corollary, which follows immediately from Corollary 19.12, has been obtained for finitely generated nilpotent groups in [74, Proposition 3] (note that in the decomposition given here, $g \in G$ actually can be chosen to lie in $\mathrm{Z}(G)$), and for locally nilpotent groups in [72, Theorem 2.4].

19.13 Corollary. *Let G be a nilpotent group, and R a $\Delta^+(G)$-adapted ring. Then $\mathrm{Out}_R(G) = 1$. For any central unit u in RG, there is $g \in \mathrm{Z}(G)$ such that ug is a unit in RN, for some finite normal subgroup N of G.* □

An observation of Gross [44, Corollary 2.4] combined with the Ward–Coleman Lemma immediately implies the following proposition (cf. also [61, Proposition 4]).

19.14 Proposition. *Let G be a finite group which has a normal p-subgroup containing its own centralizer in G, and let R be a commutative ring with $pR \neq R$. Then $\mathrm{Out}_R(G) = 1$.* □

This result extends to arbitrary groups in the following way.

19.15 Corollary. *Let G be a group whose finite normal subgroups satisfy the hypothesis of Proposition 19.14, and let R be a $\Delta^+(G)$-adapted ring. Then $\mathrm{Out}_R(G) = 1$.*

Proof. Let $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ such that $1 \in \mathrm{supp}(u)$. Then $N = \langle \mathrm{supp}(u) \rangle$ is a finite normal subgroup of G by Theorem 18.5. By hypothesis, $\mathrm{C}_N(\mathrm{O}_p(N)) \leq \mathrm{O}_p(N)$ for some rational prime p. By Proposition 19.14, there is $g \in N$ such that $ug \in \mathrm{Z}(RN)$. Note that $\mathrm{conj}(ug)$ induces the identity on $G/\mathrm{Z}(N)$, and that $\mathrm{Z}(N) \leq \mathrm{O}_p(N)$. It follows that $\mathrm{conj}(ug)$ is of p-power order, and since N satisfies the hypothesis (ii) of Lemma 19.5, the result follows from this lemma. □

If finite normal subgroups of G are either as in Lemma 19.5, or are center-less and have the normalizer property, then G too will have the normalizer property. We content ourselves with a typical example. The result also appeared in an earlier version of [72], but we feel that our proof is more conceptually.

We first demonstrate that finite Frobenius groups have the normalizer property. Restricting to the rational integers $\mathbb{Z}$ as coefficient ring only, this is the content of a paper by Lobão and Milies [102], but the proof given there does not generalize to the case of G-adapted coefficient rings. (We also remark that our proof is considerably shorter.)

19.16 Proposition. *Let G be a finite Frobenius group, and R a G-adapted ring. Then $\mathrm{Out}_R(G) = 1$.*

Proof. If the Fitting subgroup $\mathrm{F}(G)$ of G is a p-group, Proposition 19.14 shows that $\mathrm{Out}_R(G) = 1$. Hence we may assume that $\mathrm{F}(G) = A \times B$ for nontrivial normal subgroups A, B of G. Let $\sigma \in \mathrm{Aut}_R(G)$. Proceeding by induction on the order of G, we may assume that σ induces the identity on G/A, and that there is $x \in G$ such that $g^x \in gB$ for all $g \in G$. Then $\sigma|_A = \mathrm{conj}(x)|_A$ and $\sigma|_B = \mathrm{id}|_B$. Choose $a \in A \setminus \{1\}$ and $b \in B \setminus \{1\}$. Since $\sigma \in \mathrm{Aut}_{\mathrm{c}}(G)$, there is $g \in G$ such that $a^x b = (ab)\sigma = a^g b^g$. This means that $[b, g] = 1$ and $[a, xg^{-1}] = 1$, so $x = xg^{-1} \cdot g \in \mathrm{F}(G)$ as G is a Frobenius group. Hence there is $y \in \mathrm{F}(G)$ with $\sigma|_{AB} = \mathrm{conj}(y)|_{AB}$. As $\mathrm{C}_G(\mathrm{F}(G)) \leq \mathrm{F}(G)$, $\mathrm{conj}(y^{-1})\sigma$ induces the identity on both $\mathrm{F}(G)$ and $G/\mathrm{F}(G)$. Since these groups have coprime orders, the usual 1-cohomology argument shows that $\sigma \in \mathrm{Inn}(G)$. □

19.17 Corollary. *Let G be a locally finite Frobenius group, and R a $\Delta^+(G)$-adapted ring. Then $\mathrm{Out}_R(G) = 1$.*

Proof. Let $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$; then we have to show that $u \in \mathrm{Z}(RG)G$. We may assume that $1 \in \mathrm{supp}(u)$. Then $N = \langle \mathrm{supp}(u) \rangle$ is a finite normal subgroup of G by Theorem 18.5, and $N \leq F \leq G$ for some finite Frobenius group F. Hence N is either nilpotent or a Frobenius group. In the first case, $u \in \mathrm{Z}(RG)G$ follows as in the proof of Corollary 19.12. If N is a Frobenius group, we may assume that $u \in \mathrm{Z}(RN)$ by Proposition 19.16. But then $\mathrm{conj}(u)$ induces the identity on both N and G/N, so $u \in \mathrm{Z}(RG)$ as $\mathrm{Z}(N) = 1$. □

20. Trivial central units

It should be noted that analyzing $\mathrm{Out}_R(G)$ means that one studies specific central units. Indeed, let $\sigma \in \mathrm{Aut}_R(G)$, and let $\langle c \rangle$ be a cyclic group of the same order as σ. Form the semidirect product $H = G \rtimes \langle c \rangle$, where c is acting via σ, that is, $g^c = g\sigma$ for all $g \in G$. If σ is given by conjugation with $u \in \mathrm{U}(RG)$, then $uc^{-1} \in \mathrm{Z}(RH)$.

In this section, we apply the results of Section 18 to obtain a criterion (in terms of the finite normal subgroups of G) for when RG has "only trivial central units" (see Sehgal's Problem 26 in [129]), and show that this notion is really independent from the underlying group basis. Note that the finite group case has been settled by Ritter and Sehgal (see [129, Theorem (6.1)]).

The next two corollaries are essentially [72, Corollary 1.7] for a more general coefficient ring. The first observation is that RG has "only trivial central units" if and only if additionally G has the normalizer property.

20.1 Corollary. *Let R be a $\Delta^+(G)$-adapted ring. Then $\mathrm{Z}(\mathrm{V}(RG)) = \mathrm{Z}(G)$ if and only if $\mathrm{N}_{\mathrm{U}(RG)}(G) = G$.*

Proof. One implication is obvious. For the converse, assume that $\mathrm{Z}(\mathrm{V}(RG)) = \mathrm{Z}(G)$ and let $u \in \mathrm{N}_{\mathrm{U}(RG)}(G)$ such that $1 \in \mathrm{supp}(u)$; we have to show that $u \in G$. By Theorem 18.5,

$N = \langle \mathrm{supp}(u) \rangle$ is a finite normal subgroup of G, so $u^n \in \mathrm{Z}(\mathrm{V}(RG)) \cap RN \leq N$ for some $n \in \mathbb{N}$, and the result follows from Corollary 18.6. □

The next corollary tells us that all central units of RG are trivial provided that each central unit which is contained in RN for some finite normal subgroup N of G is trivial. We remark that a special case thereof has already been given in [69, Corollary 2.2].

20.2 Corollary. *Let R be a $\Delta^+(G)$-adapted ring. Assume that $\mathrm{Z}(\mathrm{V}(RG)) \cap RN \subseteq G$ for each finite normal subgroup N of G. Then $\mathrm{Z}(\mathrm{V}(RG)) = \mathrm{Z}(G)$.*

Proof. Let $z \in \mathrm{Z}(\mathrm{V}(RG))$, and take any $g \in \mathrm{supp}(z)$. Put $u = zg^{-1}$, and $N = \langle \mathrm{supp}(u) \rangle$, a finite normal subgroup by Theorem 18.5. Take $n \in \mathbb{N}$ such that $[N, g^n] = 1$, and put $m = n|N|$. Then $g^m \in \mathrm{Z}(G)$ since g maps to a central element in RG/N. It follows that $u^m \in \mathrm{Z}(RG)$, so $u^m \in N$ by assumption, and $z = ug \in G$ by Corollary 18.6. □

If R is an integral domain of characteristic zero in which no rational prime is invertible, then the phrase "RG possesses only trivial central units" is justified, as it is independent from the underlying group basis. More precisely, we use a result of Burn [23] on the support group of central idempotents to prove the following proposition. Let $\widehat{X}$ denote the sum of the elements of a set X.

20.3 Proposition. *Let R be a $\Delta^+(G)$-adapted ring, and suppose that $\mathrm{Z}(\mathrm{V}(RG)) = \mathrm{Z}(G)$. If H is a group basis of RG such that R is $\Delta^+(H)$-adapted, then $\mathrm{Z}(\mathrm{V}(RH)) = \mathrm{Z}(H)$.*

Proof. Let M be a finite normal subgroup of H, and $z \in \mathrm{Z}(\mathrm{V}(RG)) \cap RM$. Write $\widehat{M} = \sum_{g \in G} a_g g$ with $a_g \in R$ for $g \in G$. Since $\frac{1}{|M|}\widehat{M}$ is a central idempotent, $N = \langle g : a_g \neq 0 \rangle$ is a finite normal subgroup of G by [23]. Since $0 = \widehat{M}(z-1) = (\sum_{g \in N} a_g g)(z-1)$ and $z \in G$, it follows that $z \in N$. Hence z is of finite order, and $z \in H$ by Corollary 18.6. Now it follows from Corollary 20.2 that $\mathrm{Z}(\mathrm{V}(RH)) = \mathrm{Z}(H)$, which completes the proof. □

We finish this section with another application of Burn's result [23]. Let R be a commutative ring, and $N \trianglelefteq G$. We denote the kernel of the natural map $RG \to RG/N$ by $\mathrm{I}_R(N)G$. Note that if N is finite, then $\mathrm{I}_R(N)G = \mathrm{Ann}_{RG}(\widehat{N})$ and $\mathrm{Ann}_{RG}(\mathrm{I}_R(N)G) = (RG)\widehat{N}$ (see [130, III, Proposition 4.18]), where $\mathrm{Ann}_{RG}(S) = \{x \in RG \mid Sx = 0\}$ denotes the (right) annihilator of $S \subseteq RG$ in RG.

20.4 Lemma. *Let R be an integral domain of characteristic zero, and H a group basis of RG. Then for any finite normal subgroup N of G, there is a finite normal subgroup M of H such that $\mathrm{Ann}_{RG}(\widehat{N}) \subseteq \mathrm{Ann}_{RG}(\widehat{M})$.*

Proof. Let N be a finite normal subgroup of G, and write $\widehat{N} = \sum_{h\in H} a_h h$ with $a_h \in R$ for $h \in H$. Taking augmentation we see that $\sum_{h\in H} a_h = |N|$. Since $\frac{1}{|N|}\widehat{N}$ is a central idempotent, $M = \langle h : a_h \neq 0\rangle$ is a finite normal subgroup of H by [23]. Let $x \in \mathrm{Ann}_{RG}(\widehat{N})$. Multiplying the equation $0 = \widehat{N}x = (\sum_{h\in M} a_h h)x$ with $\widehat{M}$, we get $0 = (\sum_{h\in M} a_h)\widehat{M}x = |N|\widehat{M}x$, and consequently $x \in \mathrm{Ann}_{RG}(\widehat{M})$. □

20.5 Lemma. *Let R be a $\Delta^+(G)$-adapted ring. If H is another group basis of RG such that R is also a $\Delta^+(H)$-adapted ring, then $\pi(\Delta^+(G)) = \pi(\Delta^+(H))$, and $\mathrm{I}_R(\Delta^+(G))G = \mathrm{I}_R(\Delta^+(H))H$.*

Proof. Let N be a finite normal subgroup of G. By Lemma 20.4, there are finite normal subgroups M of H and L of G such that $\mathrm{Ann}_{RG}(\widehat{N}) \subseteq \mathrm{Ann}_{RG}(\widehat{M}) \subseteq \mathrm{Ann}_{RG}(\widehat{L})$. Equivalently, $(RG)\widehat{N} \supseteq (RG)\widehat{M} \supseteq (RG)\widehat{L}$, so $\widehat{M} = x\widehat{N}$ and $\widehat{L} = y\widehat{M}$ for some $x, y \in RG$, and taking augmentation shows that $|M| \in |N|R$ and $|L| \in |M|R$. As R is $\Delta^+(G)$- and $\Delta^+(H)$-adapted, it follows that $|N|$ divides $|M|$ and $|M|$ divides $|L|$. Since $\Delta^+(G)$ is the union of the finite normal subgroups of G (see [100, PART 2, §4 Lemma 1.8]), this shows that $\pi(\Delta^+(G)) \subseteq \pi(\Delta^+(H)) \subseteq \pi(\Delta^+(G))$. Finally, $\mathrm{I}_R(\Delta^+(G))G = \bigcup_N \mathrm{Ann}_{RG}(\widehat{N})$, the union over all finite normal subgroups N of G, and likewise for H, and it follows that $\mathrm{I}_R(\Delta^+(G))G = \mathrm{I}_R(\Delta^+(H))H$. □

Note that the above lemma does not follow from the subgroup correspondence for finite normal subgroups (see [130, III.4.17]), for this is based on a theorem of Bass [130, II.1.2], which is not known to hold for G-adapted rings (see Sehgal's Problem 3 in [129]).

The last corollary answers a question of Mazur [92, p. 438].

20.6 Corollary. *Assume that G is a FC-group, and let R be a G-adapted ring. Then any group basis of RG is also a FC-group.*

Proof. Let H be a group basis of RG, and $h \in H$. By Lemma 20.5, $RG/\Delta^+(G) = RH/\Delta^+(H)$, and since $G/\Delta^+(G)$ is torsion-free abelian, $RG/\Delta^+(G)$ has only trivial units (see [100, PART 2, §4 Lemma 1.6, PART 13, §1]). Hence there is $z \in \mathrm{Z}(RH)$ whose image in $RH/\Delta^+(H)$ is a multiple of the image of h, which implies that z has, with respect to the group basis H, an element hk ($k \in \Delta^+(H)$) in its support. It follows that $hk \in \Delta(H)$, and $h \in \Delta(H)$. □

VI. Hypercentral units in integral group rings

Eigentlich ist schon alles gesagt worden.
Aber noch nicht von allen.

Karl Valentin

For a group H, let $\mathrm{Z}_\infty(H)$ be the union of the terms $\mathrm{Z}_n(H)$ of the upper central series of H. Let $\mathcal{U}$ be the group of units of a group ring RG, where G is a periodic group, and R a G-adapted ring. We show that $\mathrm{Z}_\infty(\mathcal{U}) \leq \mathrm{Z}(\mathcal{U})\mathrm{Z}_2(G)$. If $\mathrm{Z}_\infty(\mathcal{U}) \neq \mathrm{Z}(\mathcal{U})$, then the structure of G is similar to that of the quaternion group (G is a so-called Q*-group). This work continues research initiated by Arora, Hales and Passi. As a consequence, we obtain an explicit description of $\mathrm{Z}_\infty(\mathcal{U})$ in the case $R = \mathbb{Z}$, a result which was obtained independently by Li and Parmenter [87].

21. Hypercentral units and Q*-groups

For a group G, and a commutative ring R, let $\mathrm{U}(RG)$ be the group of units in the group ring RG. The subject of this chapter is, under certain restrictions on G and R, the hypercenter of $\mathrm{U}(RG)$. For a finite group G, the hypercenter of $\mathrm{U}(\mathbb{Z}G)$ has already been studied by Arora, Hales and Passi [3,4], and their results have been generalized to periodic groups by Li and Parmenter [86,87]. We shall also deal with a periodic group G, but more generally with a *G-adapted ring* R, that is, an integral domain of characteristic zero such that if G has an element of order p, then p is not invertible in R.

Let us introduce the following notation. For a group H, let $\mathrm{Z}_n(H)$ be the n-th term of the upper central series (so that $\mathrm{Z}_1(H) = \mathrm{Z}(H)$ is the center of H), and set $\mathrm{Z}_\infty(H) = \bigcup_{n=1}^{\infty} \mathrm{Z}_n(H)$. If the upper central series $1 \leq \mathrm{Z}_1(H) \leq \mathrm{Z}_2(H) \leq \ldots$ of H terminates, then $\mathrm{Z}_\infty(H)$ coincides with the *hypercenter* of H, which is the terminal member of the transfinitely extended upper central series of H.

Next we define a class of groups which will play a special role in our investigations.

21.1 Definition. We say that the group G is a *Q-group* if G has an abelian subgroup A of index 2 which is not elementary abelian, and $G = \langle A, b\rangle$ for some $b \in G$ of order 4

with $x^b = x^{-1}$ for all $x \in A$. If in addition there is $a \in A$ with $a^2 = b^2$, then G is said to be a *Q^*-group*.

The term "Q-group" has been introduced by Blackburn in [11], and the term "Q*-group" has been used by Arora and Passi [4]. Q*-groups appear, possibly for the first time, in the paper [16] of Bovdi, who proved that if a group G has a non-central periodic subgroup which is normal in $\mathrm{U}(\mathbb{Z}G)$, then G is a Q*-group. Williamsen [146] showed that Q*-groups are exactly those groups containing a non-central element a which has finitely many conjugates in $\mathrm{U}(\mathbb{Z}G)$. An elementary approach was given by Parmenter [98], who showed that some weaker condition also characterizes these groups. (We will encounter finite conjugacy again in Chapter VII.)

Our results on hypercentral units (elements of the hypercenter of the group of units) can be summarized as follows.

21.2 Theorem. *Let G be a periodic group, and R a G-adapted ring. Then the following hold for $\mathcal{U} = \mathrm{U}(RG)$.*

1. $\mathrm{Z}_\infty(\mathcal{U}) = \mathrm{Z}_2(\mathcal{U}) \le \mathrm{Z}(\mathcal{U})\mathrm{Z}_2(G)$;
2. *If $\mathrm{Z}_2(\mathcal{U}) \ne \mathrm{Z}(\mathcal{U})$, then G is a Q^*-group;*
3. *If $R = \mathbb{Z}$, then exactly one of the following holds:*
   (a) $\mathrm{Z}_\infty(\mathcal{U}) = \mathrm{Z}(\mathcal{U})$;
   (b) *G is a Hamiltonian 2-group and $\mathrm{Z}_\infty(\mathcal{U}) = \mathrm{Z}(\mathcal{U})G$;*
   (c) *G is a Q^*-group, and $\mathrm{Z}_\infty(\mathcal{U}) = \mathrm{Z}(\mathcal{U})\langle g \in A \mid g^2 = a^2\rangle$ with notation as in Definition 21.1.*

Parts of the theorem have already been proved by other authors, and a few comments on their work seem to be appropriate. Let G be a group, and set $\mathcal{U} = \mathrm{U}(\mathbb{Z}G)$. Recall that Bovdi [16] described the periodic subgroups of $\mathcal{U}$ which are normal in $\mathcal{U}$. In particular, he showed that they are contained in G, and that G is a Q*-group whenever a non-central periodic subgroup of G is normal in $\mathcal{U}$.

Now let G be finite. Arora, Hales and Passi [3] studied the multiplicative Jordan decomposition for elements of $\mathcal{U}$. They noted that $[\mathrm{Z}_2(\mathcal{U}),\mathcal{U}] \le \mathrm{Z}(G)$, and that this implies that $\mathrm{Z}_\infty(\mathcal{U})/\mathrm{Z}(\mathcal{U})$ is a periodic group since $\mathrm{Z}(G)$ is finite. Thus $\mathrm{Z}_\infty(\mathcal{U})$ consists of semisimple elements, and an inductive argument then shows that elements of $\mathrm{Z}_\infty(\mathcal{U})$ commute with all unipotent elements. These observations, together with Bovdi's results, led them to the conclusion that $\mathrm{Z}_\infty(\mathcal{U}) = \mathrm{Z}_2(\mathcal{U})$. They also noted that the torsion elements of $\mathrm{Z}_\infty(\mathcal{U})$ are contained in $\mathrm{Z}_2(G)$ since they form a periodic normal subgroup of $\mathcal{U}$. Then, Arora and Passi [4] proved that $\mathrm{Z}_2(\mathcal{U}) = \mathrm{Z}(\mathcal{U})T$, where T denotes the torsion subgroup of $\mathrm{Z}_2(\mathcal{U})$. This result relies on Blackburn's classification [11] of the finite groups in which the non-normal subgroups have nontrivial intersection.

For a periodic group G, Li [86] proved that $\mathrm{Z}_\infty(\mathcal{U}) = \mathrm{Z}_2(\mathcal{U})$. Note, however, that the proof heavily relies on the fact that the coefficient ring is $\mathbb{Z}$, since a result of Krempa (see [66, 3.2. Theorem]) is used to show that $\mathrm{Z}_2(\mathcal{U})/\mathrm{Z}(\mathcal{U})$ has exponent 2 (and so $\mathrm{Z}_\infty(\mathcal{U})/\mathrm{Z}(\mathcal{U})$ is a periodic group). Then, the proof is completed along general lines as in [3]. For a periodic group G, the question remained whether $\mathrm{Z}_2(\mathcal{U}) = \mathrm{Z}(\mathcal{U})T$, where T denotes the torsion subgroup of $\mathrm{Z}_2(\mathcal{U})$. This was stated by Parmenter as Open Problem 5 in [99] (see also [88, p. 4219]) and was, finally, affirmatively answered by Li and Parmenter [87]. However, they do not use Blackburn's classification [11] any longer. Instead, they make use of Bass cyclic, bicyclic and Hoechsmann units in integral group rings. In contrast to this approach, we still use Blackburn's classification, but do not make any use of particular units in group rings. Again, the Li-Parmenter proof heavily relies on the fact that the coefficient ring is $\mathbb{Z}$, as becomes apparent from the proof of [87, Lemma 1]. The (nontrivial) generalization of this lemma is given in Proposition 23.3.

There is an obvious connection with what has become known as the "normalizer problem". Let $\mathrm{N}_\mathcal{U}(G)$ be the normalizer of G in $\mathcal{U}$. Then the observation from [3] that $[\mathrm{Z}_2(\mathcal{U}), G] \leq \mathrm{Z}(G)$ (which readily extends to periodic groups, see [86, Lemma 1]) implies that $\mathrm{Z}_2(\mathcal{U}) \leq \mathrm{N}_\mathcal{U}(G)$. The group G is said to have the normalizer property if $\mathrm{N}_\mathcal{U}(G) = \mathrm{Z}(\mathcal{U})G$, and this in turn implies that $\mathrm{Z}_2(\mathcal{U}) = \mathrm{Z}(\mathcal{U})T$. Any $u \in \mathrm{N}_\mathcal{U}(G)$ defines an automorphism $\mathrm{conj}(u) : g \mapsto g^u$ of G, and $\mathrm{conj}(u)$ is contained in $\mathrm{Aut}_\mathrm{c}(G)$, the group of class-preserving automorphisms of G (this is well known if G is finite, and stated for arbitrary G in Theorem 17.3). Thus a group G has the normalizer property once the stronger property $\mathrm{Aut}_\mathrm{c}(G) = \mathrm{Inn}(G)$ is established. This is done in Section 22 for the groups from Blackburn's list [11] (one might wish to compare this approach with the strategy pursued in [88]).

As already mentioned, we shall also deal with a periodic group G, but more generally with a G-adapted coefficient ring R. This seems to be justified since many results which hold for $\mathrm{U}(\mathbb{Z}G)$ generalize to results for $\mathrm{U}(RG)$, giving at the same time more insight into the structure of the unit groups. (However, it should be noted that such generalizations are sometimes very difficult to find.) The main results are already contained in Section 23. We believe that the achieved results are definitive, and have tried to keep the exposition as self-contained as possible. This applies in particular to Section 24, where short proofs of some of Bovdi's results are given. In Section 25, applications of Bovdi's work to hypercentral units are discussed.

22. Groups with nontrivial intersection of their non-normal subgroups

A group G is called a *Dedekind group* if any subgroup of G is normal in G. Such a group is abelian or the direct product of the quaternion group of order 8, an elementary abelian 2-group and an abelian group with all its elements of odd order (see [113, 5.3.7]). A

non-abelian Dedekind group is called *Hamiltonian*. If G is not a Dedekind group, then, following [11], we denote by $\mathrm{R}(G)$ the intersection of all non-normal subgroups of G. The following simple observation is quite useful for the determination of $\mathrm{R}(G)$.

22.1 Lemma. *If G is not a Dedekind group then $\mathrm{R}(G)$ is the intersection of all non-normal cyclic subgroups of G (in particular, $\mathrm{R}(G)$ is cyclic). If $\mathrm{R}(G)$ is finite, it is the intersection of all non-normal cyclic subgroups of prime-power order of G.*

Proof. Let $\mathcal{S}$ be the set of all non-normal subgroups of G, and $\mathcal{C}$ be the set of all non-normal cyclic subgroups of G. Clearly $\mathrm{R}(G) = \bigcap_{S\in\mathcal{S}} S \le \bigcap_{C\in\mathcal{C}} C$. Take any $x \in \bigcap_{C\in\mathcal{C}} C$ and $S \in \mathcal{S}$. We wish to show that $x \in S$. Assume the contrary. Then $x \notin \langle g\rangle$ for all $g \in S$, so all cyclic subgroups of S are normal in G, and we obtain the contradiction $S \trianglelefteq G$. Now assume that $\mathrm{R}(G)$ is finite. Let $x \in G$ be contained in all non-normal cyclic subgroups of prime-power order of G, and let $C \in \mathcal{C}$. Then there is a Sylow subgroup P of C which is not normal in G, so $x \in P \subseteq C$, which proves the supplement. □

It should be obvious that the condition $\mathrm{R}(G) \neq 1$ severely restricts the structure of G. The finite groups G for which $\mathrm{R}(G) \neq 1$ have been determined by Blackburn [11]. For convenience of the reader, we give the complete list. We do not quote literally, but it should be unproblematic for the reader to identify both lists.

We write $\mathrm{Q}_{2^n} = \langle s, t : s^{2^{n-1}} = 1, t^2 = s^{2^{n-2}}, s^t = s^{-1}\rangle$ for the generalized quaternion group of order 2^n, $n \ge 3$, and E_2 denotes an elementary abelian 2-group of finite order.

22.2 Theorem (Blackburn). *Suppose that the finite group G is not a Dedekind group and that $\mathrm{R}(G) \neq 1$.*

If G is a p-group, then $p = 2$ and one of the following holds.

(1) $G \cong \mathrm{Q}_8 \times C_4 \times \mathrm{E}_2$.

(2) $G \cong \mathrm{Q}_8 \times \mathrm{Q}_8 \times \mathrm{E}_2$.

(3) *G is a Q-group (see Definition 21.1).*

If G is not of prime-power order, then one of the following holds.

(a) *$G = N \rtimes \langle b\rangle$ with a p-element b and an abelian p'-group N. There is $m \in \mathbb{N}$ such that $x^b = x^m$ for all $x \in N$, and $1 \neq \mathrm{C}_{\langle b\rangle}(N) \neq \langle b\rangle$.*

(b) *$G = N \times H$ with N abelian of odd order and H of the kind described in (1) or (2).*

(c) *$G \cong N \rtimes \mathrm{Q}_{2^n}$ with N abelian of odd order, and $x^s = x^{-1}$, $x^t = x$ for all $x \in N$.*

(d) *$G = N \rtimes H$, where N is abelian of odd order, and the 2-group H is a Q-group. If $H = \langle A, b\rangle$ as in Definition 21.1, then $[N, A] = 1$ and b acts either trivially or by inversion on every Sylow subgroup of N.*

(e) *$G \cong H \times \mathrm{Q}_8 \times \mathrm{E}_2$, where H is of odd order and is of the kind described in (a).*

It would be interesting to know whether a similar result holds for periodic groups; some arguments from [11] certainly carries over to this more general situation.

Note that a class-preserving automorphism stabilizes every normal subgroup, and that $\mathrm{Aut}_c(-)$ commutes with taking direct products. We shall show that for G as in Theorem 22.2, $\mathrm{Aut}_c(G)$ consists of the inner automorphisms only. We begin with the following lemma (which implies [88, Theorem 2]). (A more general version is given in Proposition 14.4.)

22.3 Lemma. *Assume that a group G has an abelian normal subgroup of index 2 in G. Then $\mathrm{Out}_c(G) = 1$.*

Proof. Let $G = \langle A, g\rangle$, where A is an abelian normal subgroup of index 2 in G and $g \in G$, and take any $\sigma \in \mathrm{Aut}_c(G)$. We have to show that $\sigma \in \mathrm{Inn}(G)$, and we may assume without lost of generality that $g\sigma = g$. Note that for all $a \in A$, either $a\sigma = a$ or $a\sigma = a^g$. Choose $x \in A$ with $x \neq x\sigma = x^g$ (otherwise $\sigma = \mathrm{id}$, and we are done). Assume that there is $a \in A$ with $a\sigma \neq a^g$. In follows that $a\sigma = a$ and $x^g a = x^g(a\sigma) = (xa)\sigma$, so $x^g a$ is equal to xa or to $(xa)^g$. However, the first possibility contradicts $x^g \neq x$ and the second contradicts $a \neq a^g$. Hence $a\sigma = a^g$ for all $a \in A$, and $\sigma = \mathrm{conj}(g)$. □

Note that the next proposition improves [88, Theorem 1].

22.4 Proposition. *Suppose that the finite group G is not a Dedekind group and that $\mathrm{R}(G) \neq 1$. Then $\mathrm{R}(G) \leq \mathrm{Z}(G)$ and $\mathrm{Out}_c(G) = 1$.*

Proof. If G is of type (1) or (2), then $\mathrm{R}(G)$ is the diagonally embedded C_2 of $\mathrm{Q}_8 \times C_4$ or $\mathrm{Q}_8 \times \mathrm{Q}_8$, respectively. If G is a Q-group, say $G = \langle A, b\rangle$ as in Definition 21.1, then $\mathrm{R}(G) = \langle b^2\rangle$. In case (a), $\mathrm{R}(G) = \mathrm{C}_{\langle b\rangle}(N)$. For G as in (b), (d) or (e), $\mathrm{R}(G) = \mathrm{R}(H)$. In case (c), $\mathrm{R}(G) = \langle t^2\rangle$. In particular, $\mathrm{R}(G) \leq \mathrm{Z}(G)$ in all cases.

If G is of type (1), (2), (3) or (d), then $\mathrm{Out}_c(G) = 1$ by Lemma 22.3. It follows that $\mathrm{Out}_c(G) = 1$ for G of type (b). Assume that G is of type (a), and let $\sigma \in \mathrm{Aut}_c(G)$; we wish to show that $\sigma \in \mathrm{Inn}(G)$. Without lost of generality, we may assume that $b\sigma = b$. Note that σ maps each subgroup of N into itself. By a result of Levi (see [26, Theorem 3.4.1]), it follows that there is $l \in \mathbb{N}$ such that $g\sigma^{-1} = g^l$ for all $g \in N$. Take $x \in N$ of maximal order, and $n \in \mathbb{N}$ such that $x\sigma = x^{b^n}$. Then the automorphism $\mathrm{conj}(b^n)\sigma^{-1} : g \mapsto g^{m^n l}$ of N is of p-power order, and fixes a nontrivial element of each Sylow subgroup of the abelian p'-group N. It follows that $\sigma = \mathrm{conj}(b^n) \in \mathrm{Inn}(G)$. Hence $\mathrm{Out}_c(G) = 1$ for G of type (a), and it follows that the same is true for G of type (e). Let G be of type (c), and let $\sigma \in \mathrm{Aut}_c(G)$. In order to show that $\sigma \in \mathrm{Inn}(G)$, we may assume without lost of generality that $\sigma|_N = \mathrm{id}|_N$ and $\sigma|_{\mathrm{Q}_{2^n}} = \mathrm{conj}(g)$ for some $g \in \mathrm{Q}_{2^n}$. Take any $x \in N \setminus \{1\}$. Then $(xt)\sigma = (xt)^u$ for some $u \in \langle s\rangle$ since $[N, t] = 1$. This means that $x = x\sigma = x^u$ and $t^g = t^u$. It follows that $u \in \langle s^2\rangle$, and $g \in \mathrm{C}_{\mathrm{Q}_{2^n}}(t)\langle s^2\rangle = \langle t, s^2\rangle = \mathrm{C}_{\mathrm{Q}_{2^n}}(N)$, so $\sigma = \mathrm{conj}(g)$. The proof is complete. □

23. The hypercenter and unipotent elements

In the next three sections, G will always denote an arbitrary periodic group, unless stated otherwise, and R will denote a G-adapted ring. To avoid clumpy notation, we write $\mathcal{U} = \mathrm{U}(RG)$ for the unit group of RG. In this section, the main result, $\mathrm{Z}_\infty(\mathcal{U}) \leq \mathrm{Z}(\mathcal{U})\mathrm{Z}_2(G)$, is established.

Recall that $u \in RG$ is called *unipotent* if $u-1$ is *nilpotent*, i.e., if some power of $u-1$ is zero. Let H be a finite group, and put $U = \mathrm{U}(\mathbb{Z}H)$. Arora, Hales and Passi [3, 2.6 Theorem] proved that U is of central height at most two. The proof is essentially based on their observation that a hypercentral unit commutes with all unipotent elements. (However, note that they additionally used Bovdi's results [16] on periodic normal subgroups of the unit group.) Soon afterwards, Arora and Passi used this observation to prove that $[\mathrm{Z}_2(U), H] \leq \mathrm{R}(H)$ if H is not a Dedekind group (see [4, 2.1 Proposition]). It has been remarked in [3, 2.3 Proposition] that $\mathrm{Z}_2(U) \leq \mathrm{N}_U(H)$, which obviously remains true for a periodic group H (see [86, Lemma 1]).

We shall prove suitable generalizations of these results which will lead to the conclusion that $\mathrm{Z}_\infty(\mathcal{U}) \leq \mathrm{Z}_2(\mathcal{U})$. After recalling some basic facts about elements of $\mathrm{N}_\mathcal{U}(G)$, we shall use Blackburn's classification of finite groups H with $\mathrm{R}(H) \neq 1$ to prove that $\mathrm{Z}_\infty(\mathcal{U}) \leq \mathrm{Z}(\mathcal{U})\mathrm{Z}_2(G)$.

First of all, we like to mention the following two instances of when an element of RG commutes with all unipotent elements. Thereby, G can be arbitrary.

23.1 Lemma. *A subgroup H of G with $H \trianglelefteq \mathcal{U}$ centralizes all unipotent elements of $\mathcal{U}$. Likewise, if $\bigcap_{i=0}^{\infty} p^i R = 0$ for some prime p, and some $u \in \mathcal{U}$ has only finitely many conjugates in $\mathcal{U}$, then u commutes with every unipotent element of $\mathcal{U}$.*

Proof. Let $y = 1 - x \in \mathcal{U}$ be a unipotent element, so $x^s = 0$ for some $s \in \mathbb{N}$. Assume that $H \trianglelefteq \mathcal{U}$ for some $H \leq G$, and take any $h \in H$. Let p be a rational prime which divides the order of h, and set $y_n = 1 - p^n x$ for all $n \in \mathbb{N}$. Then $y_n \in \mathcal{U}$, with $y_n^{-1} = 1 + (p^n x) + (p^n x)^2 + \cdots + (p^n x)^{s-1}$, and $y_n^{-1} h y_n \in h + p^n RG$. As $y_n^{-1} h y_n \in G$ and p is not invertible in R, it follows that $[y_n, h] = 1$, so h commutes with x and y. Now assume that $\bigcap_{i=0}^{\infty} p^i R = 0$ for some prime p, and take $u \in \mathcal{U}$ with only finitely many conjugates in $\mathcal{U}$. With y_n as defined just now, $y_n^{-1} u y_n = u + p^n w_n$ for some $w_n \in RG$. As u has only finitely many conjugates in $\mathcal{U}$, there is $m \in \mathbb{N}$ such that $p^m w_m = p^n w_n$ for infinitely many $n \in \mathbb{N}$. Hence $w_m \in p^n RG$ for all $n \in \mathbb{N}$, and it follows that $w_m = 0$, so u commutes with y_m and y. □

We shall see that $\mathrm{Z}_\infty(\mathcal{U}) \leq \mathrm{N}_\mathcal{U}(G)$, and the reader may feel more comfortable if we list some basic facts about elements of $\mathrm{N}_\mathcal{U}(G)$ we will need, together with somewhat condensed proofs.

23.2 Remark. Let G be an arbitrary group, and let $u \in \mathrm{N}_\mathcal{U}(G)$. If $u = \sum_{g \in G} r_g g$ (all r_g in R), then $S = \mathrm{supp}(u) = \{g \in G \mid r_g \neq 0\}$ is the support of u.

(1) The group G acts on S via $x \overset{g}{\mapsto} g^{-1}xg^u$ for $x \in S$ and $g \in G$, and the elements of an orbit under this operation have the same coefficient in u (viewed as an R-linear combination of elements of G). This fundamental fact was observed independently by Coleman and Ward (see page 138, as well for the next remark).

(2) If $pR \neq R$ for some rational prime p, then there is $x \in S$ such that ux^{-1} centralizes a subgroup of G which is of finite p'-index in G (this version of the Ward–Coleman Lemma is given in Lemma 19.4). Indeed, let Q be the kernel of the operation defined in (1), and choose $Q \leq P \leq G$ such that P/Q is a Sylow p-subgroup of the (finite) group G/Q. Since the augmentation of u is a unit in R, there is a fixed point $x \in \operatorname{supp}(u)$ under the operation of P, that is, ux^{-1} centralizes P.

(3) Let $N = \langle S \rangle$, the support group of u. Assume that $1 \in S$. Then it follows from (1) that $g^{-1}g^u \in S$ for all $g \in G$; in other words, $u^g \in uS^{-1} \subseteq RN$. This immediately implies that $N \trianglelefteq G$. Moreover, $\bigcup_{g\in G} \operatorname{supp}(u^g) \subseteq SS^{-1}$ is a finite set, and it follows that each element x of N has only a finite number of conjugates in G (this has already been noted in [93, Corollary 1]). So N is a finitely generated FC-group. If G (and therewith N too) is a periodic group, it follows at once that N is finite (see [113, 14.5.8]). (However, this is always true, see Theorem 18.5).

(4) Assume that G is a periodic group, and that $u^n \in G$ for some $n \in \mathbb{N}$. Then gu is a unit of finite order for all $g \in G$, and choosing $g = x^{-1}$ for some $x \in S$, it follows from [130, II.1.2] and (3) that u is a trivial unit (i.e., of the form rg for some $r \in R$ and $g \in G$).

(5) Though we do not need it, we would like to mention that u is a trivial unit whenever $u^n \in G$ for some $n \in \mathbb{N}$, see Corollary 18.6. Note that if $R = \mathbb{Z}$, this follows readily from a classical result of Berman and Higman, since in any case $uu^* \in \mathrm{Z}(\mathcal{U})$ (see [66, 3.1. Proposition]). Also, we would like to refer the reader to the paper [34] of Farkas and Linnell.

23.3 Proposition. *The following hold:*

(1) $\mathrm{Z}_\infty(\mathcal{U}) \leq \mathrm{N}_\mathcal{U}(G)$*;*

(2) $\mathrm{Z}_\infty(\mathcal{U})/\mathrm{Z}(\mathcal{U})$ *is a periodic group;*

(3) $[\mathcal{U}, \mathrm{Z}_{n+1}(\mathcal{U})] \leq \mathrm{Z}_n(G)$ *for each* $n \in \mathbb{N}$*;*

(4) *every element of* $\mathrm{Z}_\infty(\mathcal{U})$ *commutes with every unipotent element of* $\mathcal{U}$*.*

Proof. As to (1), we shall prove inductively $\mathrm{Z}_n(\mathcal{U}) \leq \mathrm{N}_\mathcal{U}(G)$ for all $n \in \mathbb{N}$. The case $n = 1$ being trivial, let $n > 1$, and take any $u \in \mathrm{Z}_n(\mathcal{U})$ and $g \in G$. Then $g^u = g[g, u] \in \mathrm{N}_\mathcal{U}(G)$ by the induction hypothesis, and therefore $g^u \in G$ by Remark 23.2(4). Now (2) follows since $\mathrm{N}_\mathcal{U}(G)/\mathrm{Z}(\mathcal{U})$ is a periodic group by [93, Theorem 1] (this also follows from Corollary 17.9 and Proposition 19.1). Next, we prove $[\mathcal{U}, \mathrm{Z}_{n+1}(\mathcal{U})] \leq \mathrm{Z}_n(G)$ by

induction on n. Take any $u \in \mathcal{U}$ and $v \in \mathrm{Z}_{n+1}(\mathcal{U})$. Applying the commutator identity $[a,bc] = [a,c][a,b][[a,b],c]$ (see [65, III 1.2]), we get inductively for $k \in \mathbb{N}$ (with $\mathrm{Z}_0(G) = 1$, the case $n = 1$ being obvious) that

$$[u,v^k] = [u,v^{k-1}v] = [u,v][u,v^{k-1}][\underbrace{[u,v^{k-1}]}_{\in \mathrm{Z}_n(\mathcal{U})},v] \in [u,v][u,v^{k-1}] \cdot \mathrm{Z}_{n-1}(G).$$

Continuing in that way, it follows that $[u,v^k] \in [u,v]^k \cdot \mathrm{Z}_{n-1}(G)$. By (2), we can choose $k \in \mathbb{N}$ such that $v^k \in \mathrm{Z}(\mathcal{U})$, and then $[u,v]^k \in \mathrm{Z}_{n-1}(G)$, so $[u,v] \in G$ by Remark 23.2(4). Hence (3) holds for $n = 1$, and for $n > 1$ it follows inductively that $[G,[u,v]] \leq [\mathcal{U},\mathrm{Z}_n(\mathcal{U})] \leq \mathrm{Z}_{n-1}(G)$, so $[u,v] \in \mathrm{Z}_n(G)$, and (3) is proved. Let $x \in \mathcal{U}$ be a unipotent element, so $(x-1)^m = 0$ for some $m \in \mathbb{N}$. We prove inductively that $[x,\mathrm{Z}_n(\mathcal{U})] = 1$, the case $n = 1$ being trivial. Let $n > 1$, and take $u \in \mathrm{Z}_n(\mathcal{U})$. By (3), there is $g \in \mathrm{Z}_{n-1}(G)$ such that $x^u = xg$, and we may assume inductively that $[g,x] = 1$. Let K be a field, containing R, such that $K\langle g\rangle = \oplus_i K e_i$ (the e_i's being idempotents), and write $g = \sum_i \xi_i e_i$ (all ξ_i in K). Let $K[t]$ be a polynomial ring and let μ_i be the endomorphism $K[t] \to \mathrm{End}(e_iKG)$ such that $\mu_i(t)$ is left multiplication with x (note that x commutes with e_i). The kernel of μ_i is a principal ideal generated by $f(t) = (t-1)^l$ for some $l \in \mathbb{N}$ since u is unipotent. On the other hand, $e_i(\xi_i x - 1)^m = (e_i\xi_i x - e_i)^m = (e_i x^u - e_i)^m = e_i(x^u - 1)^m = e_i((x-1)^m)^u = 0$, so $f(t)$ divides $(\xi_i t - 1)^m$, and it follows that $\xi_i = 1$. This shows that $g = 1$, so $[u,x] = 1$, and (4) is proved. □

The group $G \cap \mathrm{Z}_\infty(\mathcal{U})$ will be examined in the next two sections.

23.4 Corollary. *We have $G \cap \mathrm{Z}_\infty(\mathcal{U}) \trianglelefteq \mathcal{U}$.*

Proof. Let $H = G \cap \mathrm{Z}_\infty(\mathcal{U})$. By Proposition 23.3(3), $[\mathcal{U},H] \leq G \cap \mathrm{Z}_\infty(\mathcal{U}) = H$, so $H \trianglelefteq \mathcal{U}$. □

Let H be an arbitrary group. A *power automorphism* of H is an automorphism of H which leaves every subgroup of H invariant (we already encountered power automorphisms of abelian groups in the proof of Proposition 22.4). The power automorphisms of H form an abelian group, which is usually denoted by $\mathrm{PAut}(H)$. Several authors have worked on power automorphisms. Cooper has proved that a power automorphism of H is a *central automorphism*, i.e., induces the trivial automorphism on the central factor group (see [26, Theorem 2.2.1]), and we shall apply this result in a moment.

Let $g,h \in G$, and denote by $\widehat{g}$ the sum of the elements of $\langle g\rangle$. Then $(1-g)h\widehat{g}$ is an element of square zero, and the unipotent element $1 + (1-g)h\widehat{g}$ is called a *bicyclic unit*.

A scrutiny of what is needed for and what is done in the proof of [4, 2.1 Proposition] leads to the following proposition, which paves the way for the application of Blackburn's classification, but also highlights a connection with power automorphisms.

23.5 Proposition. *Assume that some $u \in \mathrm{N}_{\mathcal{U}}(G)$ commutes with all unipotent elements of $\mathbb{Z}G$. Then* $\mathrm{conj}(u) \in \mathrm{PAut}(G)$. *If G is not a Dedekind group, then $[G,u] \leq \mathrm{R}(G)$.*

Proof. If G is a Dedekind group, then there is nothing to prove. Hence we may assume that there is a non-normal cyclic subgroup $C = \langle c \rangle$ of G. Take any $g \in G$. We show that $[g,u] \in C$, by considering the following two possibilities.

Case 1 $c^g \notin C$. Clearly $y = (1-c)g\widehat{c} = g\widehat{c} - cg\widehat{c}$ is a nilpotent element. If $gc^n = cgc^m$ for some integers n and m, then $c^g = c^{n-m}$, a contradiction. Hence $\mathrm{supp}(g\widehat{c}) \cap \mathrm{supp}(cg\widehat{c}) = \emptyset$. Therefore g^u appears with coefficient 1 in $y^u = y$, so $g^u = gc^n$ for some $n \in \mathbb{N}$, and $[g,u] = c^n \in C$.

Case 2 $c^g \in C$. Choose $h \in G$ with $c^h \notin C$, and note that $[h,u] \in C$ by Case 1. Consider the nilpotent element $y = (1-c)hg^{-1}\widehat{c} = hg^{-1}\widehat{c} - chg^{-1}\widehat{c}$. If $hg^{-1}c^n = chg^{-1}c^m$ for some integers n and m, then $c^h = g^{-1}c^{n-m}g \in C$, a contradiction. So $\mathrm{supp}(hg^{-1}\widehat{c}) \cap \mathrm{supp}(chg^{-1}\widehat{c}) = \emptyset$, and as $(hg^{-1})^u$ appears with coefficient 1 in $y^u = y$, it follows that $(hg^{-1})^u = hg^{-1}c^n$ for some $n \in \mathbb{N}$, that is, $[h,u] = g^{-1}c^n g[g,u]$, and therefore $[g,u] \in C$.

Now remember that if $\langle g \rangle \trianglelefteq G$, then obviously $g^u \in \langle g \rangle$, and otherwise we could have chosen $c = g$, so $g^u \in \langle g \rangle$ in any case. □

We remark that we have actually shown the following. If G is an arbitrary group and some $u \in \mathrm{N}_{\mathcal{U}}(G)$ commutes with all unipotent elements of $\mathbb{Z}G$, then $[G,u] \leq C$ for each *finite* non-normal cyclic subgroup C of G.

23.6 Corollary. *We have* $\mathrm{Z}_\infty(\mathcal{U}) = \mathrm{Z}_2(\mathcal{U})$.

Proof. A power automorphism of a group H induces the trivial automorphism of $H/\mathrm{Z}(H)$ (see [26, Theorem 2.2.1]). Together with Propositions 23.3 and 23.5, it follows that $[G, \mathrm{Z}_\infty(\mathcal{U})] \leq \mathrm{Z}(G)$. Hence $[\mathcal{U}, \mathrm{Z}_\infty(\mathcal{U})]$ maps to 1 under the natural map $RG \to RG/\mathrm{Z}(G)$, and therefore $[\mathcal{U}, \mathrm{Z}_\infty(\mathcal{U})] \leq \mathrm{Z}(G)$ by Proposition 23.3(3). The proof is complete. □

Let us recall Lemma 19.5:

23.7 Lemma. *Let M be a finite normal subgroup of G such that for some rational prime p, the center of a Sylow p-subgroup of M is contained in $\mathrm{O}_p(M)$. If $u \in \mathrm{N}_{\mathcal{U}}(G)$ is contained in the center of RM, and $u^{p^n} \in \mathrm{Z}(\mathcal{U})$ for some $n \in \mathbb{N}$, then $u \in \mathrm{Z}(\mathcal{U})M$.*

We have gathered enough information in order to prove the main result.

23.8 Theorem. *Assume that G is not a Dedekind group, and that some $u \in \mathrm{N}_{\mathcal{U}}(G)$ commutes with all unipotent elements of $\mathbb{Z}G$. Then $u \in \mathrm{Z}(\mathcal{U})G$.*

Proof. By Proposition 23.5, $[G,u] \le \mathrm{R}(G)$, so we may assume that $\mathrm{R}(G) \ne 1$. Take any $x \in \mathrm{supp}(u)$. Then $L = \langle \mathrm{supp}(ux^{-1}) \rangle$ is a finite normal subgroup of G by Remark 23.2(3). Since u and x have the same image under the natural map $RG \to RG/L$, and $[G,u] \le \mathrm{R}(G)$, it follows that $[G,x] \le \mathrm{R}(G)L$. Consequently, $M = \mathrm{R}(G)L\langle x \rangle$ is a finite normal subgroup of G which contains $\mathrm{supp}(u)$. If M is not a Dedekind group, then $1 \ne \mathrm{R}(G) \le \mathrm{R}(M)$ (see [11, Lemma 1(a)]). Hence M is either a Dedekind group, or one of the groups described in Theorem 22.2. By Proposition 22.4, $\mathrm{Out_c}(M) = 1$, so $v = uh \in \mathrm{Z}(RM)$ for some $h \in M$. Note that $v^l \in \mathrm{Z}(\mathcal{U})$ for some $l \in \mathbb{N}$. If M is not of type (a) or (e) (as described in Theorem 22.2), then M satisfies the hypothesis of Lemma 23.7 for all primes p, which implies that $v \in \mathrm{Z}(\mathcal{U})G$. Hence we may assume that M is of type (a) or (e), so $M = H \times K$ with normal subgroups H, K of G, and $H = N \rtimes \langle b \rangle$, where b is a p-element, and N is an abelian p'-group. Furthermore, there is $m \in \mathbb{N}$ such that $x^b = x^m$ for all $x \in N$, and $1 \ne \mathrm{R}(M) = \mathrm{C}_{\langle b \rangle}(N) \ne \langle b \rangle$. Assume that $\sigma = \mathrm{conj}(b^i x) \in \mathrm{PAut}(H)$ for some $x \in N$ and $i \in \mathbb{N}$. Then $b(x^{-b}x) = b^x = b\sigma \in \langle b \rangle$, so $x = 1$ as $\mathrm{C}_N(b) = 1$. For any $1 \ne y \in N$, it follows that $y^{b^i}b = (yb)\sigma \in \langle yb \rangle$, so $y^{b^i} = y$. That is, $b^i \in \mathrm{C}_{\langle b \rangle}(N)$, and we have shown that $\sigma = \mathrm{id}$. By Proposition 23.5, $\mathrm{conj}(u)|_H \in \mathrm{PAut}(H)$. Recall that there is $h \in M$ with $uh \in \mathrm{Z}(RM)$, and $[G,u] \le \mathrm{R}(H)$. The observation just made shows that we could have chosen $h = 1$. Thus we may assume that $u \in \mathrm{Z}(RM)$, and it follows that $u^{p^n} \in \mathrm{Z}(\mathcal{U})$ for some $n \in \mathbb{N}$. Put $C = \mathrm{C}_{\langle b \rangle}(N)$, and let $^- : RG \to (R/|N|R)G/NK$ be the natural map. Note that $\{g^x \mid x \in N\} = \{xg \mid x \in N\}$ for $g \in \langle b \rangle \setminus C$, so $\bar{u} \in \bar{R}\bar{C}$. By Lemma 23.7, $[G, u^{-1}b_1] \le NK$ for some $b_1 \in \langle b \rangle$. Assume that $b_1 \notin C$, and that $[g,u] \ne 1$ for some $g \in G$. Then $\bar{b}_1^{\bar{g}} = \bar{b}_2\bar{b}_1$ for some $1 \ne b_2 \in \langle b \rangle$. Note that $C \le \langle b_1^p \rangle$, and $(\bar{b}_1^p)^{\bar{g}} = \bar{b}_2^p\bar{b}_1^p$. Using the natural map $\bar{R}\bar{C} \to \bar{R}\bar{C}/\langle \bar{b}_2^p \rangle$, we see that $\bar{g}^{\bar{b}_1} = \bar{g}^{\bar{u}} \in \bar{g}\langle \bar{b}_2^p \rangle$. So $\bar{b}_2^{-1} = \bar{g}^{-1}\bar{g}^{\bar{b}_1} \in \langle \bar{b}_2^p \rangle$, a contradiction. Hence $u \in \mathrm{Z}(\mathcal{U})$ if $b_1 \notin C$. Now assume that $b_1 \in C$. Then $\langle b_1 \rangle \trianglelefteq G$, and $[g, u^{-1}b_1] = [g,b_1][g,u^{-1}]^{b_1} \le NK \cap \langle b \rangle = 1$ for all $g \in G$, so $u \in \mathrm{Z}(\mathcal{U})b_1$. The proof is complete. □

23.9 Theorem. *We have* $\mathrm{Z}_\infty(\mathcal{U}) \le \mathrm{Z}(\mathcal{U})\mathrm{Z}_2(G)$.

Proof. If G is not a Dedekind group, then $\mathrm{Z}_\infty(\mathcal{U}) \le \mathrm{Z}(\mathcal{U})G$ by Proposition 23.3(1), (4) and Theorem 23.8. If G is a Dedekind group, then $\mathrm{Out_c}(G) = 1$, and $\mathrm{Z}_\infty(\mathcal{U}) \le \mathrm{Z}(\mathcal{U})G$ by Proposition 23.3(1). Hence $\mathrm{Z}_\infty(\mathcal{U}) = \mathrm{Z}(\mathcal{U})H$ with $H = G \cap \mathrm{Z}_\infty(\mathcal{U})$. By Corollary 23.6, $\mathrm{Z}_\infty(\mathcal{U}) = \mathrm{Z}_2(\mathcal{U})$, and with Proposition 23.3(3) it follows that $[G,H] \le [G, \mathrm{Z}_2(\mathcal{U})] \le \mathrm{Z}(G)$. □

24. Subgroups of a group basis which are normal in the unit group

In this section, we shall see that the existence of a non-central subgroup of G which is normal in the unit group $\mathcal{U}$ strongly influences the structure of G. We do not claim that

the results and techniques are new; in fact, most of them are covered by the work [15,16] of Bovdi. We shall need part of [16, Theorem 11], and like to present a short proof for it which is based on Bovdi's work and a group-theoretical characterization of Q*-groups given by Williamson.

We begin by listing the following "elementary" properties of normal subgroups of $\mathcal{U}$ which are contained in G.

24.1 Lemma. *Assume that $H \trianglelefteq \mathcal{U}$ for some subgroup H of G. Then*

(1) $g^h \in \langle g\rangle$ *for all* $g \in G$, $h \in H$;

(2) $h^u \in \langle h\rangle$ *for all* $u \in \mathcal{U}$, $h \in H$;

(3) $[g,h] \in \langle g\rangle \cap \langle h\rangle$ *for all* $g \in G$, $h \in H$;

(4) *units of finite order in RH are trivial.*

Proof. (1) follows from Lemma 23.1 and Proposition 23.5. Assume that there is $h \in H$ such that $\langle h\rangle$ is not normal in $\mathcal{U}$, and choose $u \in \mathcal{U}$ with $g = h^u \notin \langle h\rangle$ (but note that $g \in G$). Then $x = (h-1)u\widehat{h} = hu\widehat{h} - u\widehat{h}$ is a nilpotent element, so $x = x^h$ by Lemma 23.1, and it follows that $u\widehat{h} - h^{-1}u\widehat{h} = h^{-1}x = xh^{-1} = hu\widehat{h} - u\widehat{h}$. Multiplying with u^{-1} from the left, we reach the contradiction $\widehat{h} - g^{-1}\widehat{h} = g\widehat{h} - \widehat{h}$ and $\widehat{h} = g\widehat{h}$. This proves (2), and (3) follows from (1) and (2). Let u be a unit of finite order in RH. By (1), $\langle \mathrm{supp}(u)\rangle$ is a finite group, and we may assume that H is finite. As $H \trianglelefteq \mathrm{U}(RH)$, hu is a unit of finite order too, for all $h \in H$. Hence we may assume that the 1-coefficient of u doesn't vanish. But then u is a trivial unit (see [130, II.1.4]). □

The following lemma should be compared with [16, Theorem 6].

24.2 Lemma. *Let p be a rational prime. Assume that there are p-elements $g, h \in G$ with $\langle h\rangle \trianglelefteq \mathcal{U}$ and $[h,g] \neq 1$. Then $\langle h, g\rangle$ is isomorphic to the quaternion group.*

Proof. We write $\mathrm{o}(x)$ for the order of a group element x. We shall need an elementary group-theoretical fact: if $A = \langle x, y\rangle$ is a finite abelian group with $\mathrm{o}(x) \leq \mathrm{o}(y)$, then there is $a \in A$ such that $A = \langle a\rangle \times \langle y\rangle$.

Set $X = \langle h, g\rangle$, and choose $x \in \langle g\rangle$ of smallest possible order such that $Y = \langle h, x\rangle$ is not abelian. Let $A = \langle h, x^p\rangle$. Then $A \trianglelefteq \mathrm{U}(RY)$ as $x^p \in \mathrm{Z}(Y)$. Note that $x^p \neq 1$ by Lemma 24.1(3). Assume that $\mathrm{o}(h) \leq \mathrm{o}(x^p)$. Then $A = \langle a\rangle \times \langle x^p\rangle$ for some $a \in A$. By Lemma 24.1(2), $\langle a\rangle \trianglelefteq \mathrm{U}(RY)$. As $\langle x\rangle \cap \langle a\rangle = 1$, it follows from Lemma 24.1(3) that $[x,a] = 1$. Consequently, $Y = \langle A, x\rangle = \langle a, x\rangle$ is abelian, a contradiction. Hence $\mathrm{o}(h) > \mathrm{o}(x^p)$. Assume that p is odd. Then $h^x = ch$ for some $c \in \mathrm{Z}(Y)$ of order p. Note that for all $i \in \mathbb{N}$,

$$(xh^i)^p = x^p (h^i)^{x^{p-1}} \cdots (h^i)^{x^2} (h^i)^x h^i = x^p h^{ip} \cdot \underbrace{(c^i)^{p-1} \cdots (c^i)^2 c^i}_{=1 \text{ since } p\neq 2}.$$

If $x^p \in \langle h\rangle$, then $x^p = h^{-np}$ for some $n \in \mathbb{N}$, and $\langle xh^n\rangle$ is a complement of order p to $\langle h\rangle$ in Y. So $[h,x] = 1$ by Lemma 24.1(3), a contradiction. If $x^p \notin \langle h\rangle$, then $A = \langle h\rangle \times \langle x^p h^m\rangle$ for some $m \in \mathbb{N}$. Since $\langle x\rangle \cap \langle h\rangle \neq 1$ by Lemma 24.1(3), $\mathrm{o}(x^p) = \mathrm{o}(h^m)$, so $m = np$ for some $n \in \mathbb{N}$. But then $(xh^n)^p = x^p h^m$, and again we have reached the contradiction that $\langle xh^n\rangle$ is a complement to $\langle h\rangle$ in Y. Thus $p = 2$. We shall show that $\mathrm{o}(h) = 4$. Let s be the involution in $\langle h\rangle$. Then $h^x \in \{h^{-1}, sh^{-1}, sh\}$. If $h^x = h^{-1}$ or $h^x = sh^{-1}$, then by Lemma 24.1(1), $xh^2 = x^h \in \langle x\rangle$ or $xsh^2 = x^h \in \langle x\rangle$, respectively, so $h^2 \in \langle x\rangle$ in both cases since $s \in \langle x\rangle$. But then $h^2 = (h^2)^x = h^{-2}$, and it follows that $\mathrm{o}(h) = 4$. If $h^x = sh$, take $n \in \mathbb{N}$ with $x^{2^{n-1}} \notin \langle h\rangle$, but $x^{2^n} \in \langle h\rangle$. As $\mathrm{o}(h) \geq \mathrm{o}(x)$, there is $m \in \mathbb{N}$ such that $x^{2^n} = h^{-2^n m}$. Also, there is $t \in H$ such that $t^2 = s$. Assume that $[t,x] = 1$. Then $(xh^m)^{2^n} = 1$ if m is even, and $(xth^m)^{2^n} = 1$ if m is odd. In any case, it follows that $\langle h\rangle$ has a complement in Y, contradicting Lemma 24.1(3). Hence $[t,x] \neq 1$, and $\langle h\rangle = \langle t\rangle$ since $[h^2, x] = 1$. We have seen that h is of order 4, so Y is isomorphic to the quaternion group of order 8. Finally, it follows from $[x^2, h] = 1$ that $X = Y$. □

Williamson has given the following group-theoretical characterization of Q^*-groups ([146, p. 495]; see also [98, p. 5505]).

24.3 Lemma. *If G contains a non-central element a such that for all $g \in G$, $\langle a, g\rangle$ is either abelian or isomorphic to the quaternion group, then G is a Q^*-group.*

Proof. There is $b \in G$ such that $Q = \langle a, b\rangle$ is isomorphic to the quaternion group, and it follows that a and b have order 4. Set $A = \mathrm{C}_G(a)$. Observe that $b \notin A$, so for any $g \in A$, $gb \notin A$ and $\langle a, gb\rangle \cong Q$. It follows that $b^2 = a^2 = gbgb$, that is, $g^b = g^{-1}$. Hence A is abelian ($a_1 a_2 = a_1^{-b} a_2^{-b} = (a_2 a_1)^{-b} = a_2 a_1$ for all $a_1, a_2 \in A$). Finally note that A is of index 2 in G since $\mathrm{Aut}(\langle a\rangle) \cong C_2$. □

We can now prove the part of [16, Theorem 11] which will be applied in the next section. Note that the proof could be reduced at once to the case $R = \mathbb{Z}$.

24.4 Theorem. *Assume that $H \trianglelefteq \mathcal{U}$ for some subgroup $H \leq G$ with $H \not\subseteq \mathrm{Z}(G)$. Then G is a Q^*-group.*

Proof. By assumption, there is $a \in H$ with $a \notin \mathrm{Z}(G)$, and we may clearly assume that a is a p-element for some prime p. By Lemma 24.1(2), $\langle a\rangle \trianglelefteq \mathcal{U}$. Take any $g \in G$ such that $\langle a, g\rangle$ is not abelian, and write $g = bx$ with $b, x \in \langle g\rangle$ and b a p-element, x a p'-element. By Lemma 24.1(3), $[a,x] = 1$, so $[a,b] \neq 1$ and $\langle a, b\rangle$ is a quaternion group by Lemma 24.2. Now it follows from [16, Lemma 10], or [146, Lemma 5], that $x = 1$. The basic approach here is to construct explicitly—assuming that $x \neq 1$—a unit in $\mathbb{Z}\langle b, x\rangle$ which does not normalize $\langle a\rangle$. Using a Bass cyclic unit, this has been done most elementary by Parmenter [98, pp. 5504–05]. In view of Lemma 24.3, we are done. □

We finish this section with another application of Lemma 24.1, for what we need a theorem due to Berman (see [130, II.2.18]).

24.5 Theorem. *Let G be a finite group. All units in $\mathbb{Z}G$ of finite order are trivial if and only if G is abelian or a Hamiltonian 2-group.* □

The following lemma, which is part of [16, Theorems 1, 3], can be proved quite easily. Note that we can work over a G-adapted ring R, since we are dealing with a periodic normal subgroup of $\mathcal{U}$ which is contained in G.

24.6 Proposition. *Assume that $H \trianglelefteq \mathcal{U}$ for some non-abelian subgroup H of G. Then G is a Hamiltonian 2-group.*

Proof. As H is non-abelian, it follows from Lemma 24.1(2) that H is Hamiltonian. Choose $x, y \in H$ which do not commute, and let $h \in H$. Then $\langle x, y, h\rangle$ is a finite non-abelian group, and it follows from Theorem 24.5 and Lemma 24.1(4) that h is a 2-element. Hence H is a Hamiltonian 2-group. Together with Lemma 24.1(2) it follows that each $g \in G$ acts as an inner automorphism on H, so $G = \mathrm{C}_G(H)H$. Let $g \in \mathrm{C}_G(H)$, and set $P = \langle g, H\rangle$. Then $P \trianglelefteq \mathrm{U}(RP)$ as $g \in \mathrm{Z}(P)$. So P is a Hamiltonian 2-group too, and $g^2 = 1$ since $g \in \mathrm{Z}(P)$. We have shown that $\mathrm{C}_G(H)$ is an elementary abelian 2-group, and $G = \mathrm{Z}(G)H$. Hence $G \trianglelefteq \mathcal{U}$, and G is a Hamiltonian 2-group. □

25. Non-central elements of the hypercenter

In this section, we discuss what happens when $\mathrm{Z}_2(\mathcal{U}) \neq \mathrm{Z}(\mathcal{U})$. Using results of Bovdi [15,16], a complete description of $\mathrm{Z}_2(\mathcal{U})$ is given in the case when R is a ring of algebraic integers in a totally real number field K (that is, every embedding of K into $\mathbb{C}$ is contained in $\mathbb{R}$).

First of all, however, we like to point out that Corollary 23.6 can be proved using Theorem 24.4 instead of Cooper's result on power automorphisms, in much the same way as [3, 2.6 Theorem] was proved.

Alternative proof of Corollary 23.6. Assume the contrary. Then $\mathrm{Z}_2(\mathcal{U}) < \mathrm{Z}_3(\mathcal{U})$, so $H = [\mathcal{U}, \mathrm{Z}_3(\mathcal{U})] \not\leq \mathrm{Z}(\mathcal{U})$, and $H \leq \mathrm{Z}_2(G)$ by Proposition 23.3(3). By Theorem 24.4, G is a Q^*-group. If G is Hamiltonian, then $\mathrm{Out}_{\mathrm{c}}(G) = 1$, so $\mathrm{Z}_\infty(\mathcal{U}) \leq \mathrm{Z}(\mathcal{U})G$ by Proposition 23.3(1). Let $K = G \cap \mathrm{Z}_\infty(\mathcal{U})$. Then $\mathrm{Z}_\infty(\mathcal{U}) = \mathrm{Z}(\mathcal{U})K$, and $K \trianglelefteq \mathcal{U}$ by Corollary 23.4. Since $G = \mathrm{Z}_2(G)$, $RG/\mathrm{Z}(G)$ is a commutative ring, and looking at the image of $[\mathcal{U}, K]$ under the natural map $RG \to RG/\mathrm{Z}(G)$, it follows that $[\mathcal{U}, K] \leq \mathrm{Z}(G)$, and we obtain the contradiction $H \leq [\mathcal{U}, \mathrm{Z}_\infty(\mathcal{U})] = [\mathcal{U}, \mathrm{Z}(\mathcal{U})K] = [\mathcal{U}, K] \leq \mathrm{Z}(G)$. If G is not Hamiltonian, then $\mathrm{R}(G)$ is a central subgroup of order 2 as G is a Q^*-group, and $[G, \mathrm{Z}_\infty(\mathcal{U})] \leq \mathrm{R}(G) \cong C_2$ by (1) and (4) of Proposition 23.3 and Proposition 23.5. It follows that

$$(*) \quad [G', \mathrm{Z}_\infty(\mathcal{U})] = 1, \qquad (**) \quad [G, \mathrm{Z}_\infty(\mathcal{U})^2] = 1.$$

Looking at the image of H under the natural map $RG \to RG/G'$, we see that $H \leq G'$. Let $u \in \mathcal{U}$ and $x \in \mathrm{Z}_3(\mathcal{U})$. Then $h = [u, x]$ is a typical generator of H, and $h^2 \overset{(*)}{=} h \cdot h^x = [u, x][u, x]^x = [u, x^2] \overset{(**)}{=} 1$. But elements of order 2 in G are contained in the center of G, so $H \leq \mathrm{Z}(G)$, a contradiction. The proof is complete. □

From Theorem 23.9, Corollary 23.4 and Theorem 24.4 we see that the existence of non-central elements of the hypercenter severely limits the structure of G.

25.1 Theorem. *If $\mathrm{Z}_2(\mathcal{U}) \neq \mathrm{Z}(\mathcal{U})$, then G is a Q^*-group.* □

We give a necessary condition for a group element to lie in $\mathrm{Z}_\infty(\mathcal{U})$.

25.2 Lemma. *Assume that there is $x \in G \setminus \mathrm{Z}(G)$ with $x \in \mathrm{Z}_\infty(\mathcal{U})$. Then G is a Q^*-group, and if $G = \langle A, b\rangle$ and a are as in Definition 21.1, then $x^2 = a^2$. If $x \notin A$, then G is a Hamiltonian 2-group.*

Proof. By Corollary 23.4, $G \cap \mathrm{Z}_\infty(\mathcal{U})$ is a normal subgroup of $\mathcal{U}$, and G is a Q^*-group by Theorem 24.4. Let A, b and a be as in Definition 21.1. By Lemma 24.1(3), $[g, x] \in \langle g\rangle \cap \langle x\rangle$ for all $g \in G$. Assume that $x \notin A$. Then $y^{-2} = [y, x] \in \langle y\rangle \cap \langle x\rangle \leq \langle b^2\rangle$ for all $y \in A$. It follows that $y^2 = b^2$, and that G is a Hamiltonian 2-group. Thus we may assume that $x \in A$. If $\langle b\rangle \cap \langle x\rangle = 1$, then $x^2 = [b, x] = 1$ and $x \in \mathrm{Z}(G)$, a contradiction. Hence $\langle b\rangle \cap \langle x\rangle = \langle a^2\rangle$ and $x^2 = [b, x] = a^2$. □

Using [16, Theorem 11], we can prove the following result.

25.3 Proposition. *Let G be a Q^*-group, $G = \langle A, b\rangle$ and $a \in A$ as in Definition 21.1. Let R be a ring of algebraic integers in a totally real number field. Then either G is a Hamiltonian 2-group and $\mathrm{Z}_\infty(\mathcal{U}) = \mathrm{Z}(\mathcal{U})G$, or $\mathrm{Z}_\infty(\mathcal{U}) = \mathrm{Z}(\mathcal{U})\langle g \in A \mid g^2 = a^2\rangle$.*

Proof. Let $H = G \cap \mathrm{Z}_\infty(\mathcal{U})$, a normal subgroup of $\mathcal{U}$ by Corollary 23.4. Take any $x \in H \cap A$. Then either $x \in \mathrm{Z}(G)$ or $x^2 = a^2$ by Lemma 25.2. On the other hand, let $y \in A$ with $y^2 = a^2$, and take any $u \in \mathcal{U}$. Let $*$ be the usual anti-involution of RG (that is, $g^* = g^{-1}$ for $g \in G$, and R-linear extension). Write $u = x_1 + x_2 b$ with $x_i \in RA$; then $uu^* = (x_1 x_1^* + x_2 x_2^*) + x_1 x_2 (b + b^{-1})$ clearly commutes with y, and it follows that $y^u (y^u)^* = 1$. Write $y^u = \sum_{g\in G} r_g g$ (all r_g in R); then $\sum_{g\in G} |r_g|^2 = 1$. Assume that one of the algebraic integers r_g is nonzero, but not a root of unity. Then by a well known theorem of Kronecker (see [95, Theorem 2.1]), there is an embedding $\sigma : R \hookrightarrow \mathbb{C}$ such that $|r_g^\sigma| > 1$, and we obtain the contradiction $1 < \sum_{g\in G} |r_g^\sigma|^2 = 1$ since $R^\sigma \subseteq \mathbb{R}$. Hence exactly one r_g is different from zero, and $y^u \in G$ (this is Bovdi's argument from [16, Theorem 11]). Note that y^u and y have the same image under the natural map $RG \to RG/\langle a^2\rangle$ since $[G, y] = \langle a^2\rangle$, so $[u, y] \in \langle a^2\rangle \leq \mathrm{Z}(G)$. It follows that $y \in \mathrm{Z}_2(\mathcal{U})$. Up to now, we have seen that $H \cap A = \mathrm{Z}(G)\langle g \in A : g^2 = a^2\rangle$. Assume that $H \not\subseteq A$. Then G is a Hamiltonian 2-group by Lemma 25.2 (or by Proposition 24.6,

since H is non-abelian). But then A, b and a can be chosen such that a is any given non-central element of G, so $H = G$. The proposition now follows from Theorem 23.9. □

On the other hand, if R is in a certain sense "large enough", then one should expect that $\mathrm{Z}_2(\mathcal{U}) = \mathrm{Z}(\mathcal{U})$. (In this context, note that there is an obvious gap in the proof of [16, Theorem 4].) As in the proof of [16, Lemma 4], we obtain the following proposition.

25.4 Proposition. *If there are* $r_i \in R$ *with* $r_1^2 + r_2^2 + r_3^2 = r_1$ *and* $(r_1, r_2, r_3) \notin \{(0,0,0), (1,0,0)\}$*, then* $\mathrm{Z}_2(\mathcal{U}) = \mathrm{Z}(\mathcal{U})$*.*

Proof. Assume the contrary. Then G is a Q^*-group by Theorem 25.1, say $G = \langle A, b\rangle$ and $a \in A$ as in Definition 21.1, and there is $g \in G$ with $g \in G \setminus \mathrm{Z}(G)$ and $g \in \mathrm{Z}_2(\mathcal{U})$. By Lemma 25.2, $g^2 = a^2$. Let $r_i \in R$ with $r_1^2 + r_2^2 + r_3^2 = r_1$ and (r_1, r_2, r_3) different from $(0,0,0)$ and $(1,0,0)$. Then $\langle g, h\rangle$ is a quaternion group, and $u = r_1 g + (1 - r_1)g^3 + r_2(h - g^2h) + r_3(gh - g^3h)$ is a nontrivial unit of RG of order 4. By Corollary 23.4 and Lemma 24.1, $\langle g\rangle \trianglelefteq \mathcal{U}$, so $g^{-1}u$ and $g^{-3}u$ are nontrivial units of finite order too. But one of these units has nonzero 1-coefficient, so must be a trivial unit (see [76, Theorem 3.2.3]). We have reached a contradiction, and the proposition is proved. □

VII. Finite conjugacy for orders in division rings

Knowledge does not keep any better than fish.

Alfred North Whitehead
The aims of education, 1929

We show that for a periodic group G, the FC-center of $\mathrm{U}(\mathbb{Z}G)$ and the second center of $\mathrm{U}(\mathbb{Z}G)$ coincide, using a characterization of the FC-subring of $\mathbb{Z}H$ for a finite group H given by Sehgal and Zassenhaus [131]. Together with work of Li and Parmenter [87] on the hypercenter of $\mathrm{U}(\mathbb{Z}G)$, this yields a short proof of a recent result of Jespers and Juriaans [70] on the FC-center which avoids the use of Amitsur's classification [2] of finite subgroups in division rings. Also, for a totally definite quaternion algebra generated (as $\mathbb{Q}$-algebra) by a finite multiplicative subgroup G, the group of units of the $\mathbb{Z}$-order $\mathbb{Z}[G]$ spanned by G is described explicitly.

26. The finite conjugacy center and the second center

Herstein [51] proved that any element of a division ring is either central or has infinitely many conjugates. The proof is based on the Brauer-Cartan-Hua theorem, and in the sequel further results aiming at a dichotomy as expressed in this theorem have been proved (see [53, Chapter 6]). Somewhat more precisely, the objective was to show that certain subgroups or subrings of a division ring which are invariant with respect to certain natural operations must be small or large, in a very well specified way. One might ask whether similar results also hold for $\mathbb{Z}$-orders in division rings, a question that naturally arises in the study of the *FC-subring* $\mathrm{FC}(\mathbb{Z}G)$ of the integral group ring of a group G, which is defined as the set of all elements of $\mathbb{Z}G$ having only finitely many conjugates under the action of the group of units $\mathrm{U}(\mathbb{Z}G)$. First results on $\mathrm{FC}(\mathbb{Z}G)$ are contained in A. A. Bovdi's paper [16]. Williamson [146] gave a necessary and sufficient condition for an element of G to belong to $\mathrm{FC}(\mathbb{Z}G)$. Motivated by this result, Sehgal and Zassenhaus [131] characterized the FC-subring $\mathrm{FC}(\mathbb{Z}G)$ for a finite group G as follows:

26.1 Theorem (Sehgal, Zassenhaus). *Let G be a finite group. Then the FC-subring of $\mathbb{Z}G$ consists of all those elements x of $\mathbb{Z}G$ for which $\Gamma(x)$ is central in $\Gamma(\mathbb{Z}G)$ for*

every irreducible representation Γ *of* $\mathbb{Q}G$ *over* $\mathbb{Q}$ *for which* $\Gamma(\mathbb{Q}G)$ *is not a totally definite quaternion algebra.*

(Recall that a finite dimensional $\mathbb{Q}$-algebra A is said to be a *totally definite quaternion algebra* if the center F of A is a totally real field and $A \otimes_F \mathbb{R}$ is a Hamilton quaternion algebra.)

After that, FC-elements in group rings over fields were studied in [105, 24]. Recently, finite conjugacy in orders and algebras was re-investigated in [33]. This paper contains some general results on FC-units in algebras, with a few applications to group rings. (However, one might note that the first remark in Section 4 is a special case of [131, Theorem 2], and that Lemma 4.3 and Proposition 4.4 are already contained in [16].) V. Bovdi [17] investigated the FC-subring of quite general rings.

For any group G, the set $\Delta(G)$ of elements of G having only a finite number of conjugates form a characteristic subgroup of G, called the FC-center of G. Note that $\Delta(\mathrm{U}(\mathbb{Z}G)) = \mathrm{U}(\mathbb{Z}G) \cap \mathrm{FC}(\mathbb{Z}G)$. Jespers and Juriaans [70] characterized the periodic groups G with $\Delta(\mathrm{U}(\mathbb{Z}G))$ non-central in $\mathbb{Z}G$ (these are the so-called Q*-groups, see Definition 21.1), and described $\Delta(\mathrm{U}(\mathbb{Z}G))$ explicitly. This classification coincides with the classification of the periodic groups G with $\mathrm{U}(\mathbb{Z}G)$ having non-central second center $\mathrm{Z}_2(\mathrm{U}(\mathbb{Z}G))$, given by Li and Parmenter [86, 87] (see Theorem 21.2). This connection is not even mentioned in [70], though a crucial step in both classifications is to establish that the considered subgroups of $\mathrm{U}(\mathbb{Z}G)$ are periodic over the center of $\mathrm{U}(\mathbb{Z}G)$ (cf. Proposition 23.3). In Section 27, we show how Theorem 26.1 can be used to give a short and rigorous proof of the following theorem.

26.2 Theorem. *If* G *is a periodic group then* $\Delta(\mathrm{U}(\mathbb{Z}G)) = \mathrm{Z}_2(\mathrm{U}(\mathbb{Z}G))$.

Taking the description of $\mathrm{Z}_2(\mathrm{U}(\mathbb{Z}G))$ given by Li and Parmenter for granted, this proves the Jespers–Juriaans result without the use of Amitsur's classification of the finite groups that are embeddable in the multiplicative groups of division rings, which was achieved in the technically complicated paper [2].

As noted in [70], Theorem 18.3 should prove to be very useful to achieve a description of $\Delta(\mathrm{U}(\mathbb{Z}G))$ for more general G.

If a group G is embedded in the multiplicative group of a division ring of characteristic zero, we will write $\mathbb{Q}[G] = \{\sum a_g g \mid g \in G, a_g \in \mathbb{Q}\}$ and $\mathbb{Z}[G] = \{\sum a_g g \mid g \in G, a_g \in \mathbb{Z}\}$. In the remaining sections of this chapter, we will prove the following theorem.

26.3 Theorem. *Let* G *be a non-cyclic finite group contained in the multiplicative group of a division ring of characteristic zero. Then one of the following holds.*

(i) *Any* $u \in \mathbb{Z}[G]$ *is either central in* $\mathbb{Z}[G]$ *or has infinitely many conjugates under the action of* $\mathrm{U}(\mathbb{Z}G)$ *induced by the natural homomorphism* $\mathrm{U}(\mathbb{Z}G) \to \mathbb{Z}[G]^\times$.

(ii) G *is isomorphic to one of the following groups:* $\mathrm{SL}(2,3)$, $\mathrm{SL}(2,5)$, *the binary octahedral group, or to one of the groups* $C_k \rtimes C_4$, $C_k \rtimes Q_{2^l}$ *described in Proposition 29.2*

below, and then any element of $\mathbb{Q}[G]$ has only a finite number of conjugates under the action of the unit group $\mathbb{Z}[G]^\times$.

Actually, this theorem follows almost immediately from Theorem 26.1 and Amitsur's classification. What we are really doing is to construct in case (i) units in $\mathrm{U}(\mathbb{Z}G)$ that can be used to produce infinitely many different conjugates of an element, if there are any (this is done in Section 28), and in case (ii), explicit descriptions of the unit groups $\mathbb{Z}[G]^\times$ are given in Section 29. This might be useful for the problem of describing generators of a subgroup of finite index of $\mathrm{U}(\mathbb{Z}G)$ for fixed-point free groups G, a problem which seems to be still open (see [38, 96]).

Amitsur's classification

As preparation for Sections 28 and 29, we recall parts of Amitsur's classification [2] of the finite groups that can be embedded in the multiplicative group of a division ring of characteristic zero, thereby fixing the notation.

Let m, r be two relatively prime integers. Set $s = (r-1, m)$, $t = m/s$ and let n be the minimal integer satisfying $r^n \equiv 1 \pmod{m}$. Then[1]

$$G_{m,r} = \langle a, b \mid a^m = 1, b^n = a^t, a^b = a^r \rangle$$

is a group of order mn with center $\langle a^t \rangle$. By [2, Theorem 7], a finite group G can be embedded in a division ring of characteristic zero if and only if G is one of the following types: (1) a cyclic group, (2) a group $G_{m,r}$, where the integers m, r etc. satisfy certain conditions, (3) a group $\mathrm{SL}(2,3) \times G_{m,r}$, again with certain conditions on m, r etc. ($G_{m,r} = 1$ is allowed), (4) the binary octahedral group or $\mathrm{SL}(2,5)$.

Let ϵ_m be a fixed primitive mth root of unity, and set $\epsilon_s = \epsilon_m^t$. Set $\mathcal{C}_m = \mathbb{Q}(\epsilon_m)$, and let σ be the automorphism of $\mathcal{C}_m$ determined by the mapping $\epsilon_m \mapsto \epsilon_m^r$. Let $\mathcal{Z}$ be the fixed field under the operation of σ. The cyclic algebra determined by $\mathcal{C}_m$, σ and ϵ_s will be denoted by $\mathfrak{A}_{m,r}$; this is a crossed product algebra in the sense of [106, Section 29]. In particular, $\mathfrak{A}_{m,r}$ is a central simple algebra of dimension n^2 over its center $\mathcal{Z}$.

If a group $G_{m,r}$ is contained in a division ring of characteristic zero, then $\mathbb{Q}[G_{m,r}] \cong \mathfrak{A}_{m,r}$ (see [2, Lemma 4]), and the isomorphism is given by the correspondence $a \leftrightarrow A$, $b \leftrightarrow B$, where

$$A = \begin{bmatrix} \epsilon_m & & & & \\ & \epsilon_m^\sigma & & & \\ & & \epsilon_m^{\sigma^2} & & \\ & & & \ddots & \\ & & & & \epsilon_m^{\sigma^{n-1}} \end{bmatrix}, \quad B = \begin{bmatrix} & & & & \epsilon_s \\ 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \end{bmatrix}$$

[1] There should be no mistaking with the wreath products $G_{n,r}$ from Section 9.

(this is a quite convenient representation to work with). Sometimes we will identify $\mathcal{C}_m$ with $\mathbb{Q}[A]$. Clearly, we have an action of $\mathrm{U}(\mathbb{Z}G_{m,r})$ on $\mathfrak{A}_{m,r}$ induced by the natural homomorphism $\mathrm{U}(\mathbb{Z}G_{m,r}) \to \mathfrak{A}_{m,r}^{\times}$.

27. On the finite conjugacy center

Let $\mathcal{U}$ be the unit group of the integral group ring $\mathbb{Z}G$ of a periodic group G. In this section, a short proof is given for the fact that the finite conjugacy center $\Delta(\mathcal{U})$ coincides with the second center $\mathrm{Z}_2(\mathcal{U})$. Note that $\mathrm{Z}_2(\mathcal{U})$ has been completely determined by Parmenter and Li [87], see also Chapter VI.

Some information on elements of $\Delta(\mathcal{U})$ will be needed in case G is finite. We first recall two basic observations. The following well known lemma, which was already known to Berman, shows that Wedderburn components of $\mathbb{Q}G$ which are division rings deserve special attention (a slightly more general version is given as Lemma 23.1).

27.1 Lemma. *Let G be a group. If some element u in $\mathbb{Z}G$ has only finitely many conjugates (under the action of $\mathrm{U}(\mathbb{Z}G)$), then u commutes with every nilpotent element of $\mathbb{Z}G$.* □

If G is finite, then each Wedderburn component of $\mathbb{Q}G$ which is a proper matrix ring is generated (as $\mathbb{Q}$-algebra) by elements of $\mathbb{Z}G$ of square zero, so $\Delta(\mathcal{U})$ centralizes such components (this too is known for a long time).

If a Wedderburn component is a division ring, one may wish to have a reduction to the case that G embeds into this component. This is achieved by the following lemma.

27.2 Lemma. *Let G be a finite group, and u an element of $\mathbb{Z}G$ which has only finitely many conjugates (under the action of $\mathrm{U}(\mathbb{Z}G)$). Then for a normal subgroup N of G, the image of u in $\mathbb{Z}G/N$ has only finitely many conjugates, too.*

Proof. Set $n = |N|$. It is well known that $\mathbb{Z}G$ is a pullback over the *finite* ring $(\mathbb{Z}/|n|\mathbb{Z})\,(G/N)$:

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \mathbb{Z}G/N \\ \downarrow & & \downarrow \\ \mathbb{Z}G/(\hat{N}) & \longrightarrow & (\mathbb{Z}/|n|\mathbb{Z})\,(G/N) \end{array} .$$

Assume, by way of contradiction, that the image $\bar{u}$ of u in $\mathbb{Z}G/N$ has infinitely many conjugates. Then there are units $v_0, v_1, v_2, \ldots$ in $\mathbb{Z}G/N$ which all have the same image in $(\mathbb{Z}/|n|\mathbb{Z})\,(G/N)$, and $\bar{u}^{v_0}, \bar{u}^{v_1}, \bar{u}^{v_2}, \ldots$ are pairwise different conjugates of $\bar{u}$. The units $w_1 := v_1 v_0^{-1}, w_2 := v_2 v_0^{-1}, \ldots$ map to 1 in $(\mathbb{Z}/|n|\mathbb{Z})\,(G/N)$ and can therefore be lifted to units of $\mathbb{Z}G$. This provides a contradiction since $\bar{u}^{w_1}, \bar{u}^{w_2}, \ldots$ are pairwise different conjugates. □

In view of Theorem 26.1, we record the following well known fact.

27.3 Remark. Let D be a totally definite quaternion algebra, generated (as $\mathbb{Q}$-algebra) by a finite multiplicative subgroup G. Let $*$ be the involution induced by G, $(\sum a_g g)^* = \sum a_g g^{-1}$ ($a_g \in \mathbb{Q}$, $g \in G$). Then $*$ is the "classical" involution, and dd^* lies in the center of D, for all $d \in D$. Indeed, if F denotes the center of D, then by definition we have $G \subset D \otimes_F \mathbb{R} \cong \{\left[\begin{smallmatrix} r & s \\ -\bar{s} & \bar{r} \end{smallmatrix}\right] \mid r, s \in \mathbb{R}\}$. For $g \in G$, $\det(g)$ is a positive real number, so $\det(g) = 1$ and $g^{-1} = \bar{g}^{\mathrm{tr}}$, the hermitian transposed. Thus for $d = \left[\begin{smallmatrix} r & s \\ -\bar{s} & \bar{r} \end{smallmatrix}\right]$, we have $dd^* = \left[\begin{smallmatrix} r & s \\ -\bar{s} & \bar{r} \end{smallmatrix}\right]\left[\begin{smallmatrix} \bar{r} & -s \\ \bar{s} & r \end{smallmatrix}\right] = \left[\begin{smallmatrix} r\bar{r}+s\bar{s} & 0 \\ 0 & r\bar{r}+s\bar{s} \end{smallmatrix}\right]$.

Thus Theorem 26.1 has the following corollary.

27.4 Corollary. *Let G be a finite group. Then uu^* is central in $\mathbb{Z}G$ for all $u \in \mathrm{FC}(\mathbb{Z}G)$. In particular, if $u \in \Delta(\mathrm{U}(\mathbb{Z}G))$, then $u \in \mathrm{N}_{\mathrm{U}(\mathbb{Z}G)}(G)$ (since $(g^u)(g^u)^* = 1$ for $g \in G$; see also Lemma 6.1(vii)).* □

Note that this also follows from claim (AC) in [70], and that this is what is actually needed for the proof of [70, Theorem 1.1]. The result also follows from Lemma 27.1, Lemma 27.2 and the results from Section 28, but such a proof then relies on Amitsur's classification.

Here is a quick proof of Theorem 26.2:

Proof of Theorem 26.2. Set $\mathcal{U} = \mathrm{U}(\mathbb{Z}G)$ and let $u \in \Delta(\mathcal{U})$. Then $F := \langle x^g \mid x \in \mathrm{supp}(u), g \in G\rangle \trianglelefteq G$ is a finitely generated periodic FC-group, that is, a finite group. Take any $g \in G$, and set $H = \langle F, g\rangle$ (a finite group). Clearly $u \in \Delta(\mathrm{U}(\mathbb{Z}H))$. By Corollary 27.4, $u \in \mathrm{N}_{\mathrm{U}(\mathbb{Z}F)}(H)$. Since g was arbitrarily chosen, it follows that $u \in \mathrm{N}_{\mathrm{U}(\mathbb{Z}F)}(G)$. In particular, u has finite order over the center of $\mathcal{U}$, so $\mathcal{U}^{-1+\langle u\rangle} := \{[v, u^n] \mid v \in \mathcal{U}, n \in \mathbb{Z}\}$ is a finite set. By a theorem of Baer (see Theorem 17.4), this condition ensures that $M := \langle \mathcal{U}^{-1+\langle u\rangle}\rangle = [\mathcal{U}, \langle u\rangle]$ is a finite normal subgroup of $\mathcal{U}$. Clearly M is augmented, so $M \leq G$ by a result of Berman and Rossa (see [15]), and each subgroup of M is a finite normal subgroup of $\mathcal{U}$ (see [16, Theorem 2]). Consequently $[\mathcal{U}, M] \leq \mathrm{Z}(G)$ by [146, Theorem 1]. Thus $\langle u\rangle \subseteq \mathrm{Z}_3(\mathcal{U})$. By [86, Theorem 2], we have $\mathrm{Z}_3(\mathcal{U}) = \mathrm{Z}_2(\mathcal{U})$, and it follows that $\Delta(\mathcal{U}) \subseteq \mathrm{Z}_2(\mathcal{U})$. The converse inclusion follows immediately from [87, Theorem 2] and [146, Theorem 1]. □

There are even more approaches to the characterization of $\Delta(\mathrm{U}(\mathbb{Z}G))$ for a periodic group G. Set $\mathcal{U} = \mathrm{U}(\mathbb{Z}G)$ and let $u \in \Delta(\mathcal{U})$. By Corollary 27.4, we have $u \in \mathrm{N}_{\mathrm{U}(\mathbb{Z}G)}(G)$. By Lemma 27.1, u commutes with every nilpotent element of $\mathbb{Z}G$. But this implies $u \in \mathrm{Z}(\mathcal{U})G$ by Theorem 23.8.[2] Thus we get a complete characterization of $\Delta(\mathrm{U}(\mathbb{Z}G))$ from [146].

One could also first characterize $\Delta(\mathrm{U}(\mathbb{Z}G))$ for G finite using [4, Theorem 3.7], and then argue as in the proof of [70, Corollary 2.4].

[2] This argument now appears in the final version [71] of [70].

27.5 Remark. One might ask whether there is a complete description of $\Delta(\mathrm{U}(\mathbb{Z}G))$ for an arbitrary group G. Though Theorem 18.3 gives in some sense a reduction to finite groups, this seems not really within reach. We shall content ourselves with a few comments.

Let $u \in \Delta(\mathrm{U}(\mathbb{Z}G))$. By Theorem 18.3, there is a finite normal subgroup T of G and a group element $g \in G$ such that $u = vg$ for some $v \in \mathrm{U}(\mathbb{Z}T)$. Then $uu^* = vv^* \in \Delta(\mathrm{U}(\mathbb{Z}T))$, and it follows from Theorem 26.1 and Remark 27.3 that $vv^* \in \mathrm{Z}(\mathrm{U}(\mathbb{Z}T))$. By the usual star-argument, it follows that $v \in \mathrm{N}_{\mathrm{U}(\mathbb{Z}T)}(T)$ (this was also noted in [70]).

Now assume that g has infinite order. Clearly we can assume that v has augmentation 1. Then $H := \langle T, vg\rangle$ is a group basis of $\mathbb{Z}\langle T, g\rangle$. Trivially $vg \in \mathrm{N}_{\mathrm{U}(\mathbb{Z}H)}(H)$, and since by Lemma 23.1, vg commutes with all unipotent elements of $\mathbb{Z}H$, we have $[T, vg] \leq C$ for each cyclic non-normal subgroup C of T, by the remark following Proposition 23.5. Note that conjugation with vg on T is a power automorphism. We now could try to imitate the proof of Theorem 23.8 to show that $vg \in \mathrm{Z}(\mathrm{U}(\mathbb{Z}H))H$, but we did not elaborate on that. We remark that if $vg \notin \mathrm{Z}(\mathrm{U}(\mathbb{Z}H))$, then T is either a Dedekind group or a group from Blackburn's list (see Theorem 22.2).

Note that vg has finite order over the center of H. Thus we may apply Theorem 17.4 of Baer to obtain that $[\mathrm{U}(\mathbb{Z}H), vg]$ is a finite normal subgroup of $\mathrm{U}(\mathbb{Z}H)$. By [15], $[\mathrm{U}(\mathbb{Z}H), vg] \leq T$. We may also apply Cooper's result [26, Theorem 2.2.1] to obtain that $[\mathrm{U}(\mathbb{Z}T), vg] \leq \mathrm{Z}(T)$.

We finish this remark with an example (cf. [24, Example 1], [5]). Let $G = C_3 \rtimes \langle a\rangle$, where the element a is of infinite order and acts by inversion on C_3. By Lemma 18.1, we have $\mathrm{U}(\mathbb{Z}G) = \pm G$, so $\Delta(\mathrm{U}(\mathbb{Z}G)) = \mathrm{U}(\mathbb{Z}G)$. The element a cannot be multiplied with a central unit so that the resulting unit has finite order.

28. Division rings of dimension greater than 4 over the center

In this section, we treat the algebras $\mathfrak{A}_{m,r}$ which are division rings of dimension greater than 4 over the center. Nevertheless, to prove the main result Proposition 28.4, we will need some information about a particular class of algebras $\mathfrak{A}_{m,r}$ with $n = 2$:

28.1 Proposition. *Let p be an odd prime and q an odd number with $(p, q) = 1$, and choose an integer r with $r \equiv 1 \pmod p$ and $r \equiv -1 \pmod q$. Set $m = 2pq$, and note that*

$$G := G_{m,r} = \langle a, b \mid a^{2pq} = 1, b^2 = a^q, (a^p)^b = a^{-p}\rangle.$$

The element $A^{2p} - B$ is a unit in $\mathbb{Z}[\langle A, B\rangle]$ having two eigenvalues with different absolute values. There is a unit in $\mathbb{Z}G$ and a certain power of $a^{2p} - b$ having the same image in $\mathbb{Z}G/(\widehat{b^{2p}}, \widehat{b^4})$. Consequently any element of $\mathfrak{A}_{m,r}$ is either central in $\mathfrak{A}_{m,r}$ or has infinitely many conjugates under the action of $\mathrm{U}(\mathbb{Z}G)$.

Proof. Recall that $A^{2p} = \left[\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 0 & 1 \\ -\xi & 0 \end{smallmatrix}\right]$, where ζ and ξ are primitive qth and pth complex roots of unity, respectively. Thus $A^{2p} - B$ has determinant $1 + \xi$ and is therefore a unit in $\mathbb{Z}[\langle A, B\rangle]$. Its eigenvalues are $\lambda_{1,2} = ((\zeta + \zeta^{-1}) \pm \sqrt{D})/2$ with $D = (\zeta + \zeta^{-1})^2 - 4(1 + \xi)$. Assume that $|\lambda_1| = |\lambda_2|$. Then $\sqrt{D}$ has to be pure imaginary, for geometrical reason, meaning that D, and hence $4(1 + \xi)$ too, is a real number. This contradiction proves that $|\lambda_1| \neq |\lambda_2|$.

Note that $(a^{2p} - b)(a^{-2p} + b) = 1 + a^{2p}b - ba^{-2p} - b^2 = 1 - b^2$. We have $b^2 = b^{2p}b^{2(p+1)}$ with b^{2p} of order 2 and $b^{2(p+1)}$ of order p. Thus $1 - b^2$ and $1 + b^{2(p+1)}$ have the same image in $\Lambda := \mathbb{Z}G/(\widehat{b^{2p}}, \widehat{b^4})$. Since $1 + b^{2(p+1)}$ becomes a unit in the quotient $\mathbb{Z}\langle b^4\rangle/(\widehat{b^4})$ (which is isomorphic to $\mathbb{Z}[\xi]$), it follows that the image λ of $a^{2p} - b$ in Λ is a unit. The group ring $\mathbb{Z}G$ can be written as a pullback

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \Gamma \\ \downarrow & & \downarrow \\ \Lambda & \longrightarrow & \bar{\Lambda} \end{array}$$

with $\bar{\Lambda}$ a *finite* ring (this is well known, see Section 7). Thus a power of λ maps to 1 in $\bar{\Lambda}$, and can therefore be lifted to a unit of $\mathbb{Z}G$.

Let x be any element in $\mathfrak{A}_{m,r}$ which has only a finite number of conjugates under the action of $\mathrm{U}(\mathbb{Z}G)$. Then x commutes with some power of $A^{2p} - B$. Since $A^{2p} - B$ has eigenvalues with different absolute values, this means that x and $A^{2p} - B$ can be simultaneously diagonalized, so x commutes with $A^{2p} - B$ and is therefore of the form $\left[\begin{smallmatrix} \alpha & \beta \\ -\xi\beta & \alpha + (\zeta - \zeta^{-1})\beta \end{smallmatrix}\right]$ for some $\alpha, \beta \in \mathbb{Q}(\zeta, \xi)$. Also, x commutes with $A^{-2p} - B$, hence is of the form $\left[\begin{smallmatrix} \alpha & \beta \\ -\xi\beta & \alpha + (\zeta^{-1} - \zeta)\beta \end{smallmatrix}\right]$. Thus $\beta = 0$ and x is central in $\mathfrak{A}_{m,r}$. □

We will need the following well known facts.

28.2 Lemma. *Let $n_1, n_2 \in \mathbb{N}$ with $n_1 \geq 2$, $n_2 > 2$ and let ζ be a primitive $(n_1 n_2)$th root of unity. Assume that $\mathbb{Q}(\zeta^{n_1}) \subset \mathbb{Q}(\zeta)$. Then there is a cyclotomic unit u of $\mathbb{Z}[\zeta]$ such that $u^k \notin \mathbb{Z}[\zeta^{n_1}]$ for all $k \in \mathbb{N}$.*

Proof. Set $\zeta = \exp(2\pi i/n_1 n_2)$ and let σ be a nontrivial Galois automorphism of $\mathbb{Q}(\zeta)$ which fixes ζ^{n_1}. Clearly $\zeta^\sigma = \zeta^s$ and $st \equiv 1 \pmod{n_1 n_2}$ for some $s, t \in \mathbb{N}$. Set $u = (1 - \zeta^t)/(1 - \zeta)$, a cyclotomic unit of $\mathbb{Z}[\zeta]$, and assume that $u^k \in \mathbb{Z}[\zeta^{n_1}]$ for some $k \in \mathbb{N}$. Then $u^k = (u^\sigma)^k$. In particular, $|u| = |u^\sigma|$, that is, $|1 - \zeta^t||1 - \zeta^s| = |1 - \zeta|^2$. However, a simple geometric consideration shows that $|1 - \zeta| \leq |1 - \zeta^l|$ for all $l \in \mathbb{N}$, with equality if and only if $\zeta^l = \zeta^{\pm 1}$. Hence σ is complex conjugation, a contradiction. □

28.3 Lemma. *Let C be a cyclic group, and ζ a root of unity of the same order as C. Then the natural map $\mathrm{U}(\mathbb{Z}C) \to \mathbb{Z}[\zeta]^\times$ has finite cokernel.* □

The first part of the proof of the next proposition was essentially noted in [70, Lemma 5.1].

28.4 Proposition. *Assume that $\mathfrak{A}_{m,r}$ is a division algebra with $n^2 > 4$. Then any element of $\mathfrak{A}_{m,r}$ is either central in $\mathfrak{A}_{m,r}$ or has infinitely many conjugates under the action of $\mathrm{U}(\mathbb{Z}G_{m,r})$.*

Proof. We first show that if some element $c \in \mathcal{C}_m$ has only a finite number of conjugates under the action of $\mathrm{U}(\mathbb{Z}\langle b\rangle)$ then already $c \in \mathcal{Z}$. Set $S = \mathrm{C}_{\langle B\rangle}(c)$. If $S = \langle B\rangle$, then $c \in \mathcal{Z}$ follows readily from $B^{-1}AB = A^\sigma$. Thus assume that $d := [\langle B\rangle : S] \geq 2$. Note that $\langle B^n\rangle \leq S < \langle B\rangle$, and that n divides the order of $\langle B^n\rangle$ (see [2, Lemma 5]). Let ζ be a primitive (ns)th root of unity. By Lemma 28.2, there is a cyclotomic unit u in $\mathbb{Z}[\zeta]$ such that $u^k \notin \mathbb{Z}[\zeta^d]$ for all $k \in \mathbb{N}$. There are homomorphisms $\mathbb{Z}\langle b\rangle \to \mathbb{Z}[\zeta] \to \mathfrak{A}_{m,r}$, defined by $b \mapsto \zeta \mapsto B$, and $u^{\varphi(ns)}$, where φ denotes Euler's function, can be lifted to a unit v of $\mathbb{Z}\langle b\rangle$ (in fact, to a Bass cyclic unit, see [129, (10.3)]). By assumption, c commutes with the image of some power of v, and by construction of v, this image is of the form $\sum_{i=0}^{n-1} c_i B^i$ (all $c_i \in \mathcal{C}_m$) with $c_i \neq 0$ and $B^i \notin S$ for some index i. This contradiction proves that $c \in \mathcal{Z}$.

Now let x be any element in $\mathfrak{A}_{m,r}$ which has only a finite number of conjugates under the action of $\mathrm{U}(\mathbb{Z}G_{m,r})$; we have to show that $x \in \mathcal{Z}$. Note that by [2, Theorem 4], m is divisible by an odd prime. Thus the elements $u_i := 1 - (-1)^m \epsilon_m^{r^i}$, $0 \leq i < n$, are units in $\mathbb{Z}[\epsilon_m]$ (see [143, Proposition 2.8]), and $1 - (-1)^m A$ is a unit in $\mathbb{Z}[A]$. Since some power of $1 - (-1)^m A$ lifts to a unit in $\mathrm{U}(\mathbb{Z}\langle a\rangle)$ (see Lemma 28.3), it follows that x commutes with $(1 - (-1)^m A)^k$ for some $k \in \mathbb{N}$. Thus if the (i,j)th entry in x is nonzero, we must have $u_i^k u_j^{-k} = 1$. Taking absolute values, wee see that this can happen only if $i = j$ or $u_i = \overline{u_j}$. If n is odd or $4 \mid n$, it follows that x is a diagonal matrix, i.e, $x \in \mathcal{C}_m$, and therefore $x \in \mathcal{Z}$ as shown above. Thus we can assume that n is divisible by 2, but not by 4. Then $\epsilon_s = -\xi$ with $\xi \neq 1$, $\xi^q = 1$ for some odd number q, by [2, Lemma 5]. We can also assume that for some odd prime p, $\mathcal{C}_m$ contains a primitive pth root of unity ζ with $\zeta^{\sigma^{n/2}} = \zeta^{-1}$. Let $\tilde{A}$ be an element of order p in $\langle A\rangle$. Note that

$$B^{n/2} = \begin{bmatrix} & & & \epsilon_s \\ & & \iddots & \\ & & & \epsilon_s \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{bmatrix}.$$

Thus $x = k_1 + k_2 B^{n/2}$ for some $k_i \in \mathcal{C}_m$. It follows at once that k_1 and k_2 have only a finite number of conjugates under the action of $\mathrm{U}(\mathbb{Z}\langle b\rangle)$, so they are contained in the center $\mathcal{Z}$. By Proposition 28.1, $M = \tilde{A} - B^{n/2}$ is a unit in $\mathbb{Z}[G]$, and after conjugation with a

permutation matrix we can assume that B is a block diagonal matrix with block entries $\left[\begin{smallmatrix} 0 & 1 \\ -\xi & 0 \end{smallmatrix}\right]$. Then M is a block diagonal matrix with block entries of the form $M_i = \left[\begin{smallmatrix} \zeta^i & 1 \\ -\xi & \zeta^{-i} \end{smallmatrix}\right]$, $1 \leq i < p$. By Proposition 28.1, each M_i has eigenvalues with different absolute values. Since $B^{n/2}$ and M does not commute, it follows that $B^{n/2}$ does not commute with any power of M (otherwise $B^{n/2}$ and M could be simultaneously diagonalized). Again by Proposition 28.1 it follows that $B^{n/2}$ has infinitely many conjugates under the action of $\mathrm{U}(\mathbb{Z}G)$. Thus $k_2 = 0$ and $x = k_1 \in \mathcal{Z}$. □

28.5 Proposition. *Assume that $G = \mathrm{SL}(2,3) \times G_{m,r}$ can be embedded in a division ring of characteristic zero, for some nontrivial group $G_{m,r}$. Then any element of $\mathbb{Q}[G]$ is either central in $\mathbb{Q}[G]$ or has infinitely many conjugates under the action of $\mathrm{U}(\mathbb{Z}G)$.*

Proof. Assume that $G_{m,r}$ is not cyclic. Then by [2, Theorem 6a (and its proof)], we can assume that $G_{m',r'} \subset G$ for some numbers m', r', and that $\mathbb{Q}[G] = \mathfrak{A}_{m',r'}$ is of dimension > 4 over its center. Thus the claim follows from Proposition 28.4.

Assume that $G_{m,r}$ is a cyclic group C_m of odd order. By [2, Theorem 6a, Lemma 12], we can assume that G is generated by the matrices $P = \left[\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right]$, $Q = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ and $R = \frac{1}{2}\left[\begin{smallmatrix} -1-i & -1-i \\ 1-i & i-1 \end{smallmatrix}\right]$, and the matrix $C = \left[\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta \end{smallmatrix}\right]$, where ζ is a primitive mth root of unity. Then $D = 1 + CP = \left[\begin{smallmatrix} 1+i\zeta & 0 \\ 0 & 1-i\zeta \end{smallmatrix}\right]$, having determinant $1 + \zeta^2$, is a unit in $\mathbb{Z}[G]$, and the eigenvalues of D have different absolute values. Note that some power of D lifts to a unit of the integral group ring of G (details in a similar case are given in the proof of Proposition 28.1). Now let x be an element in $\mathbb{Q}[G]$ which has only a finite number of conjugates under the action of $\mathrm{U}(\mathbb{Z}G)$. Then x commutes with some power of D, meaning that x is a diagonal matrix, $\left[\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right]$, say. Likewise, $R^{-1}xR = \frac{1}{2}\left[\begin{smallmatrix} \lambda_1+\lambda_2 & \lambda_1-\lambda_2 \\ \lambda_1-\lambda_2 & \lambda_1+\lambda_2 \end{smallmatrix}\right]$ is a diagonal matrix, so $\lambda_1 = \lambda_2$ and x lies in the center of $\mathbb{Q}[G]$. □

29. Division rings of dimension 2 over the center

If $G_{m,r}$ with $n = 2$ is such that $\mathfrak{A}_{m,r}$ is a division ring, then $G_{m,r}$ is one of the groups described in the next two propositions. This follows from Amitsur's classification; the reader might wish to compare with the presentation given in [134, Section 2]. After having dealt with these cases, we determine the structure of $\mathbb{Z}[G]^\times$ in the remaining "exceptional" cases.

29.1 Proposition. *Let C_k be a cyclic group of odd order k, and assume that $G = G_{m,r}$ is isomorphic to either*

(i) *$Q_8 \times C_k$, where Q_8 is the quaternion group, or*

(ii) *$(C_q \rtimes C_{2^l}) \times C_k$, where $l > 1$ and C_{2^l} acts by inversion on C_q, q odd.*

Then any element of $\mathfrak{A}_{m,r}$ is either central in $\mathfrak{A}_{m,r}$ or has infinitely many conjugates under the action of $\mathrm{U}(\mathbb{Z}G)$.

Proof. Let x be an element of $\mathfrak{A}_{m,r}$ which has only a finite number of conjugates under the action of $\mathrm{U}(\mathbb{Z}G)$.

In case (i), $\mathfrak{A}_{m,r}$ contains the matrices $P = \left[\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right]$, $Q = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ and $C = \left[\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta \end{smallmatrix}\right]$, where ζ is a primitive kth root of unity, as homomorphic images of elements of G. The matrices $M_1 = 1+CP$ and $M_2 = 1+CQ$ are units in $\mathfrak{A}_{m,r}$, with suitable powers of them lifting to units of the integral group ring of G (see the proof of Proposition 28.5). Thus x commutes with some power of M_1 and is therefore a diagonal matrix, $\left[\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right]$, say. Likewise, $M_2^{-1}xM_2 = (1+\zeta^2)^{-1}\left[\begin{smallmatrix} \lambda_1+\zeta^2\lambda_2 & \zeta(\lambda_1-\lambda_2) \\ \zeta(\lambda_1-\lambda_2) & \lambda_2+\zeta^2\lambda_1 \end{smallmatrix}\right]$ is a diagonal matrix, so $\lambda_1 - \lambda_2 = 0$ and x lies in the center of $\mathfrak{A}_{m,r}$.

In case (ii), $\mathfrak{A}_{m,r}$ contains as homomorphic images of elements of G the matrices $P = \left[\begin{smallmatrix} 0 & 1 \\ \epsilon\zeta^{-1} & 0 \end{smallmatrix}\right]$, $D = \left[\begin{smallmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{smallmatrix}\right]$ and $C = \left[\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta \end{smallmatrix}\right]$, where ϵ, ξ and ζ are primitive 2^{l-1}th, qth, and kth roots of unity, respectively. The matrices $M_1 = 1 + CD$ and $M_2 = 1 + CP$ are units in $\mathfrak{A}_{m,r}$, with suitable powers of them lifting to units of the integral group ring of G. Since the eigenvalues of M_1 have different absolute values, x commutes with some power of M_1 and is therefore a diagonal matrix, $\left[\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right]$, say. Likewise, $M_2^{-1}xM_2 = (1-\epsilon\zeta)^{-1}\left[\begin{smallmatrix} \lambda_1-\epsilon\zeta\lambda_2 & \zeta(\lambda_1-\lambda_2) \\ -\epsilon(\lambda_1-\lambda_2) & \lambda_2-\epsilon\zeta\lambda_1 \end{smallmatrix}\right]$ is a diagonal matrix, so $\lambda_1 - \lambda_2 = 0$ and x lies in the center of $\mathfrak{A}_{m,r}$. □

Note that in all cases we will consider from now on, $\mathbb{Q}[G]$ is a totally definite quaternion algebra.

29.2 Proposition. *Let C_k be a nontrivial cyclic group of odd order k, and assume that $G = G_{m,r}$ is isomorphic to either*

(i) *$C_k \rtimes C_4$, where C_4 acts by inversion, or*

(ii) *$C_k \rtimes Q_{2^l}$, where $l > 2$, a cyclic subgroup $C_{2^{l-1}}$ acts trivially on C_k, and a subgroup of order 4 acts by inversion.*

Identify G with its image in $\mathfrak{A}_{m,r}$. Then $\mathbb{Z}[G]^\times = \mathbb{Z}[A]^\times G$. In particular, any element of $\mathfrak{A}_{m,r}$ has only a finite number of conjugates under the action of the unit group $\mathbb{Z}[G]^\times$.

Proof. Note that $\mathbb{Z}[\epsilon_m]^\times_{\mathbb{R}} := \mathbb{Z}[\epsilon_m]^\times \cap \mathbb{R} = \mathbb{Z}[\epsilon_m^i + \epsilon_m^{-i}, i \in \mathbb{N}]$ is of finite index in $\mathbb{Z}[\epsilon_m]^\times$, and that $\mathbb{Z}[\epsilon_m]^\times_{\mathbb{R}}$ is contained in the center of $\mathfrak{A}_{m,r}$.

Let $M = \left[\begin{smallmatrix} x & y \\ -\bar{y} & \bar{x} \end{smallmatrix}\right]$ be a matrix in $\mathbb{Z}[G]$ with determinant 1, that is, $x\bar{x} + y\bar{y} = 1$. If both x and y would be nonzero, this would imply that the norm $\mathrm{N}_{\mathbb{Q}(\epsilon_m)/\mathbb{Q}}(x)$ lies strictly between 0 and 1, which is impossible. If $x\bar{x} = 1$, then x is a root of unity. The same holds for y, so $M \in G$.

Now take any $M = \left[\begin{smallmatrix} x & y \\ -\bar{y} & \bar{x} \end{smallmatrix}\right] \in \mathbb{Z}[G]^\times$. Note that $\delta := \det(M) \in \mathbb{Z}[\epsilon_m]^\times_{\mathbb{R}}$, that is, δ is contained in the center of $\mathbb{Z}[G]$. Since $\left[\begin{smallmatrix} \delta & 0 \\ 0 & \delta \end{smallmatrix}\right]^{-1} M^2$ has determinant 1, it follows that $M^2 \in \mathbb{Z}[\epsilon_m]^\times_{\mathbb{R}} G$. In particular, either the diagonal entries of M^2 or the off-diagonal entries of M^2 vanish. Since $M^2 = \left[\begin{smallmatrix} x^2-y\bar{y} & y(x+\bar{x}) \\ -\bar{y}(x+\bar{x}) & \bar{x}^2-y\bar{y} \end{smallmatrix}\right]$, this means that either $x^2 = \bar{x}^2$ and $x + \bar{x} \neq 0$, or $y(x + \bar{x}) = 0$. In the first case, one gets $x = \bar{x}$ and the contradiction $2xy \in \mathbb{Z}[\epsilon_m]^\times$. Assume that both x and y are nonzero. Then $x + \bar{x} = 0$, that is, x is pure imaginary. But the entries of AM are also all nonzero (recall that $A = \left[\begin{smallmatrix} \epsilon_m & 0 \\ 0 & \epsilon_m^{-1} \end{smallmatrix}\right]$), thus $\epsilon_m x$ is pure imaginary, by the same reasoning. This contradiction shows that $\mathbb{Z}[G]^\times = \mathbb{Z}[A]^\times G$. In particular, $\mathbb{Z}[G]^\times$ is finite over its center. □

29.3 Proposition. *Let G be the binary tetrahedral group of order 24 (so $G \cong \mathrm{SL}(2,3)$), embedded in the multiplicative group of a division ring of characteristic zero. Then $\mathbb{Z}[G]^\times = G$.*

Proof. By [2, Lemma 12], we have $\mathbb{Q}[G] = \{\left[\begin{smallmatrix} r & s \\ -\bar{s} & \bar{r} \end{smallmatrix}\right] \mid r, s \in \mathbb{Q}(i)\}$, and we can assume that $G = \langle P, Q\rangle \rtimes \langle R\rangle$, where $P = \left[\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right]$, $Q = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ and $R = \frac{1}{2}\left[\begin{smallmatrix} -1-i & -1-i \\ 1-i & i-1 \end{smallmatrix}\right]$. Then $\mathbb{Z}[G] \subset \frac{1}{2}\mathrm{Mat}_2(\mathbb{Z}[i])$. Let $M = \left[\begin{smallmatrix} r & s \\ -\bar{s} & \bar{r} \end{smallmatrix}\right] \in \mathbb{Z}[G]^\times$. Then $\det(M) = r\bar{r} + s\bar{s} > 0$, so $\det(M) = 1$ as $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$. One readily verifies that $\mathrm{Mat}_2(\mathbb{Z}[i])$ contains exactly 8 matrices of determinant 1 and 16 matrices of determinant 4, which shows that $\mathbb{Z}[G]^\times = G$. □

29.4 Proposition. *Let G be the binary octahedral group of order 48, embedded in the multiplicative group of a division ring of characteristic zero. Then $\mathbb{Z}[G]^\times \cong G \times C_\infty$. If $G = \langle T, Q, R\rangle$ as in [2, Lemma 13], then the factor C_∞ is generated by $1+T^3R+TQR$.*

Proof. By [2, Lemma 13], we have $\mathbb{Q}[G] = \left\{\left[\begin{smallmatrix} r & s \\ -\bar{s} & \bar{r} \end{smallmatrix}\right] \mid r, s \in \mathbb{Q}(i, \sqrt{2})\right\}$, and we can assume that $G = \langle T, Q, R\rangle$, where $T = \frac{\sqrt{2}}{2}\left[\begin{smallmatrix} 1+i & 0 \\ 0 & 1-i \end{smallmatrix}\right]$, $Q = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ and $R = \frac{1}{2}\left[\begin{smallmatrix} -1-i & -1-i \\ 1-i & i-1 \end{smallmatrix}\right]$. Then $\mathbb{Z}[G] \subset \Lambda := \frac{1}{2}\mathrm{Mat}_2(\mathbb{Z}[i, \sqrt{2}]) \cap \mathbb{Q}[G]$. Note that $\mathbb{Z}[\sqrt{2}] \subset \mathbb{Z}[G]$ (in fact, we have $T^3R + TQR = \left[\begin{smallmatrix} \sqrt{2} & 0 \\ 0 & \sqrt{2} \end{smallmatrix}\right]$), and that $\mathbb{Z}[\sqrt{2}]^\times = \langle\varepsilon\rangle$, where $\varepsilon = 1 + \sqrt{2}$. Let $M \in \Lambda^\times$, and write $M = \frac{1}{2}\left[\begin{smallmatrix} r & s \\ -\bar{s} & \bar{r} \end{smallmatrix}\right]$ with $r, s \in \mathbb{Z}[i, \sqrt{2}]$. Note that

$$r = \alpha + \beta\sqrt{2} + \gamma i + \delta i\sqrt{2} \quad \text{with } \alpha, \beta, \gamma, \delta \in \mathbb{Z},$$
$$r\bar{r} = (\alpha^2 + \gamma^2) + 2(\beta^2 + \delta^2) + 2(\alpha\beta + \gamma\delta)\sqrt{2},$$

and similarly for s. One readily verifies that $\det(M) = (r\bar{r} + s\bar{s})/4 \neq \varepsilon$. Therefore $\det(M)$ is an even power of ε, and it follows that $\Lambda^\times = \langle\tilde{\varepsilon}\rangle\Lambda_1^\times$, where $\Lambda_1^\times = \{M \in \Lambda \mid \det(M) = 1\}$ and $\tilde{\varepsilon} = \left[\begin{smallmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{smallmatrix}\right]$. Clearly $\Lambda_1^\times$ is a finite group, and $\mathbb{Z}[G]^\times = \langle\tilde{\varepsilon}\rangle(\mathbb{Z}[G] \cap \Lambda_1^\times)$. Since $\mathbb{Z}[G] \cap \Lambda_1^\times$ is a finite group in $\mathbb{Q}[G]^\times$ containing G, it follows from Amitsur's classification that $G = \mathbb{Z}[G] \cap \Lambda_1^\times$. □

29.5 Proposition. *Let G be the binary icosahedral group of order* 120 *(i.e., $G = \mathrm{SL}(2,5)$), embedded in the multiplicative group of a division ring of characteristic zero. Then $\mathbb{Z}[G]^\times \cong G \times C_\infty$. If $G = \langle \epsilon, j, i_1 \rangle$ as in [2, Lemma 14], then the factor C_∞ is generated by $\epsilon + \epsilon^{-1}$.*

Proof. By [2, Lemma 14 and subsequent discussion], we can assume that $G = \langle \epsilon, j, i_1 \rangle \subset \mathfrak{A}_{5,-1}$, where ($\zeta$ denotes a primitive 5th complex root of unity) $\epsilon = \left[\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}\right]$, $j = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ and $i_1 = \frac{\sqrt{5}}{5}\left[\begin{smallmatrix} \zeta^2-\zeta^3 & \zeta-\zeta^4 \\ \zeta-\zeta^4 & -(\zeta^2-\zeta^3) \end{smallmatrix}\right]$. The following matrices form a system of right coset representatives for the subgroup $\langle \epsilon, j \rangle$ of order 20 (this has been checked using Maple [144]):

$$
\begin{aligned}
r_1 &= \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \\
r_2 = (i_1\epsilon)^2 &= \tfrac{1}{5}\left[\begin{smallmatrix} -2+\zeta-\zeta^2+2\zeta^3 & -1-2\zeta+2\zeta^2+\zeta^3 \\ -1-2\zeta-3\zeta^2-4\zeta^3 & -3-\zeta+\zeta^2-2\zeta^3 \end{smallmatrix}\right], \\
r_3 = r_2^2 &= \tfrac{1}{5}\left[\begin{smallmatrix} -3-\zeta+\zeta^2-2\zeta^3 & 1+2\zeta-2\zeta^2-\zeta^3 \\ 1+2\zeta+3\zeta^2+4\zeta^3 & -2+\zeta-\zeta^2+2\zeta^3 \end{smallmatrix}\right], \\
r_4 = i_1\epsilon i_1 &= \tfrac{1}{5}\left[\begin{smallmatrix} 3+\zeta+4\zeta^2+2\zeta^3 & -1-2\zeta-3\zeta^2+\zeta^3 \\ -1-2\zeta-3\zeta^2+\zeta^3 & 2-\zeta+\zeta^2+3\zeta^3 \end{smallmatrix}\right], \\
r_5 = r_4^3 &= \tfrac{1}{5}\left[\begin{smallmatrix} -1-2\zeta-3\zeta^2-4\zeta^3 & 2+4\zeta+\zeta^2+3\zeta^3 \\ 2+4\zeta+\zeta^2+3\zeta^3 & 1+2\zeta-2\zeta^2-\zeta^3 \end{smallmatrix}\right], \\
r_6 = r_4^7 &= \tfrac{1}{5}\left[\begin{smallmatrix} 1+2\zeta-2\zeta^2-\zeta^3 & -2-4\zeta-\zeta^2-3\zeta^3 \\ -2-4\zeta-\zeta^2-3\zeta^3 & -1-2\zeta-3\zeta^2-4\zeta^3 \end{smallmatrix}\right].
\end{aligned}
$$

Note that $\mathbb{Z}[\zeta]^\times = \langle \zeta \rangle \times \langle \omega \rangle$, where $\omega = \zeta + \zeta^{-1}$, and that $\tilde{\omega} := \epsilon + \epsilon^{-1}$ is a central unit in $\mathbb{Z}[G]$ corresponding to ω. We have $r_5 + r_6 = \frac{-1}{5}\left[\begin{smallmatrix} \zeta^2+\zeta^3 & 0 \\ 0 & \zeta^2+\zeta^3 \end{smallmatrix}\right]$, so $\frac{1}{5} \in \mathbb{Z}[G]$ and $\mathbb{Z}[G] = \Lambda := \frac{1}{5}\mathrm{Mat}_2(\mathbb{Z}[\zeta]) \cap \mathfrak{A}_{5,-1}$.

Set $\Lambda_1^\times = \{M \in \Lambda \mid \det(M) = 1\}$; we will show that $\Lambda_1^\times$ is finite. Take any $M \in \Lambda_1^\times$, and write $M = \frac{1}{5}\left[\begin{smallmatrix} r & s \\ -\bar{s} & \bar{r} \end{smallmatrix}\right]$ with $r, s \in \mathbb{Z}[\zeta]$. Assume that $s = 0$. Then $r\bar{r} = 25$, and it is a finite problem to check that $r = 5\zeta^n$ for some $n \in \mathbb{N}$, so $M \in G$. This also holds if $t = 0$, so assume from now on that $s, t \neq 0$. It follows from $r\bar{r} + s\bar{s} = 25$ that the norms $\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(r)$ and $\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(s)$ are bounded above by 25^2. Consequently, there are finitely many elements of $\mathbb{Z}[\zeta]$ (not depending on M) such that both r and s is associated to one of these elements. A quick calculation shows that if for some $a, b \in \mathbb{Z}$, the matrix $M = \frac{1}{5}\left[\begin{smallmatrix} r\omega^a & s\omega^b \\ -\bar{s}\omega^b & \bar{r}\omega^a \end{smallmatrix}\right]$ lies in $\Lambda_1^\times$, then $(1-\omega^{2b})/(1-\omega^{2a}) = -r\bar{r}/s\bar{s} < 0$. Now assume that there exists an infinite number of pairs $(a_1, b_1), (a_2, b_2), \ldots$ of integers such that $(1-\omega^{2b_n})/(1-\omega^{2a_n}) = -r\bar{r}/s\bar{s}$ for all n. Assume further that $\omega^{2a_n} < 1$ for all n. This forces $\omega^{2b_n} > 1$ for all n (because of the minus sign!), so $\lim_{n\to\infty} 1 - \omega^{2a_n} = 1$ and $\lim_{n\to\infty} 1 - \omega^{2b_n} = -\infty$, which is impossible. Similarly, the case $\omega^{2a_n} > 1$ (all n) is ruled out. Thus we obtain a contradiction by considering a suitable sub-sequence. Altogether, we have shown that $\Lambda_1^\times$ is finite. As $G \subseteq \Lambda_1^\times$, it follows from Amitsur's classification that $G = \Lambda_1^\times$.

Take any $M \in \mathbb{Z}[G]^\times$. Then $\det(M) \in \mathbb{Z}[\zeta]^\times \cap \mathbb{R} = \langle \omega \rangle$. We wish to show that $M \in G \times \langle \tilde{\omega} \rangle$; by the above, this holds if $\det(M) \in \langle \omega^2 \rangle$. Thus assume that $\det(M) = \omega^n$ for some odd number n; we will reach at once a contradiction. We can assume that $n = 1$. There is $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ with $\omega^\tau < 0$, and then $0 < (r\bar{r} + s\bar{s})^\tau = \det(M)^\tau < 0$. This final contradiction proves that $\mathbb{Z}[G]^\times = G \times \langle \tilde{\omega} \rangle$. □

VIII. Central units in p-blocks

> Alice laughed: "There's no use trying," she said; "one can't believe impossible things." "I daresay you haven't had much practice," said the Queen. "When I was younger, I always did it for half an hour a day. Why, sometimes I've believed as many as six impossible things before breakfast."
>
> *Lewis Carroll*
> *Alice's Adventures in Wonderland, 1865*

We show that the principal 3-block of a finite group G contains a nontrivial central unit of order 3 provided that $O_{3'}(G) = 1$ and G contains a non-central element of order 3 which commutes with none of its other conjugates. This supplements Robinson's results [114,115] on the character theory of a counterexample to the Z_p^*-theorem for odd p. That non-principal p-blocks may very well have nontrivial central units of order p is shown by means of an example.

30. On Robinson's unit

It is an important open problem to find a direct and "representation-theoretic" proof of some odd analogue to Glauberman's Z^*-theorem [39], which would provide a significant simplification in the classification of finite simple groups (see [43, Remark 7.8.3], [19, 6.5]). The following theorem comprises Glauberman's theorem ($p = 2$), and follows for odd p easily from the classification of finite simple groups (see [47, Theorem 4.1], and [6]).

Z_p^*-theorem. *Let G be a finite group and p a prime. If x is an element of order p in G with $x^G \cap P = \{x\}$ for some Sylow p-subgroup P of G, then $[x, G] \leq O_{p'}(G)$.*

Nevertheless, it would be useful and instructive to find a direct proof. Robinson studied in [114] the character theory of a minimal counterexample, K, to the Z_p^*-theorem for odd p. It is well known that K is either simple, or else $K = K'\langle x\rangle$ where K' is simple, $K' \neq K$, and x is an element of order p in K which commutes with none of its other conjugates. In [115], Robinson showed that his results can be used to place the problem in quite another context, that of units in group rings: he demonstrated the existence of

a nontrivial central unit of order p in the principal p-block of K, provided that $p \geq 5$, or that $p = 3$ and K is not simple.

To be more precise, we introduce the following notation. Let G be a finite group. For a prime p, let $\mathbb{Z}_{(p)} = \{a/b \mid a \in \mathbb{Z},\, b \in \mathbb{Z} \setminus p\mathbb{Z}\}$. Let $\mathrm{B}_0(\mathbb{Z}_{(p)}G)$ be the principal block of $\mathbb{Z}_{(p)}G$, with block idempotent e_0, so that $\mathrm{B}_0(\mathbb{Z}_{(p)}G) = e_0(\mathbb{Z}_{(p)}G)$. For an element $g \in G$, let C_g denote the class sum of g in $\mathbb{Z}G$.

Robinson's unit is $f_0C_{x^2}(f_0C_x)^{-1}$, where f_0 is the block idempotent of $\mathrm{B}_0(\mathbb{Z}_{(p)}K)$.

We shall give an elementary proof of the following theorem (note that together with Robinson's results, it ensures the existence of a nontrivial central unit of order p in all cases).

30.1 Theorem. *Let x be an element of order 3 in G which commutes with none of its other conjugates. Then e_0C_x is a unit in $\mathrm{B}_0(\mathbb{Z}_{(3)}G)$, and setting*

$$u_x = e_0C_x(e_0C_{x^{-1}})^{-1},$$

we have:

(i) *u_x is a normalized unit of order 3 in the center of $\mathrm{B}_0(\mathbb{Z}_{(3)}G)$.*

(ii) *If u_x is a trivial unit, i.e., if $u_x = e_0g$ for some $g \in G$, then $[x, G] \leq \mathrm{O}_{3'}(G)$.*

We begin with a couple of remarks and well known facts. Let G be an arbitrary finite group and keep the previous notation.

The first two remarks are essentially taken from Robinson's paper [115].

30.2 Lemma. *Let x be an element of G which is contained in the center of a Sylow p-subgroup of G. Then e_0C_x is a unit in $\mathrm{B}_0(\mathbb{Z}_{(p)}G)$.*

Proof. Let $R = \mathbb{Z}_{(p)}[\theta]$, where θ is a primitive $|G|$th root of unity. Then e_0 remains primitive in $\mathrm{Z}(RG)$ (as is well known). Let $\mathrm{Irr}_0^{(p)}(G)$ be the set of irreducible complex characters belonging to the principal p-block of G, and set $K = \mathbb{Q}[\theta]$. For $\chi \in \mathrm{Irr}_0^{(p)}(G)$, let e_χ be the associated idempotent of $\mathrm{Z}(KG)$ and ω_χ the associated central character of $\mathrm{Z}(KG)$. Then $e_0C_x = \sum_{\chi \in \mathrm{Irr}_0^{(p)}(G)} \omega_\chi(C_x)e_\chi$. By the standard congruence for the principal block, we have for any $\chi \in \mathrm{Irr}_0^{(p)}(G)$ that $\omega_\chi(C_x) := [G : \mathrm{C}_G(x)](\chi(x)/\chi(1)) \equiv [G : \mathrm{C}_G(x)] \pmod{\mathrm{rad}(R)}$, so that $u := e_0C_x$ is a unit in $\Lambda_1 := \bigoplus_{\chi \in \mathrm{Irr}_0^{(p)}(G)} e_\chi RG$ (since $\omega_\chi(C_x) \in \mathbb{Z}[\theta] \subset R$ and $p \nmid [G : \mathrm{C}_G(x)]$). Set $\Lambda_2 = e_0RG$. The abelian group Λ_1/Λ_2 is a finitely generated R-module, is annihilated by $|G|$, and is therefore finite. Thus the elements $u^{-1}, u^{-2}, \ldots$ cannot lie in pairwise different cosets of Λ_2, which means that $\lambda := u^{-n} - u^{-m} \in \Lambda_2$ for some $n, m \in \mathbb{N}$ with $1 \leq n < m$. Then $u^{-1} = (1 - \lambda u^n)u^{m-n-1} \in \Lambda_2$. Set $\Lambda_0 = e_0\mathbb{Z}_{(p)}G$. Note that Λ_2 is a noetherian $\mathbb{Z}_{(p)}$-module (since it is finitely generated over $\mathbb{Z}_{(p)}$). Hence the chain $\Lambda_0 \subseteq \Lambda_0u^{-1} \subseteq \Lambda_0u^{-2} \subseteq \ldots \subseteq \Lambda_2$ becomes stationary, $\Lambda_0u^{-n} = \Lambda_0u^{-(n+1)}$ for some $n \in \mathbb{N}$. It follows that $\Lambda_0 = \Lambda_0u^{-1}$, so u is a unit in Λ_0, and we are done. □

It is clear that this observation can be generalized to arbitrary blocks, using [35, (IV.4.3)].

30.3 Remark. Let x be an element of G which is contained in the center of a Sylow p-subgroup of G. Then e_0C_x is a unit in $\mathrm{B}_0(\mathbb{Z}_{(p)}G)$, and setting $u_x = e_0C_x(e_0C_{x^{-1}})^{-1}$, we have:

(i) u_x is a normalized unit in the center of $\mathrm{B}_0(\mathbb{Z}_{(p)}G)$.

(ii) u_x is of finite order if and only if $\chi(x)$ is rational or a real multiple of a root of unity, for all $\chi \in \mathrm{Irr}_0^{(p)}(G)$. The order of u_x divides, if finite, the order of x.

(iii) If x is not conjugate to x^{-1} in G, then $u_x \neq e_0$.

(iv) If u_x is a trivial unit, i.e., if $u_x = e_0g$ for some $g \in G$, then $[g, G] \leq \mathrm{O}_{p'}(G)$, and g may be chosen such that x is conjugate to gx^{-1} in G and $[x, g] = 1$.

Proof. That u_x is a unit in $\mathrm{B}_0(\mathbb{Z}_{(p)}G)$ is shown in Lemma 30.2, and it is clear that u_x has augmentation 1, so (i) holds. We have $u_x = \sum_{\chi \in \mathrm{Irr}_0^{(p)}(G)}(\chi(x)/\chi(x^{-1}))e_\chi$ (with notation as above). If $\chi(x)$ is rational, then $\chi(x) = \chi(x^{-1})$, and if $\chi(x)$ is a real multiple of a root of unity ξ, then $\chi(x)/\chi(x^{-1}) = \chi(x)/\overline{\chi(x)} = \xi^2$. This already establishes one part of (ii). On the other hand, if u_x is of finite order, and $\chi \in \mathrm{Irr}_0^{(p)}(G)$, then $\chi(x) = \xi \cdot \chi(x^{-1}) = \xi \cdot \overline{\chi(x)}$ for some root of unity ξ, which implies that $\chi(x)$ is a real multiple of a root of unity. The remark on the order of u_x is clear from the description of u_x.

Let a, b be p-elements in G with $e_0C_a = e_0C_b$. Then C_a and C_b have the same augmentation, and therefore $\chi(a) = \chi(b)$ for all $\chi \in \mathrm{Irr}_0^{(p)}(G)$. Thus it follows from block orthogonality (see [35, (IV.6.3)]) that a and b are conjugate in G. This proves (iii).

Assume that u_x is a trivial unit, i.e., that $u_x = e_0g$ for some $g \in G$. Then e_0g is a central unit, and since $\mathrm{O}_{p'}(G)$ is the kernel of $\mathrm{B}_0(\mathbb{Z}_{(p)}G)$ (see [35, (IV.4.12)]), it follows that $[g, G] \leq \mathrm{O}_{p'}(G)$. By (ii), u_x has order a power of p, so we can assume that g is a p-element. Moreover, we can assume that x and g are contained in a Sylow p-subgroup; then $[x, g] = 1$. Set $\bar{G} = G/\mathrm{O}_{p'}(G)$. It follows from $e_0C_x = e_0gC_{x^{-1}}$ that $\bar{e}_0C_{\bar{x}} = \bar{e}_0C_{\bar{g}\bar{x}^{-1}}$ in the principal p-block $\bar{e}_0\mathbb{Z}_{(p)}\bar{G}$ of $\mathbb{Z}_{(p)}\bar{G}$. Thus $\bar{x}$ and $\bar{g}\bar{x}^{-1}$ are conjugate in $\bar{G}$ (see the last paragraph), which implies that x and gx^{-1} are conjugate in G. The proof is complete. □

If P is a p-group, and x an element in P which commutes with none of its other conjugates, then clearly $x \in \mathrm{Z}(P)$. Thus, in the situation of Theorem 30.1, e_0C_x is a unit in $\mathrm{B}_0(\mathbb{Z}_{(3)}G)$, by Lemma 30.2. As to part (ii) of the theorem, assume that $u_x = e_0g$ for some $g \in G$. By Remark 30.3(iv), $[g, G] \leq \mathrm{O}_{3'}(G)$ and g can be chosen such that x is conjugate to gx^{-1} in G and $[x, g] = 1$. Then $x = gx^{-1}$ by the assumption of the theorem, and it follows that $[x, G] \leq \mathrm{O}_{3'}(G)$. It remains to prove part (i).

30.4 Remark. Let R be a complete discrete valuation ring of characteristic 0, and let π be a prime element of R. Suppose that $R/\pi R$ has prime characteristic p, and let $v(p)$ be the ramification index of p in R, i.e., $p = \pi^{v(p)}$. The order RG is said to be of finite (infinite) representation type if the number of non-isomorphic indecomposable RG-lattices is finite (infinite). Let G be a p-group. By [67], RG is of infinite representation type except when G is cyclic of order p or p^2; even in these cases, moreover, RG is of infinite representation type unless $v(p)$ is small (see [32]).

We will be interested in the case $R = \mathbb{Z}_3[\zeta]$, ζ a primitive 3rd root of unity, and $G = C_3$ of order 3. Then RC_3 is of finite representation type, and there are 9 isomorphism classes of indecomposable RC_3-lattices (see [31, 3.2]). It is easily seen that the following matrices of order 3 give rise to 9 pair-wise non-isomorphic indecomposable RC_3-lattices.

$$1.\ \begin{bmatrix}1\end{bmatrix} \quad 2.\ \begin{bmatrix}\zeta\end{bmatrix} \quad 3.\ \begin{bmatrix}\zeta^2\end{bmatrix} \quad 4.\ \begin{bmatrix}1 & 0\\ 1 & \zeta\end{bmatrix} \quad 5.\ \begin{bmatrix}1 & 0\\ 1 & \zeta^2\end{bmatrix} \quad 6.\ \begin{bmatrix}\zeta & 0\\ 1 & \zeta^2\end{bmatrix}$$

$$7.\ \begin{bmatrix}1 & 0 & 0\\ 1 & \zeta & 0\\ 0 & 1 & \zeta^2\end{bmatrix} \quad 8.\ \begin{bmatrix}1 & 0 & 0\\ 1 & \zeta & 0\\ 1 & 0 & \zeta^2\end{bmatrix} \quad 9.\ \begin{bmatrix}1 & 0 & 0\\ 0 & \zeta & 0\\ 1 & 1 & \zeta^2\end{bmatrix}$$

(Let V_n (V_n') be the right (left) RC_3-lattice defined by letting a generator g of C_3 act on rows (columns) via the nth matrix. Clearly $V_i \cong V_j$ if and only if $V_i' \cong V_j'$. The regular representation V_7 contains a trivial submodule W such that V/W is an indecomposable lattice; this distinguishes V_7 from V_8. The same argument distinguishes V_8 from V_9. The lattice V_7' contains a submodule W on which g acts by multiplication with ζ^2 such that V/W is an indecomposable lattice; this distinguishes V_7' from V_9'.)

We will only need the fact that if V is an indecomposable RC_3-lattice of rank ≥ 2, then g (a generator of C_3) acts on V via a matrix of trace zero. This can also be checked by performing elementary transformations on rows and columns (Note that any $X \in \mathrm{GL}_n(R)$ of order 3 is conjugate within $\mathrm{GL}_n(R)$ to a lower triangular matrix.)

From now on, let ζ a primitive 3rd root of unity, and set $R = \mathbb{Z}_3[\zeta]$, $K = \mathbb{Q}_3(\zeta)$. Then each matrix $X \in \mathrm{GL}_n(R)$ with $X^3 = \mathrm{Id}_n$ is conjugate within $\mathrm{GL}_n(R)$ to a block diagonal matrix, the block entries being from the list given in Remark 30.4.

For $M \in \mathrm{Mat}_n(R)$ and $X \in \mathrm{GL}_n(R)$ of order 3 we write

$$\mathrm{Tr}_1^{\langle X\rangle}(M) = M + X^{-1}MX + X^{-2}MX^2,$$

a relative trace map in the usual sense.

The following simple observation is the key lemma to the proof of Theorem 30.1.

30.5 Lemma. *Let $M \in \mathrm{Mat}_n(R)$ and $X \in \mathrm{GL}_n(R)$ of order 3 (for some $n \in \mathbb{N}$), and assume that for some $\omega \in R$,*

$$X + \mathrm{Tr}_1^{\langle X\rangle}(M) \equiv \omega \cdot \mathrm{Id}_n \pmod{3R}.$$

Then the trace of X is an integral multiple of a power of ζ.

Proof. Replacing X by a conjugate of it, if necessary, we can assume that X is a block diagonal matrix, the block entries $X_1, X_2, \dots X_s$ being from the list given in Remark 30.4. Partition M in accordance with this decomposition, i.e., write

$$X = \begin{bmatrix} X_1 & & & 0 \\ & X_2 & & \\ & & \ddots & \\ 0 & & & X_s \end{bmatrix}, \quad M = \begin{bmatrix} M_1 & & & * \\ & M_2 & & \\ & & \ddots & \\ * & & & M_s \end{bmatrix}.$$

Then $X_i + \mathrm{Tr}_1^{\langle X_i \rangle}(M_i) \equiv \omega \cdot \mathrm{Id}_{n_i} \pmod{3R}$ for $1 \le i \le s$, where n_i is the size of the matrix X_i. It follows that $\mathrm{trace}(X_i) \equiv n_i\omega \pmod{3R}$ for all i. In particular $\mathrm{trace}(X_i) \equiv \mathrm{trace}(X_j) \pmod{3R}$ if X_i and X_j are of the same size. By direct inspection, it follows that all blocks of dimension 1, as well as all blocks of dimension 2, are equal (if there are any). Assume that there are blocks of both dimensions, for example $[\,\zeta^m\,]$ for some $m \in \mathbb{N}$, and $\left[\begin{smallmatrix} 1 & 0 \\ 1 & \zeta \end{smallmatrix}\right]$. Then $\zeta^m \equiv \omega \pmod{3R}$ and $1+\zeta \equiv 2\omega \pmod{3R}$, so $1+\zeta \equiv 2\zeta^m \pmod{3R}$, which forces $\zeta^m = \zeta^2$; finally note that $\mathrm{trace}\left(\left[\begin{smallmatrix} 1 & 0 \\ 1 & \zeta \end{smallmatrix}\right]\right) = -\zeta^2$. One can deal similarly with the other cases, which shows that the contribution of the blocks of dimension 1 and 2 to the trace of X is is an integral multiple of a power of ζ. This concludes the proof since blocks of dimension 3 have trace zero, and there are no other blocks. □

Let $L = \mathbb{Q}_3(\theta)$, where θ is a primitive $|G|$th root of unity, and let $\mathcal{O}$ be the ring of integers in L over $\mathbb{Z}_3$. Then L is a splitting field for G, and each irreducible L-representation can be realized over $\mathcal{O}$. Since R is a principal ideal domain, $\mathcal{O}$ is a free R-module of rank $m := [L : K]$. Thus for $n \in \mathbb{N}$, we have an embedding $\iota : \mathrm{Mat}_n(\mathcal{O}) \hookrightarrow \mathrm{Mat}_{nm}(R)$ such that

$$\mathrm{trace}(\iota(M)) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\mathrm{trace}(M)) \qquad \text{for } M \in \mathrm{Mat}_n(\mathcal{O}).$$

Now let x be an element of order 3 in G which commutes with none of its other conjugates; equivalently, $C_x \in x + \mathrm{Tr}_1^{\langle x \rangle}(\mathbb{Z}G)$. Let $\rho : G \to \mathrm{Mat}_n(\mathcal{O})$ be an irreducible representation of G affording the character $\chi \in \mathrm{Irr}_0^{(p)}(G)$. Then $\rho(x) + \mathrm{Tr}_1^{\langle \rho(x) \rangle}(M) = \omega_\chi(C_x) \cdot \mathrm{Id}_n$ for some $M \in \mathrm{Mat}_n(\mathcal{O})$. Note that $\omega_\chi(C_x) \in R$. Thus for an embedding ι as above, we have $\iota\rho(x) + \mathrm{Tr}_1^{\langle \iota\rho(x) \rangle}(\iota(M)) = \omega_\chi(C_x) \cdot \mathrm{Id}_{nm}$, and we can apply Lemma 30.5 to conclude that the trace of $\iota\rho(x)$ is an integral multiple of a power of ζ. Since $\mathrm{trace}(\rho(x)) \in R$, we have $\mathrm{trace}(\iota\rho(x)) = m \cdot \mathrm{trace}(\rho(x)) = m \cdot \chi(x)$. This clearly implies that $\chi(x)$ is an integral multiple of a power of ζ.

Therefore $u_x = e_0 C_x (e_0 C_{x^{-1}})^{-1}$ is a normalized unit of order 3 in the center of $\mathrm{B}_0(\mathbb{Z}_{(p)}G)$, by Remark 30.3. The proof of Theorem 30.1 is complete.

30.6 Remark. We remark that we have shown that $\chi(x)$ is an integral multiple of a power of ζ, for *each* irreducible character $\chi \in \mathrm{Irr}(G)$.

We finish this section with some examples.

30.7 Example. There is at least no obvious reason why a block should not occur. For example, let $X = \left[\begin{smallmatrix} \zeta & 0 \\ 1 & \zeta^2 \end{smallmatrix}\right]$ and $M = \left[\begin{smallmatrix} 1 & -\zeta \\ 0 & 0 \end{smallmatrix}\right]$. Then $X + \mathrm{Tr}_1^{\langle X\rangle}(M) = \mathrm{Id}$. As another example, let

$$X = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \zeta & 0 \\ 1 & 1 & \zeta^2 \end{bmatrix}, \quad M_1 = \begin{bmatrix} \zeta & 0 & -\zeta \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 0 & 0 & \zeta^2 \\ 0 & 0 & 1 \\ 0 & 0 & \zeta^2 \end{bmatrix}.$$

Then we have $X + \mathrm{Tr}_1^{\langle X\rangle}(M_1) = \zeta \cdot \mathrm{Id}$ and $X + \mathrm{Tr}_1^{\langle X\rangle}(M_2) = \zeta^2 \cdot \mathrm{Id}$.

30.8 Example. If in the situation above, χ would be afforded by another representation $\rho' : G \to \mathrm{Mat}_n(\mathcal{O})$ such that $\rho'(x)$ is a diagonal matrix, then $\rho(x)$ would have to be a scalar! In this context, one might think of the following simple examples.

Let $\langle X, Y\rangle$ be the non-abelian group of order 3^3 and exponent 3. An irreducible representation of $\langle X, Y\rangle$ is given by the matrices below.

$$X = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \zeta & 0 \\ 0 & 0 & \zeta^2 \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta \end{bmatrix}.$$

Then $T^{-1}XT = Y$ and $T^{-1}YT = X^{-1}$.

Let

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}; \quad \text{then} \quad T^{-1}AT = \frac{1}{3}\begin{bmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{bmatrix}.$$

Here, $\langle A, X\rangle$ is the alternating group of order 12, and the above matrices give the irreducible representation of degree 3. Any K-equivalent representation exhibiting X as a diagonal matrix is not written over R (however, the representation does not belong to the principal 3-block, as it should be).

30.9 Example. The following example shows that non-principal p-blocks may contain nontrivial central elements of order p. It has been found using GAP [37]. There is a finite group G of order $216 = 2^3 \cdot 3^3$ having Sylow subgroups

$$\langle a, b \mid a^2 = b^4 = 1, b^a = b^{-1}\rangle, \quad \langle x, y \mid x^3 = y^9 = 1, x^y = xy^6\rangle$$

and where the elements a, b, x, y satisfy the relations

$$[a, x] = [b, x] = 1, \quad ya = b^2y, \quad yb = bay^{-1}.$$

We note that G is a complete group, that is, $\mathrm{Z}(G) = 1$ and $\mathrm{Out}(G) = 1$.
A representative system of the conjugacy classes of G is given by

$$\begin{array}{llll}
\mathtt{1a} = 1, & \mathtt{6a} = ax^2y^3, & \mathtt{2a} = a, & \mathtt{3a} = x^2y^3, \\
\mathtt{4a} = ab^{-1}y^5, & \mathtt{6b} = axy^6, & \mathtt{12a} = b^{-1}xy^{-1}, & \mathtt{3b} = xy^6, \\
\mathtt{12b} = ab^{-1}x^2y^2, & \mathtt{2b} = ab, & \mathtt{6c} = abx^2y^6, & \mathtt{9a} = ab^2x^2y^7, \\
\mathtt{6d} = abxy^3, & \mathtt{9b} = b^2xy, & \mathtt{9c} = ab^2y^4, & \mathtt{6e} = ax, \\
\mathtt{6f} = ax^2y^6, & \mathtt{6g} = ay^3, & \mathtt{3c} = y^3. &
\end{array}$$

The character table and the table of central characters $(\omega_\chi(C_g))$ of G is given in Figure VIII.1.

The group ring $\mathbb{Z}_{(3)}G$ has exactly two blocks. The non-principal 3-block B has defect 2, and normal defect group $\mathrm{O}_3(G)$. The characters belonging to B are $\mathtt{X}_i$, $10 \le i \le 18$. The decomposition matrix of B is given by

	$\mathtt{Y}_3$	$\mathtt{Y}_4$
$\mathtt{X}_{10}$	1	.
$\mathtt{X}_{11}$	.	1
$\mathtt{X}_{12}$	1	.
$\mathtt{X}_{13}$	.	1
$\mathtt{X}_{14}$	1	.
$\mathtt{X}_{15}$	.	1
$\mathtt{X}_{16}$	1	1
$\mathtt{X}_{17}$	1	1
$\mathtt{X}_{18}$	1	1

Note that for each irreducible character χ belonging to B, the central character value $[G : \mathrm{C}_G(ax)](\chi(ax)/\chi(1))$ is of the form $-2\zeta^i$. Thus if e denotes the block idempotent belonging to B, then eC_{ax} is a unit in B (see proof of Lemma 30.2), and

$$eC_{ax}(eC_{ax^2y^6})^{-1}$$

is a nontrivial central unit of order 3 in B.

	1a	6a	2a	3a	4a	6b	12a	3b	12b	2b	6c	9a	6d	9b	9c	6e	6f	6g	3c
χ_1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
χ_2	1	1	1	1	−1	1	−1	1	−1	−1	−1	1	−1	1	1	1	1	1	1
χ_3	1	ζ^2	1	ζ^2	1	ζ	ζ	ζ	ζ^2	1	ζ^2	ζ^2	ζ	ζ	1	ζ	ζ^2	1	1
χ_4	1	ζ^2	1	ζ^2	−1	ζ	$-\zeta$	ζ	$-\zeta^2$	−1	$-\zeta^2$	ζ^2	$-\zeta$	ζ	1	ζ	ζ^2	1	1
χ_5	1	ζ	1	ζ	1	ζ^2	ζ^2	ζ^2	ζ	1	ζ	ζ	ζ^2	ζ^2	1	ζ^2	ζ	1	1
χ_6	1	ζ	1	ζ	−1	ζ^2	$-\zeta^2$	ζ^2	$-\zeta$	−1	$-\zeta$	ζ	$-\zeta^2$	ζ^2	1	ζ^2	ζ	1	1
χ_7	2	2	2	2	0	2	0	2	0	0	0	−1	0	−1	−1	2	2	2	2
χ_8	2	2ζ	2	2ζ	0	$2\zeta^2$	0	$2\zeta^2$	0	0	0	$-\zeta$	0	$-\zeta^2$	−1	$2\zeta^2$	2ζ	2	2
χ_9	2	$2\zeta^2$	2	$2\zeta^2$	0	2ζ	0	2ζ	0	0	0	$-\zeta^2$	0	$-\zeta$	−1	2ζ	$2\zeta^2$	2	2
χ_{10}	3	−1	−1	3	−1	−1	−1	3	−1	1	1	0	1	0	0	−1	−1	−1	3
χ_{11}	3	−1	−1	3	1	−1	1	3	1	−1	−1	0	−1	0	0	−1	−1	−1	3
χ_{12}	3	$-\zeta$	−1	3ζ	−1	$-\zeta^2$	$-\zeta^2$	$3\zeta^2$	$-\zeta$	1	ζ	0	ζ^2	0	0	$-\zeta^2$	$-\zeta$	−1	3
χ_{13}	3	$-\zeta$	−1	3ζ	1	$-\zeta^2$	ζ^2	$3\zeta^2$	ζ	−1	$-\zeta$	0	$-\zeta^2$	0	0	$-\zeta^2$	$-\zeta$	−1	3
χ_{14}	3	$-\zeta^2$	−1	$3\zeta^2$	−1	$-\zeta$	$-\zeta$	3ζ	$-\zeta^2$	1	ζ^2	0	ζ	0	0	$-\zeta$	$-\zeta^2$	−1	3
χ_{15}	3	$-\zeta^2$	−1	$3\zeta^2$	1	$-\zeta$	ζ	3ζ	ζ^2	−1	$-\zeta^2$	0	$-\zeta$	0	0	$-\zeta$	$-\zeta^2$	−1	3
χ_{16}	6	4	−2	0	0	4	0	0	0	0	0	0	0	0	0	−2	−2	1	−3
χ_{17}	6	4ζ	−2	0	0	$4\zeta^2$	0	0	0	0	0	0	0	0	0	$-2\zeta^2$	-2ζ	1	−3
χ_{18}	6	$4\zeta^2$	−2	0	0	4ζ	0	0	0	0	0	0	0	0	0	-2ζ	$-2\zeta^2$	1	−3
χ_{19}	6	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	−3	−3

	1a	6a	2a	3a	4a	6b	12a	3b	12b	2b	6c	9a	6d	9b	9c	6e	6f	6g	3c
χ_1	1	3	3	3	18	3	18	3	18	18	18	24	18	24	24	6	6	6	2
χ_2	1	3	3	3	−18	3	−18	3	−18	−18	−18	24	−18	24	24	6	6	6	2
χ_3	1	$3\zeta^2$	3	$3\zeta^2$	18	3ζ	18ζ	3ζ	$18\zeta^2$	18	$18\zeta^2$	$24\zeta^2$	18ζ	24ζ	24	6ζ	$6\zeta^2$	6	2
χ_4	1	$3\zeta^2$	3	$3\zeta^2$	−18	3ζ	-18ζ	3ζ	$-18\zeta^2$	−18	$-18\zeta^2$	$24\zeta^2$	-18ζ	24ζ	24	6ζ	$6\zeta^2$	6	2
χ_5	1	3ζ	3	3ζ	18	$3\zeta^2$	$18\zeta^2$	$3\zeta^2$	18ζ	18	18ζ	24ζ	$18\zeta^2$	$24\zeta^2$	24	$6\zeta^2$	6ζ	6	2
χ_6	1	3ζ	3	3ζ	−18	$3\zeta^2$	$-18\zeta^2$	$3\zeta^2$	-18ζ	−18	-18ζ	24ζ	$-18\zeta^2$	$24\zeta^2$	24	$6\zeta^2$	6ζ	6	2
χ_7	1	3	3	3	0	3	0	3	0	0	0	−12	0	−12	−12	6	6	6	2
χ_8	1	3ζ	3	3ζ	0	$3\zeta^2$	0	$3\zeta^2$	0	0	0	-12ζ	0	$-12\zeta^2$	−12	$6\zeta^2$	6ζ	6	2
χ_9	1	$3\zeta^2$	3	$3\zeta^2$	0	3ζ	0	3ζ	0	0	0	$-12\zeta^2$	0	-12ζ	−12	6ζ	$6\zeta^2$	6	2
χ_{10}	1	−1	−1	3	−6	−1	−6	3	−6	6	6	0	6	0	0	−2	−2	−2	2
χ_{11}	1	−1	−1	3	6	−1	6	3	6	−6	−6	0	−6	0	0	−2	−2	−2	2
χ_{12}	1	$-\zeta$	−1	3ζ	−6	$-\zeta^2$	$-6\zeta^2$	$3\zeta^2$	-6ζ	6	6ζ	0	$6\zeta^2$	0	0	$-2\zeta^2$	-2ζ	−2	2
χ_{13}	1	$-\zeta$	−1	3ζ	6	$-\zeta^2$	$6\zeta^2$	$3\zeta^2$	6ζ	−6	-6ζ	0	$-6\zeta^2$	0	0	$-2\zeta^2$	-2ζ	−2	2
χ_{14}	1	$-\zeta^2$	−1	$3\zeta^2$	−6	$-\zeta$	-6ζ	3ζ	$-6\zeta^2$	6	$6\zeta^2$	0	6ζ	0	0	-2ζ	$-2\zeta^2$	−2	2
χ_{15}	1	$-\zeta^2$	−1	$3\zeta^2$	6	$-\zeta$	6ζ	3ζ	$6\zeta^2$	−6	$-6\zeta^2$	0	-6ζ	0	0	-2ζ	$-2\zeta^2$	−2	2
χ_{16}	1	2	−1	0	0	2	0	0	0	0	0	0	0	0	0	−2	−2	1	−1
χ_{17}	1	2ζ	−1	0	0	$2\zeta^2$	0	0	0	0	0	0	0	0	0	$-2\zeta^2$	-2ζ	1	−1
χ_{18}	1	$2\zeta^2$	−1	0	0	2ζ	0	0	0	0	0	0	0	0	0	-2ζ	$-2\zeta^2$	1	−1
χ_{19}	1	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	−3	−1

Figure VIII.1.: Character table and table of central characters of G

Bibliography

[1] R. Ž. Aleev, *Higman's central unit theory, units of integral group rings of finite cyclic groups and Fibonacci numbers*, Internat. J. Algebra Comput. **4** (1994), no. 3, 309–358. MR 95h:16042 48, 51, 53

[2] S. A. Amitsur, *Finite subgroups of division rings*, Trans. Amer. Math. Soc. **80** (1955), 361–386. MR 17,577c 160, 161, 162, 167, 168, 170, 171

[3] Satya R. Arora, A. W. Hales, and I. B. S. Passi, *Jordan decomposition and hypercentral units in integral group rings*, Comm. Algebra **21** (1993), no. 1, 25–35. MR 93m:20005 145, 146, 147, 150, 157

[4] Satya R. Arora and I. B. S. Passi, *Central height of the unit group of an integral group ring*, Comm. Algebra **21** (1993), no. 10, 3673–3683. MR 95a:20004 145, 146, 150, 152, 164

[5] V. A. Artamonov and A. A. Bovdi, *Integral group rings: groups of invertible elements and classical K-theory*, Algebra. Topology. Geometry, Vol. 27 (Russian), Itogi Nauki i Tekhniki, Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1989, Translated in J. Soviet Math. **57** (1991), no. 2, 2931–2958, pp. 3–43, 232. MR 91e:16028 165

[6] O. D. Artemovich, *Isolated elements of prime order in finite groups*, Ukrain. Mat. Zh. **40** (1988), no. 3, 397–400, 408. MR 90e:20018 173

[7] Reinhold Baer, *Endlichkeitskriterien für Kommutatorgruppen*, Math. Ann. **124** (1952), 161–177. MR 13,622a 129

[8] Garrett Birkhoff, *On the combination of subalgebras*, Proc. Camb. Philos. Soc. **29** (1933), 441–464. 114

[9] ———, *Subdirect unions in universal algebra*, Bull. Amer. Math. Soc. **50** (1944), 764–768. MR 6,33d 114

[10] ———, *Lattice Theory*, American Mathematical Society, New York, N. Y., 1948. MR 10,673a 114

[11] Norman Blackburn, *Finite groups in which the nonnormal subgroups have nontrivial intersection*, J. Algebra **3** (1966), 30–37. MR 32 #7643 146, 147, 148, 149, 154

[12] Peter Floodstrand Blanchard, *Exceptional group ring automorphisms for some metabelian groups. I, II*, Comm. Algebra **25** (1997), no. 9, 2727–2733, 2735–2742. MR 98k:20007 75, 81

[13] ———, *Exceptional group ring automorphisms for groups of order 96*, Comm. Algebra **29** (2001), no. 11, 4823–4830. MR 1 856 917 7, 74, 75, 81

[14] Frauke M. Bleher, Meinolf Geck, and Wolfgang Kimmerle, *Automorphisms of generic Iwahori-Hecke algebras and integral group rings of finite Coxeter groups*, J. Algebra **197** (1997), no. 2, 615–655. MR 99f:20010 7, 64, 65, 70, 71

[15] A. A. Bovdi, *Periodic normal divisors of the multiplicative group of a group-ring*, Siberian Math. J. **9** (1968), no. 3, 374–376. 45, 155, 157, 164, 165

[16] ———, *The periodic normal divisors of the multiplicative group of a group-ring. II.*, Siberian Math. J. **11** (1970), no. 3, 374–388. 12, 146, 150, 155, 156, 157, 158, 159, 160, 161, 164

[17] Victor Bovdi, *On elements in algebras having finite number of conjugates*, Publ. Math. Debrecen **57** (2000), no. 1-2, 231–239. MR 2001i:16058 161

[18] Richard Brauer, *Representations of finite groups*, Lectures on Modern Mathematics, Vol. I, Wiley, New York, 1963, pp. 133–175. MR 31 #2314 1

[19] Michel Broué, *Equivalences of blocks of group algebras*, Finite-dimensional algebras and related topics (Ottawa, ON, 1992), Kluwer Acad. Publ., Dordrecht, 1994, pp. 1–26. MR 97c:20004 173

[20] Kenneth S. Brown, *Cohomology of groups*, Springer-Verlag, New York, 1982. MR 83k:20002 110

[21] R. A. Bryce, *Subdirect product closed Fitting classes*, Bull. Austral. Math. Soc. **33** (1986), no. 1, 75–80. MR 87d:20023 114

[22] R. A. Bryce and John Cossey, *Subdirect product closed Fitting classes*, Proceedings of the Second International Conference on the Theory of Groups (Australian Nat. Univ., Canberra, 1973) (Berlin), Springer, 1974, pp. 158–164. Lecture Notes in Math., Vol. 372. MR 51 #3292 114

[23] R. G. Burn, *Central idempotents in group rings*, Canad. Math. Bull. **13** (1970), 527–528. MR 42 #7794 143, 144

[24] Sônia P. Coelho and César Polcino Milies, *Finite conjugacy in group rings*, Comm. Algebra **19** (1991), no. 3, 981–995. MR 93b:16048 161, 165

[25] Donald B. Coleman, *On the modular group ring of a p-group*, Proc. Amer. Math. Soc. **15** (1964), 511–514. MR 29 #2306 138

[26] Christopher D. H. Cooper, *Power automorphisms of a group*, Math. Z. **107** (1968), 335–356. MR 38 #4550 149, 152, 153, 165

[27] Charles W. Curtis and Irving Reiner, *Methods of representation theory. Vol. II*, John Wiley & Sons Inc., New York, 1987, With applications to finite groups and orders, A Wiley-Interscience Publication. MR 88f:20002 1, 18, 76, 84, 85, 87, 90, 96, 97, 98, 99

[28] ———, *Methods of representation theory. Vol. I*, John Wiley & Sons Inc., New York, 1990, With applications to finite groups and orders, Reprint of the 1981 original, A Wiley-Interscience Publication. MR 90k:20001 1, 18, 19, 59, 90, 97

[29] Everett C. Dade, *Automorphismes extérieurs centralisant tout sousgroupe de Sylow*, Math. Z. **117** (1970), 35–40. MR 43 #7497 110, 121

[30] ———, *Deux groupes finis distincts ayant la même algèbre de groupe sur tout corps*, Math. Z. **119** (1971), 345–348. MR 43 #6329 20

[31] Ernst Dieterich, *Representation types of group rings over complete discrete valuation rings*, Integral representations and applications (Oberwolfach, 1980), Springer, Berlin, 1981, pp. 369–389. MR 83f:20004 176

[32] ———, *Representation types of group rings over complete discrete valuation rings. II*, Orders and their applications (Oberwolfach, 1984), Springer, Berlin, 1985, pp. 112–125. MR 87f:20015 176

[33] M. A. Dokuchaev, S. O. Juriaans, C. Polcino Milies, and M. L. Sobral Singer, *Finite conjugacy in algebras and orders*, Proc. Edinb. Math. Soc. (2) **44** (2001), no. 1, 201–213. MR 1 879 219 161

[34] Daniel R. Farkas and Peter A. Linnell, *Trivial units in group rings*, Canad. Math. Bull. **43** (2000), no. 1, 60–62. MR 2001b:16034 151

[35] Walter Feit, *The representation theory of finite groups*, North-Holland Publishing Co., Amsterdam, 1982. MR 83g:20001 175

[36] A. Fröhlich, *The Picard group of noncommutative rings, in particular of orders*, Trans. Amer. Math. Soc. **180** (1973), 1–45. MR 47 #6751 18, 76

[37] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.3*, 2002, (http://www.gap-system.org). 72, 107, 108, 178

[38] Antonio Giambruno and Sudarshan K. Sehgal, *Generators of large subgroups of units of integral group rings of nilpotent groups*, J. Algebra **174** (1995), no. 1, 150–156. MR 96j:16033 162

[39] George Glauberman, *Central elements in core-free groups*, J. Algebra **4** (1966), 403–420. MR 34 #2681 173

[40] ———, *On the automorphism groups of a finite group having no non-identity normal subgroups of odd order*, Math. Z. **93** (1966), 154–160. MR 33 #2713 107

[41] K. R. Goodearl, *Surjective endomorphisms of finitely generated modules*, Comm. Algebra **15** (1987), no. 3, 589–609. MR 88d:16010 4

[42] Ju. M. Gorčakov, *Gruppy s konechnymi klassami sopryazhennykh elementov*, "Nauka", Moscow, 1978, Sovremennaya Algebra. [Modern Algebra Series]. MR 80b:20001 114

[43] Daniel Gorenstein, Richard Lyons, and Ronald Solomon, *The classification of the finite simple groups. Number 3. Part I. Chapter A*, American Mathematical Society, Providence, RI, 1998, Almost simple K-groups. MR 98j:20011 109, 173

[44] Fletcher Gross, *Automorphisms which centralize a Sylow p-subgroup*, J. Algebra **77** (1982), no. 1, 202–233. MR 83i:20020 106, 119, 141

[45] Jean Guérindon, *Décomposition canonique d'un module artinien*, C. R. Acad. Sci. Paris Sér. A-B **286** (1978), no. 20, A867–A869. MR 81e:16019 4

[46] Robert M. Guralnick and Susan Montgomery, *On invertible bimodules and automorphisms of noncommutative rings*, Trans. Amer. Math. Soc. **341** (1994), no. 2, 917–937. MR 94d:16027 76

[47] Robert M. Guralnick and Geoffrey R. Robinson, *On extensions of the Baer-Suzuki theorem*, Israel J. Math. **82** (1993), no. 1-3, 281–297. MR 94i:20034 173

[48] William H. Gustafson and Klaus W. Roggenkamp, *A Mayer-Vietoris sequence for Picard groups, with applications to integral group rings of dihedral and quaternion groups*, Illinois J. Math. **32** (1988), no. 3, 375–406. MR 90a:11145 76

[49] Helmut Hasse, *Verallgemeinerung des Dualitätssatzes für die Charaktere endlicher abelscher Gruppen auf beliebige endliche Gruppen*, Math. Nachr. **3** (1949), 1–3. MR 11,495c 46

[50] Hermann Heineken and Hans Liebeck, *The occurrence of finite groups in the automorphism group of nilpotent groups of class* 2, Arch. Math. (Basel) **25** (1974), 8–16. MR 50 #2337 33

[51] I. N. Herstein, *Conjugates in division rings*, Proc. Amer. Math. Soc. **7** (1956), 1021–1022. MR 18,557d 160

[52] ———, *A counterexample in Noetherian rings*, Proc. Nat. Acad. Sci. U.S.A. **54** (1965), 1036–1037. MR 32 #5692 4

[53] ———, *Rings with involution*, The University of Chicago Press, Chicago, Ill.-London, 1976, Chicago Lectures in Mathematics. MR 56 #406 160

[54] Martin Hertweck, *Eine Lösung des Isomorphieproblems für ganzzahlige Gruppenringe von endlichen Gruppen*, Ph.D. thesis, University of Stuttgart, 1998, ISBN 3-8265-6055-8. 20, 21, 61, 102

[55] ———, *Another counterexample to a conjecture of Zassenhaus*, to appear in Beiträge zur Algebra und Geometrie (Contributions to Algebra and Geometry), 2001. 75

[56] ———, *Class-preserving automorphisms of finite groups*, J. Algebra **241** (2001), no. 1, 1–26. MR 2002e:20047 64, 102, 105, 131

[57] ———, *A counterexample to the isomorphism problem for integral group rings*, Ann. of Math. (2) **154** (2001), no. 1, 115–138. MR 2002e:20010 16, 20, 21, 23, 25, 26, 27, 32, 33, 74

[58] ———, *Local analysis of the normalizer problem*, J. Pure Appl. Algebra **163** (2001), no. 3, 259–276. MR 1 852 119 20, 45, 131

[59] ———, *Class-preserving Coleman automorphisms of finite groups*, Monatsh. Math. **136** (2002), no. 1, 1–7. MR 1 908 076 102

[60] ———, *Integral group ring automorphisms without Zassenhaus factorization*, Illinois J. Math. **46** (2002), no. 1, 233–245. MR 2003i:20009 60, 62, 75, 80, 92, 95

[61] Martin Hertweck and Wolfgang Kimmerle, *Coleman automorphisms of finite groups*, Math. Z. **242** (2002), no. 2, 203–215. MR 1 980 619 9, 20, 105, 106, 111, 121, 139, 141

[62] ———, *On principal blocks of p-constrained groups*, Proc. London Math. Soc. (3) **84** (2002), no. 1, 179–193. MR 1 863 399 39, 90

[63] Martin Hertweck and Gabriele Nebe, *On group ring automorphisms*, to appear in Algebr. Represent. Theory. 65

[64] I. Hughes and K. R. Pearson, *The group of units of the integral group ring ZS_3*, Canad. Math. Bull. **15** (1972), 529–534. MR 48 #4089 92

[65] B. Huppert, *Endliche Gruppen. I*, Springer-Verlag, Berlin, 1967. MR 37 #302 38, 41, 108, 112, 131, 132, 133, 136, 139, 140, 152

[66] Stefan Jackowski and Zbigniew Marciniak, *Group automorphisms inducing the identity map on cohomology*, J. Pure Appl. Algebra **44** (1987), no. 1-3, 241–250. MR 88b:20085 20, 45, 127, 136, 138, 139, 147, 151

[67] H. Jacobinski, *Sur les ordres commutatifs avec un nombre fini de réseaux indécomposables*, Acta Math. **118** (1967), 1–31. MR 35 #2876 176

[68] ———, *Über die Geschlechter von Gittern über Ordnungen*, J. Reine Angew. Math. **230** (1968), 29–39. MR 37 #5250 17

[69] E. Jespers and S. O. Juriaans, *Isomorphisms of integral group rings of infinite groups*, J. Algebra **223** (2000), no. 1, 171–189. MR 2000k:16032 143

[70] E. Jespers and S. O. Juriaans, *The finite conjugacy centre of the unit group of orders in algebras*, earlier (submitted) version of [71], 2001. 11, 14, 134, 135, 160, 161, 164, 165, 167

[71] ———, *The finite conjugacy centre of the unit group of integral group rings*, J. Group Theory **6** (2003), no. 1, 93–102. 14, 164, 186

[72] E. Jespers, S. O. Juriaans, J. M. de Miranda, and J. R. Rogerio, *On the normalizer problem*, J. Algebra **247** (2002), no. 1, 24–36. MR 1 873 381 3, 11, 12, 20, 126, 134, 136, 137, 139, 141, 142

[73] E. Jespers and M. M. Parmenter, *Bicyclic units in $\mathbf{Z}S_3$*, Bull. Soc. Math. Belg. Sér. B **44** (1992), no. 2, 141–146. MR 95j:16035 92, 99

[74] E. Jespers, M. M. Parmenter, and S. K. Sehgal, *Central units of integral group rings of nilpotent groups*, Proc. Amer. Math. Soc. **124** (1996), no. 4, 1007–1012. MR 96g:16044 11, 134, 141

[75] Gregory Karpilovsky, *The Schur multiplier*, The Clarendon Press Oxford University Press, New York, 1987. MR 93j:20002 111

[76] ———, *Unit groups of group rings*, Longman Scientific & Technical, Harlow, 1989. MR 91h:16001 16, 135, 159

[77] Otto H. Kegel and Bertram A. F. Wehrfritz, *Locally finite groups*, North-Holland Publishing Co., Amsterdam, 1973, North-Holland Mathematical Library, Vol. 3. MR 57 #9848 141

[78] E. I. Khukhro, *Nilpotent subdirect products*, Sibirsk. Mat. Zh. **23** (1982), no. 6, 178–180, 207. MR 84f:20038 114

[79] W. Kimmerle, *Class sums of p-elements*, [121, pp. 117–124]. 39

[80] W. Kimmerle and K. W. Roggenkamp, *Projective limits of group rings*, J. Pure Appl. Algebra **88** (1993), no. 1-3, 119–142. MR 94f:20008 22, 38, 102, 114, 116, 117, 118, 120

[81] Wolfgang Kimmerle, *Beiträge zur ganzzahligen Darstellungstheorie endlicher Gruppen*, Bayreuth. Math. Schr. (1991), no. 36, 139. MR 92h:20011 17, 40, 103

[82] Lee Klingler, *Construction of a counterexample to a conjecture of Zassenhaus*, Comm. Algebra **19** (1991), no. 8, 2303–2330. MR 92i:20004 75

[83] M. Künzer and H. Weber, *On the cyclotomic Dedekind embedding and the cyclic Wedderburn embedding*, to appear in Algebr. Represent. Theory. 52

[84] T. Y. Lam and K. H. Leung, *On vanishing sums of roots of unity*, J. Algebra **224** (2000), no. 1, 91–109. MR 2001f:11135 48, 53, 54, 55, 57

[85] Serge Lang, *Algebra*, third ed., Addison-Wesley Publishing Company, Reading, MA, 1993. 46

[86] Yuanlin Li, *The hypercentre and the n-centre of the unit group of an integral group ring*, Canad. J. Math. **50** (1998), no. 2, 401–411. MR 99f:16034 3, 145, 147, 150, 161, 164

[87] Yuanlin Li and M. M. Parmenter, *Hypercentral units in integral group rings*, Proc. Amer. Math. Soc. **129** (2001), no. 8, 2235–2238 (electronic). MR 1 823 905 3, 145, 147, 160, 161, 163, 164

[88] Yuanlin Li, S. K. Sehgal, and M. M. Parmenter, *On the normalizer property for integral group rings*, Comm. Algebra **27** (1999), no. 9, 4217–4223. MR 2000h:20010 147, 149

[89] F. Loonstra, *Über subdirekte Produkte von Gruppen*, Rend. Mat. e Appl. (5) **21** (1962), 364–372. MR 27 #1514 114

[90] Z. Marciniak, J. Ritter, S. K. Sehgal, and A. Weiss, *Torsion units in integral group rings of some metabelian groups. II*, J. Number Theory **25** (1987), no. 3, 340–352. MR 88k:20019 45

[91] Marcin Mazur, *Automorphisms of finite groups*, Comm. Algebra **22** (1994), no. 15, 6259–6271. MR 95i:20036 20, 102

[92] ———, *On the isomorphism problem for infinite group rings*, Exposition. Math. **13** (1995), no. 5, 433–445. MR 96k:20007 12, 16, 20, 21, 102, 144

[93] ———, *The normalizer of a group in the unit group of its group ring*, J. Algebra **212** (1999), no. 1, 175–189. MR 2000a:16058 3, 11, 45, 127, 128, 129, 130, 131, 132, 135, 136, 139, 151

[94] S. Montgomery, *A generalized Picard group for prime rings*, Topics in algebra, Part 1 (Warsaw, 1988), Banach Center Publ., vol. 26, PWN, Warsaw, 1990, pp. 55–63. MR 93g:16026 76

[95] Władysław Narkiewicz, *Elementary and analytic theory of algebraic numbers*, PWN—Polish Scientific Publishers, Warsaw, 1974, Monografie Matematyczne, Tom 57. MR 50 #268 44, 158

[96] Olaf Neisse and Sudarshan K. Sehgal, *Gauss units in integral group rings*, J. Algebra **204** (1998), no. 2, 588–596. MR 99e:16040 162

[97] Aurora Olivieri and Ángel del Río, *Bicyclic units of* $\mathbb{Z}S_n$, Proc. Amer. Math. Soc. **131** (2003), no. 6, 1649–1653 (electronic). MR 2003k:16045 99

[98] M. M. Parmenter, *Conjugates of units in integral group rings*, Comm. Algebra **23** (1995), no. 14, 5503–5507. MR 96m:16047 146, 156

[99] ———, *Central units in integral group rings*, Algebra, Birkhäuser, Basel, 1999, pp. 111–116. MR 2000d:16047 147

[100] Donald S. Passman, *The algebraic structure of group rings*, Wiley-Interscience [John Wiley & Sons], New York, 1977, Pure and Applied Mathematics. MR 81d:16001 127, 130, 144

[101] Gary L. Peterson, *Automorphisms of the integral group ring of* S_n, Proc. Amer. Math. Soc. **59** (1976), no. 1, 14–18. MR 54 #385 71

[102] Thierry Petit Lobão and César Polcino Milies, *The normalizer property for integral group rings of Frobenius groups*, J. Algebra **256** (2002), no. 1, 1–6. MR 2003g:16033 141

[103] Martin R. Pettet, *On inner automorphisms of finite groups*, Proc. Amer. Math. Soc. **106** (1989), no. 1, 87–90. MR 90a:20042 33, 124

[104] K. I. Pimenov and A. V. Yakovlev, *Artinian modules over a matrix ring*, Infinite length modules (Bielefeld, 1998), Trends Math., Birkhäuser, Basel, 2000, pp. 101–105. MR 2001j:16031 4

[105] César Polcino Milies and Sudarshan K. Sehgal, *FC-elements in a group ring*, Comm. Algebra **9** (1981), no. 12, 1285–1293. MR 82i:16013 161

[106] I. Reiner, *Maximal orders*, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1975, London Mathematical Society Monographs, No. 5. MR 52 #13910 18, 19, 162

[107] Robert Remak, *Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produkte*, J. Reine Angew. Math. **163** (1930), 1–44. 113

[108] ———, *Über minimale invariante Untergruppen in der Theorie der endlichen Gruppen*, J. Reine Angew. Math. **162** (1930), 1–16. 113

[109] ———, *Über die erzeugenden invarianten Untergruppen der subdirekten Darstellungen endlicher Gruppen*, J. Reine Angew. Math. **164** (1931), 197–242. 113

[110] ———, *Über Untergruppen direkter Produkte von drei Faktoren*, J. Reine Angew. Math. **166** (1931), 65–100. 113

[111] Claus Michael Ringel, *Infinite length modules. Some examples as introduction*, Infinite length modules (Bielefeld, 1998), Trends Math., Birkhäuser, Basel, 2000, pp. 1–73. MR 2002d:16002 4

[112] ———, *Algebra at the turn of the century*, Southeast Asian Bull. Math. **25** (2001), no. 1, 147–160. MR 2002c:01044 4

[113] Derek J. S. Robinson, *A course in the theory of groups*, second ed., Springer-Verlag, New York, 1996. MR 96f:20001 147, 151

[114] Geoffrey R. Robinson, *Remarks on coherence and the Reynolds isometry*, J. Algebra **88** (1984), no. 2, 489–501. MR 85m:20011 3, 173

[115] ———, *The Z_p^*-theorem and units in blocks*, J. Algebra **134** (1990), no. 2, 353–355. MR 91m:20019 3, 15, 173, 174

[116] K. W. Roggenkamp, *From Dedekind's group determinant to the isomorphism problem*, C. R. Math. Acad. Sci. Soc. R. Can. **21** (1999), no. 4, 97–126. MR 2000h:20014 76

[117] K. W. Roggenkamp and L. L. Scott, *On a conjecture of Zassenhaus for finite group rings*, manuscript, November 1988. 2, 18, 48, 59, 74, 75, 102, 117

[118] K. W. Roggenkamp and A. Zimmermann, *On the isomorphism problem for integral group rings of finite groups*, Arch. Math. (Basel) **59** (1992), no. 6, 534–544. MR 94a:20014 38

[119] Klaus Roggenkamp and Leonard Scott, *Isomorphisms of p-adic group rings*, Ann. of Math. (2) **126** (1987), no. 3, 593–647. MR 89b:20021 17, 18, 19, 38, 39, 40, 84, 90

[120] Klaus W. Roggenkamp, *Problems on group rings*, Trends in ring theory (Miskolc, 1996), Amer. Math. Soc., Providence, RI, 1998, pp. 173–186. MR 1 491 924 76

[121] Klaus W. Roggenkamp and Martin J. Taylor, *Group rings and class groups*, Birkhäuser Verlag, Basel, 1992. MR 92m:20008 76, 187

[122] Klaus W. Roggenkamp and Alexander Zimmermann, *Outer group automorphisms may become inner in the integral group ring*, J. Pure Appl. Algebra **103** (1995), no. 1, 91–99. MR 97b:20004 20, 74

[123] Chih-han Sah, *Automorphisms of finite groups*, J. Algebra **10** (1968), 47–68. MR 37 #5287 109

[124] A. I. Saksonov, *Group rings of finite groups. I*, Publ. Math. Debrecen **18** (1971), 187–209 (1972). MR 46 #5425 138

[125] Robert Sandling, *The isomorphism problem for group rings: a survey*, Orders and their applications (Oberwolfach, 1984), Lecture Notes in Math., vol. 1142, Springer, Berlin, 1985, pp. 256–288. MR 87b:20007 45

[126] Peter Schmid, *On the Clifford theory of blocks of characters*, J. Algebra **73** (1981), no. 1, 44–55. MR 83c:20019 119

[127] L. L. Scott, *On a conjecture of Zassenhaus, and beyond*, Proceedings of the International Conference on Algebra, Part 1 (Novosibirsk, 1989) (Providence, RI), Amer. Math. Soc., 1992, pp. 325–343. MR 93g:20010 18, 32, 42, 59, 75, 81

[128] Leonard L. Scott, *Recent progress on the isomorphism problem*, The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986), Amer. Math. Soc., Providence, RI, 1987, pp. 259–273. MR 89c:20015 15, 120

[129] S. K. Sehgal, *Units in integral group rings*, Longman Scientific & Technical, Harlow, 1993, With an appendix by Al Weiss. MR 94m:16039 7, 99, 134, 142, 144, 167

[130] Sudarshan K. Sehgal, *Topics in group rings*, Marcel Dekker Inc., New York, 1978. MR 80j:16001 16, 143, 144, 151, 155, 157

[131] Sudarshan K. Sehgal and Hans Zassenhaus, *On the supercentre of a group and its ring theoretic generalization*, Integral representations and applications (Oberwolfach, 1980), Springer, Berlin, 1981, pp. 117–144. MR 83f:16015 160, 161

[132] Jean-Pierre Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977, Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42. MR 56 #8675 68

[133] G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canadian J. Math. **6** (1954), 274–304. MR 15,600b 64

[134] M. Shirvani and B. A. F. Wehrfritz, *Skew linear groups*, Cambridge University Press, Cambridge, 1986. MR 89h:20001 168

[135] Lance W. Small, *An example in Noetherian rings*, Proc. Nat. Acad. Sci. U.S.A. **54** (1965), 1035–1036. MR 32 #5691 4

[136] Michio Suzuki, *Group theory. I*, Springer-Verlag, Berlin, 1982, Translated from the Japanese by the author. MR 82k:20001c 114

[137] Fernando Szechtman, *n-inner automorphisms of finite groups*, Proc. Amer. Math. Soc. **131** (2003), no. 12, 3657–3664 (electronic). MR 1 998 171 102

[138] Jacques Thévenaz, *Maximal subgroups of direct products*, J. Algebra **198** (1997), no. 2, 352–361. MR 98m:20031 114, 115

[139] K. Varadarajan, *RRF rings which are not LRF*, Proc. Indian Acad. Sci. Math. Sci. **110** (2000), no. 2, 133–136. MR 2001a:16050 4

[140] V. A. Vedernikov, *Subdirect products and formations of finite groups*, Algebra i Logika **29** (1990), no. 5, 523–548, 626, English translation in: Algebra Logic **29** (1990), no. 5, 348–361. MR 93b:20065 114

[141] ———, *Subdirect products of finite groups with Hall π-subgroups*, Mat. Zametki **59** (1996), no. 2, 311–314, in russian; translation in Math. Notes 59 (1996), no. 1-2, 219–221. MR 97b:20019 114

[142] H. N. Ward, *Some results on the group algebra of a group over a prime field*, Seminar in Group Theory, Harvard University, 1960-61, Mimeographed Notes, pp. 13–19. 138

[143] Lawrence C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1982. MR 85g:11001 167

[144] Waterloo Maple Inc., Waterloo · Ontario, Canada, *MAPLE*, (http://www.maplesoft.com). 75, 99, 171

[145] U. H. M. Webb, *The occurrence of groups as automorphisms of nilpotent p-groups*, Arch. Math. (Basel) **37** (1981), no. 6, 481–498. MR 84g:20071 33

[146] Alan Williamson, *On the conjugacy classes in an integral group ring*, Canad. Math. Bull. **21** (1978), no. 4, 491–496. MR 80e:20005 146, 156, 160, 164

[147] Robert Wisbauer, *Grundlagen der Modul- und Ringtheorie*, Verlag Reinhard Fischer, Munich, 1988, Ein Handbuch für Studium und Forschung. [A handbook for study and research]. MR 90e:16001 4

[148] Kenichi Yamauchi, *On automorphisms of a character ring*, Tsukuba J. Math. **20** (1996), no. 2, 525–527. MR 97k:20017 46