Bestimmung von Kompositionsfaktoren endlicher Gruppen aus Burnsideringen und ganzzahligen Gruppenringen

Von der Fakultät Mathematik und Physik
der Universität Stuttgart
zur Erlangung der Würde eines
Doktors der Naturwissenschaften (Dr. rer. nat.)
genehmigte Abhandlung

Vorgelegt von

Christian R. Höfert

geboren in Hardheim

Hauptberichter:	Prof. Dr. Wolfgang Kimmerle
Mitberichter:	PD Dr. Martin Hertweck
	Prof. Dr. Eric Jespers
Tag der mündlichen Prüfung:	13. März 2008

Institut für Geometrie und Topologie der Universität Stuttgart
2008

Inhaltsverzeichnis

English Summary

Preliminaries

Underlying this thesis is the question of how far the structure of a finite group G is determined by special arithmetical properties like order, spectrum or prime graph. At first the main focus lies on the prime graph of the group. The results lead to the question whether the prime graph can be used to study algebraic structures that are derived from the group. Two such structures which will be investigated here are the Burnside ring $\mathsf{B}(\mathsf{G})$ and the integral group ring $\mathbb{Z}\mathsf{G}$ of the group G. In the study of both the prime graph can play a role:

If the Burnside rings of two groups are isomorphic it is well known that the orders and the prime graphs of the groups are identical. During the first part of this thesis it will be shown that additional properties of the common prime graph imply that the composition factors of the involved groups coincide up to isomorphism and permutation.

In the case of the integral group ring $\mathbb{Z}\mathsf{G}$ of G we are interested in another question. Not only for the group G, but also for the group of normalized units $\mathsf{V}(\mathbb{Z}\mathsf{G})$ of $\mathbb{Z}\mathsf{G}$, the prime graph $\Gamma(\mathsf{V}(\mathbb{Z}\mathsf{G}))$ can be defined. Obviously the prime graph $\Gamma(\mathsf{G})$ of G is a subgraph of $\Gamma(\mathsf{V}(\mathbb{Z}\mathsf{G}))$. As a weaker version of a conjecture of H. Zassenhaus one can ask if $\Gamma(\mathsf{V}(\mathbb{Z}\mathsf{G})) = \Gamma(\mathsf{G})$ holds.

This question will be discussed in chapter 2.

The last two chapters deal with finite subgroups in the integral group ring of some special groups.

Chapter 1

In Chapter 1 the prime graph $\Gamma(G)$, also called the Gruenberg–Kegel graph, of a (not necessarily finite) group G is introduced. For an infinite group the prime graph can take any shape, i.e. for each graph Γ whose vertices are labeled by mutually different primes, it is possible to construct a group G with $\Gamma(G) = \Gamma$. In the finite case the situation is different. In particular the number of connected components of the prime graph of a finite group is bounded by 6. The structure of finite groups whose prime graph is disconnected was described by K. W. Gruenberg and O. Kegel (see Satz 1.6).

In case of a solvable finite group the Gruenberg–Kegel theorem states, that the prime graph is either connected, or has two connected components.

Our first aim is to study finite groups with multiply disconnected prime graph, i.e. groups whose prime graph decomposes into at least three connected components. If G is such a group, then G is, by the Gruenberg–Kegel theorem, non-solvable and has a uniquely determined non-abelian composition factor G_0. Moreover G has a maximal nilpotent normal subgroup N, such that the quotient $G' := G/N$ is isomorphic to a subgroup of $\mathrm{Aut}(G_0)$.

By the Feit-Thompson theorem it is clear that the prime 2 must appear as a vertex in the prime graph of a finite non-solvable group. J. S. Williams proved that each connected component of a prime graph not containing the vertex 2 corresponds to a nilpotent $\pi_i(G)$-Hall subgroup of G (see Satz 1.8), where $\pi_i(G)$ is the set of vertices of the respective component.

If G and H are finite groups with identical multiply disconnected prime graph Γ and if furthermore $|G'| = |H'|$, then the orders of the $\pi_i(G)$-Hall subgroups of G and H are equal. The conditions obtained by these equalities are fundamental to the proof of the following proposition:

> **Satz 1.10.** *Let G and H be finite groups such that $\Gamma = \Gamma(G) = \Gamma(H)$ and $|\Gamma| \geqslant 3$. If $|G'| = |H'|$, then $G_0 \cong H_0$. If furthermore $|G| = |H|$ then the composition factors of G and H and their multiplicities are the same up to isomorphism and permutation.*

In order to prove the theorem the first step is to show that the π_i-Hall subgroups are already subgroups of the non-abelian composition factor (see Lemma 1.12). The main part of the proof is based on comparing connected components of the prime graph, respectively the orders of the Hall subgroups induced by the components. For this the classification of the prime graph components of the finite simple groups is essential. This classification was done by J. S. Williams for alternating groups, sporadic simple groups and groups of Lie-type in odd characteristic. For groups of Lie-type in even characteristic this was proved, almost at the same time, by A. S. Kondrat'ev and by N. Iiyori and H. Yamaki. A main element of the proof of the classification is the classification of the finite simple groups.

Note that the simple groups that appear in the first chapter are given in Lie notation, because this is the usual way when dealing with prime graphs. In Chapter 3 and 4 the simple groups are given by their classical names.

In most the cases comparing the orders of the π_i-Hall subgroups involved is sufficient to prove the theorem. If not, the order of G' is used to finish the proof. These cases are highlighted in table 1.1.

The proof is, due to the may calculations needed, technical; the main parts involve only elementary number theory. Difficulty arise since the numerous cases have to deal with differently.

The theorem has an important application to the theory of Burnside rings.

If G and H are groups with isomorphic Burnside rings then one might ask if G and H are isomorphic. In general this is not true: for a group G the table of marks $MT(G)$ stands in a very close relation to the Burnside ring $B(G)$. It is possible to construct the Burnside ring $B(G)$ by using the table of marks $MT(G)$. Therefore for two different groups, isomorphic tables of marks lead to isomorphic Burnside rings. The converse is an open problem.

W. Kimmerle showed that if, for two groups, there exists an isomorphism between their lattices of subgroups that is order- and conjugacy-preserving, then their tables of marks are isomorphic. Already A. Rottlaender had described non-isomorphic groups with identical lattices of subgroups. Thus the tables of marks, and therefore the Burnside rings of these groups are isomorphic.

Although a group is not determined by its table of marks, W. Kimmerle proved, that the table of marks determines the chief factors, and therefore the composition factors of the group up to isomorphism and permutation (see Satz 1.22).

At the moment a similar result for Burnside rings seems to be out of range. It is not even known (although a proof seems to be near, see Satz 1.21) if the Burnside ring $B(G)$ of a non-abelian simple group G determines G.

Satz 1.10 can be used as a first step towards a Burnside ring version of Satz 1.22: If G and H are groups with isomorphic Burnside rings, then the orders and the prime graphs of G and H coincide. If this prime graph is multiply disconnected the groups G and H satisfy all conditions of Satz 1.10 and we get:

> **Satz 1.24.** *Let* G *and* H *be finite groups with* $B(G) \cong B(H)$ *and* $|\Gamma| = |\Gamma(G)| = |\Gamma(H)| \geqslant 3$. *Then the composition factors and their multiplicities of* G *and* H *are equal, up to isomorphism and permutation.*

Chapter 2

In the second part of the thesis we will concentrate on the integral group ring $\mathbb{Z}G$ of a finite group G. A central point in the studies of integral group rings is the description of the group of normalized units $V(\mathbb{Z}G)$.

The well known conjectures of H. Zassenhaus deal with these normalized units. The conjectures state that elements respectively subgroups of finite order in $V(\mathbb{Z}G)$ are rationally conjugate, i.e. conjugate by an unit of $\mathbb{Q}G$, to elements respectively subgroups of G. Already K. W. Roggenkamp and L. L. Scott gave a counterexample to the conjecture that treats group bases of $\mathbb{Z}G$ (the so-called second Zassenhaus-conjecture (ZC·2)). Therefore the conjecture that states that every finite subgroup of $V(\mathbb{Z}G)$ is rationally conjugate to a subgroup of G (the third conjecture of Zassenhaus (ZC·3)), does also not hold in general. The first Zassenhaus-conjecture (ZC·1) (every torsion element of $V(\mathbb{Z}G)$ is rationally conjugate to an element of G) is still open.

A general approach to (ZC·1) seems to be, until now, very difficult. Therefore especially during recent years, weaker versions of (ZC·1) have been discussed. A question that appears at once and which is unsolved in general is if for any (finite) element order within $V(\mathbb{Z}G)$ there exists an element of the same order in the group G. Weakening this question one might ask if the prime graph of $V(\mathbb{Z}G)$ coincides with the prime graph of G.

The partial augmentations has proven to be a powerful tool when investigating a group with respect to (ZC·1). It is even possible to give an equivalent formulation of (ZC·1) in terms of partial augmentations.

In Chapter 2 partial augmentations are used to prove:

Proposition 2.9. *Let* G *be a finite group with* $\Gamma(G) = \Gamma(V(\mathbb{Z}G))$*, and let*

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

be a short exact sequence of groups. If A *is a* p*-group then*

$$\Gamma(E) = \Gamma(V(\mathbb{Z}E))\,.$$

A direct consequence is, that the prime graph of a solvable group E coincides with $V(\mathbb{Z}E)$. The results obtained in Chapter 2 are joint work with W. Kimmerle.

Meanwhile M. Hertweck proved for solvable E that not only $\Gamma(E)$ coincides with $\Gamma(V(\mathbb{Z}E))$, but furthermore that for each finite order of an element in $V(\mathbb{Z}E)$ there is an element in G of the same order.

Chapter 3

If G is a solvable group we know that the spectra of $V(\mathbb{Z}G)$ and G are the same. If G is solvable we also know that any finite subgroup of $V(\mathbb{Z}G)$ is solvable. In particular any composition factor of a finite subgroup of $V(\mathbb{Z}G)$ is isomorphic to a subgroup of G. If G is not solvable little is known in this direction, i.e. it is not known if any non-abelian composition factor of a subgroup in $V(\mathbb{Z}G)$ appears as a factor of a subgroup of G.

In Chapter 3 we will give a positive answer to this question for minimal-simple groups, i.e. non-abelian simple groups in which every proper subgroup is solvable:

> **Satz 3.3.** *Let G be a finite minimal-simple group and let H be a finite subgroup of $V(\mathbb{Z}G)$ with $|H| < |G|$. Then H is solvable.*

First recall the theorem of S. D. Berman which says that the order of a finite subgroup H of $V(\mathbb{Z}G)$ is a divisor of $|G|$. Therefore it is a consequence of Satz 3.3 that any finite non-solvable subgroup of $V(\mathbb{Z}G)$ is isomorphic to the minimal-simple group G.

The basis of the proof is the classification of the finite minimal-simple groups obtained by J. G. Thompson. According to this classification, every finite minimal-simple group G is isomorphic to one of the following groups (notation as Lie-type groups and as classical groups):

- $A_1(2^p) = PSL(2, 2^p)$, p prime.
- $A_1(3^p) = PSL(2, 3^p)$, p odd and prime.
- $A_1(p) = PSL(2, p)$, $p \neq 3$ prime and $p^2 + 1 \equiv 0 \bmod 5$.
- $A_2(3) = PSL(3, 3)$.
- ${}^2B_2(2^p) = Sz(2^p)$, $p \geqslant 3$ prime.

(Note that the group $PSL(3, 3)$ is the only group above whose prime graph is not multiply-disconnected).

The proof of Satz 3.3 starts by analyzing the structure of a smallest counterexample $H \leqslant V(\mathbb{Z}G)$. At first the structure of such a counterexample $H \leqslant V(\mathbb{Z}G)$ is analysed. We will see that H has a solvable normal subgroup such that the quotient $H_0 := H/A$ is also minimal-simple, so the proof can be carried out by ruling out any "smaller" minimal-simple group as a possible quotient of a finite subgroup of $V(\mathbb{Z}G)$. Therefore all possible types of G will be compared with the possible types of H_0.

Figure 3.1 gives a schematical overview of which method is used to rule out H_0 as a section of a finite subgroup of $V(\mathbb{Z}G)$:

The first method that is used to exclude H_0 as a possible factor of a finite subgroup in $V(\mathbb{Z}G)$ is the checking of the conditions the Berman-theorem gives. E.g. the fact, that the Suzuki-groups $Sz(2^p)$ are the only simple groups whose order is not divisible by 3 shows immediately, that G being a Suzuki-group requires H_0 to be a Suzuki-group too.

The next step is to use the latest results by W. Kimmerle and M. Hertweck, who proved, that

the integral group ring of a finite group G contains an elementary abelian group of prime-power order if and only if G contains such a group. In this context it is important that the subgroups of $\mathsf{PSL}(2, p^f)$ are known by a theorem of L. E. Dickson.

Applying these two methods, we know that for both G and H_0 must be of the form $\mathsf{PSL}(2, *)$. Due to several results obtained by R. Wagner and M. Hertweck a lot is known about the units in the corresponding integral group ring. In particular it is known for many torsion elements of $V(\mathbb{Z}G)$ that they are rationally conjugate to elements of G. This fact allows the counting of conjugacy classes. For some prime divisors r of $|H_0|$ we can show, that the number of conjugacy classes whose elements have order r must be equal or greater than the number of such classes in G. Such an argument for example is used to rule out the group $H_0 = \mathsf{PSL}(2, r)$ with $r \geqslant 7$ prime as a section in $V(\mathbb{Z}G)$ with $G = \mathsf{PSL}(2, 2^p)$: If $V(\mathbb{Z}G)$ contains elements of order r, then these elements are rationally conjugate to elements of G. Furthermore G contains more than two conjugacy classes with elements of order r, but in H_0 there are only two such classes.

Considerations like this can solve all open cases except the situation where $G = \mathsf{PSL}(2, q)$ with q prime and $H_0 = \mathsf{PSL}(2, 2^p)$ with p prime. All previous methods fail. A solution can be found by using characters: an ordinary irreducible character χ of G can be extended to a character of $V(\mathbb{Z}G)$, and then restricted to a character $\chi\big|_H$ of the subgroup H. So the standard scalar product $\langle \cdot, \cdot \rangle$ on the space of class functions of H must take on the characters $\chi\big|_H$ and $\psi \in \mathrm{Irr}(H)$, an integral non-negative value.

This condition can be checked using the generic character tables of the groups $\mathsf{PSL}(n, p^f)$. When doing this it is important to know the character values for each element of H. Therefore knowledge about the units in the integral group ring of $\mathsf{PSL}(n, p^f)$ is essential. In particular the character χ must be chosen in such a way that all character values are known. Namely, if (ZC·1) is not verified for $\mathbb{Z}G$, the character values of an element in $V(\mathbb{Z}G)$ are only given in terms of partial augmentations.

Using suitable characters, we can prove:

> **Proposition 3.11.** *Let be* $G = \mathsf{PSL}(2, p^f)$. *Then every finite abelian 2-subgroup of* $V(\mathbb{Z}G)$ *is isomorphic to a subgroup of* G. *If p=2 then this is true for any finite 2-subgroup.*

With elementary theory of p-groups we can conclude easily:

> **Korollar 3.12.** *Let be* $G = \mathsf{PSL}(2, p^f)$ *with* $p \neq 2$ *and* $S \leqslant V(\mathbb{Z}G)$ *a finite 2-group. Then* $S \leqslant D_4$ *or every abelian normal subgroup of* S *is cyclic. Particularly* S *contains a cyclic normal subgroup of index 2.*

All in all the case $G \cong \mathsf{PSL}(2, q)$ with q prime and $H_0 \cong \mathsf{PSL}(2, 2^p)$ with p prime is impossible, because for $p \neq 3$ the Sylow 2-subgroups of H_0 are generated by at least three elements, contradicting Korollar 3.12.

Chapter 4

In the final Chapter finite subgroups in the integral group ring of $\mathsf{PSL}(2, \mathfrak{p}^{\mathsf{f}})$ will be investigated more thoroughly. Therefore we fix $\mathsf{G} = \mathsf{PSL}(2, \mathfrak{p}^{\mathsf{f}})$.

We start with the investigation of finite 2-groups in $\mathsf{V}(\mathbb{Z}\mathsf{G})$. Proposition 3.11 states that any finite abelian 2-subgroup of $\mathsf{V}(\mathbb{Z}\mathsf{G})$ is isomorphic to a subgroup of G. We will now prove that this is also true for non-abelian 2-subgroups.

The main problem is to show that the quaternion group Q_8 of order 8 does not appear as a subgroup within $\mathsf{V}(\mathbb{Z}\mathsf{G})$. This will be done in Proposition 4.1.

The idea of the proof is that the irreducible 4-dimensional representation of Q_8 over the reals splits into two 2-dimensional representation if the real representation is considered as an ordinary representation. So each complex Q_8-representation that can be realised over the reals must contain pairs of the ordinary irreducible 2-dimensional representation, if it contains this representation at all.

For a suitable ordinary representation of G we can show that it contains, considered as a representation of a putative quaternion subgroup of $\mathsf{V}(\mathbb{Z}\mathsf{G})$, an odd number of copies of the irreducible 2-dimensional representation. Using the Frobenius-Schur-indicator of this representation we can show that it can be realised over the reals. But this is a contradiction to the observations above. Thus the quaternion group can not appear as a subgroup of $\mathsf{V}(\mathbb{Z}\mathsf{G})$.

I'd like to thank Martin Hertweck, who gave the crucial idea for the proof - the usage of real representations.

Now we know, that the quaternion group does not appear within $\mathsf{V}(\mathbb{Z}\mathsf{G})$ and we can prove:

> **Proposition 4.2.** *If* $\mathsf{G} = \mathsf{PSL}(2, \mathfrak{p}^{\mathsf{f}})$*, than every finite 2-subgroup* $\mathsf{H} \leqslant \mathsf{V}(\mathbb{Z}\mathsf{G})$ *is isomorphic to a subgroup of* G*.*

This knowledge can be used in the cases $\mathfrak{p} = 2$ or $\mathfrak{p}^{\mathsf{f}} \equiv 3, 5 \bmod 8$, i.e. the cases in which the 2-Sylow subgroups of G are abelian, to show that every non-solvable subgroup of $\mathsf{V}(\mathbb{Z}\mathsf{G})$ has a uniquely determined non-abelian composition factor, which is isomorphic to a subgroup of G (see Proposition 4.3). This result can be considered as a first generalization of the results in Chapter 3.

The methods already used in chapter 3 can be used to show that if $\mathsf{f} = 1$ then every finite group $\mathsf{H} \leqslant \mathsf{V}(\mathbb{Z}\mathsf{G})$ whose order is divisible by $\mathfrak{p}$ is isomorphic to a subgroup of G (see Proposition 4.4).

Although these results require strong restrictions on G they have nice applications when G is small.

The last two sections will give:

> **Satz 4.5.** *If* $\mathsf{G} = \mathsf{PSL}(2, 7)$ *then every finite subgroup of* $\mathsf{V}(\mathbb{Z}\mathsf{G})$ *is rationally conjugate to a subgroup of* G*.*

and

Proposition 4.8. *If* $\mathsf{G} = \mathsf{PSL}(2,11)$ *or* $\mathsf{G} = \mathsf{PSL}(2,13)$ *then every finite subgroup of* $\mathsf{V}(\mathbb{Z}\mathsf{G})$ *is isomorphic to a subgroup of* G.

The second proposition is easily proved by considering all possible minimal normal subgroups of a finite group $\mathsf{H} \leqslant \mathsf{V}(\mathbb{Z}\mathsf{G})$. Therefore it is important that the orders of the groups $\mathsf{PSL}(2,11)$ and $\mathsf{PSL}(2,13)$ are not divisible by 8. So the isomorphism classes of finite 2-subgroups in $\mathsf{V}(\mathbb{Z}\mathsf{G})$ are already known.

For Satz 4.5, i.e. $\mathsf{G} = \mathsf{PSL}(2,7)$, the proof of the isomorphism of a subgroup H in $\mathsf{V}(\mathbb{Z}\mathsf{G})$ to a subgroup of G is again base on a case-by-case differentiation of possible minimal normal subgroups of H.

The proof that all subgroups are not only isomorphic, but also rationally conjugate, to subgroups of G uses the character table of G and a lemma (Lemma 4.7) that associates the fact of rational conjugacy of subgroups with character values of the subgroup's elements. This finishes the proof.

So the group $\mathsf{PSL}(2,7)$ is, besides the alternating group $\mathsf{A}_5 \cong \mathsf{PSL}(2,5) \cong \mathsf{PSL}(2,2^2)$, the second non-abelian simple group for which the third conjecture of Zassenhaus ($\mathsf{ZC}{\cdot}3$) is verified.

Einleitung und Zusammenfassung

Einleitung

Ausgangspunkt dieser Arbeit ist die Frage, inwieweit die Struktur einer endlichen Gruppe G durch spezielle arithmetische Eigenschaften, wie z.B. Ordnung, Spektrum und Primgraph, festgelegt ist. Dabei liegt das Hauptaugenmerk zunächst auf dem Primgraphen der Gruppe. Aus dieser Betrachtung entwickelt sich dann die Frage, inwieweit der Primgraph der Gruppe dazu verwendet werden kann, algebraische Strukturen zu untersuchen, die aus der Gruppe G abgeleitet werden können. Zwei solcher Strukturen, die in dieser Arbeit betrachtet werden, sind der Burnsidering $\mathsf{B}(\mathsf{G})$ der Gruppe G und ihr ganzzahliger Gruppenring $\mathbb{Z}\mathsf{G}$. Bei der Untersuchung beider Strukturen spielt der Primgraph von G eine Rolle:

Bei Gruppen mit isomorphen Burnsideringen ist bekannt, dass sie identische Primgraphen und Ordnungen besitzen. Im ersten Teil der Arbeit wird gezeigt, dass aus gewissen zusätzlichen Eigenschaften des gemeinsamen Primgraphs folgt, dass die Kompositionsfaktoren der Gruppen übereinstimmen.

Beim ganzzahligen Gruppenring $\mathbb{Z}\mathsf{G}$ von G ist eine andere Frage interessant. Für die normierten Einheiten $\mathsf{V}(\mathbb{Z}\mathsf{G})$ von $\mathbb{Z}\mathsf{G}$ kann wie für G der Primgraph $\Gamma(\mathsf{V}(\mathbb{Z}\mathsf{G}))$ definiert werden. Der Primgraph $\Gamma(\mathsf{G})$ von G ist dann ein Teilgraph von $\Gamma(\mathsf{V}(\mathbb{Z}\mathsf{G}))$. Als schwächere Version einer Vermutung von H. Zassenhaus stellt sich dann die Frage ob $\Gamma(\mathsf{V}(\mathbb{Z}\mathsf{G})) = \Gamma(\mathsf{G})$ gilt.

Diese Frage wird im zweiten Kapitel diskutiert.

In den letzten beiden Kapiteln werden dann endliche Untergruppen im ganzzahligen Gruppenring spezieller Gruppen untersucht.

Kapitel 1

Im ersten Kapitel wird zunächst der Primgraph $\Gamma(G)$, auch Gruenberg–Kegel-Graph genannt, einer (nicht notwendigerweise endlichen) Gruppe G eingeführt. Der Primgraph einer unendlichen Gruppe kann jede beliebige Gestalt annehmen, d.h. zu jedem Graphen Γ, dessen Ecken mit paarweise verschiedenen Primzahlen identifiziert sind, lässt sich eine Gruppe G angeben mit $\Gamma(G) = \Gamma$. Im Fall einer endlichen Gruppe ist das nicht so. Insbesondere ist die Anzahl der Zusammenhangskomponenten des Primgraphen im endlichen Fall auf 6 beschränkt. Die Struktur von endlichen Gruppen mit zerfallendem Primgraphen wurde von K. W. Gruenberg und O. Kegel bestimmt (Satz 1.6).

Für endliche auflösbare Gruppen gilt nach dem Satz von Gruenberg und Kegel sogar, dass der Primgraph entweder zusammenhängend ist oder aber aus zwei Zusammenhangskomponenten besteht.

Erstes Ziel ist die Untersuchung von endlichen Gruppen mit mehrfach zerfallendem Primgraphen, d.h. Primgraphen mit mehr als zwei Zusammenhangskomponenten. Ist G eine solche Gruppe, dann ist G nach Gruenberg und Kegel nicht auflösbar, und besitzt einen eindeutig bestimmten nicht-abelschen Kompositionsfaktor G_0. Außerdem besitzt G einen maximalen nilpotenten Normalteiler N und der Quotient $G' := G/N$ ist isomorph zu einer Untergruppe von $\mathrm{Aut}(G_0)$.

Nach dem Satz von Feit-Thompson ist die Primzahl 2 eine Ecke des Primgraphen von endlichen nicht-auflösbaren Gruppen. Von J. S. Williams wurde gezeigt, dass jede Primgraphkomponente, die die Ecke 2 nicht enthält, mit einer nilpotenten $\pi_i(G)$-Hall-Untergruppe der Gruppe G korrespondiert (Satz 1.8), wobei $\pi_i(G)$ für die Menge der Ecken der jeweiligen Primgraphkomponente steht.

Sind nun G und H endliche Gruppen mit identischem mehrfach zerfallendem Primgraphen Γ und gilt $|G'| = |H'|$, dann stimmen insbesondere die Ordnungen der oben erwähnten π_i-Hallgruppen von G und H überein. Diese Gleichheit und die daraus gewonnenen Bedingungen tragen wesentlich zum Beweis der folgenden Proposition bei.

> **Satz 1.10.** *Seien G und H endliche Gruppen mit $\Gamma = \Gamma(G) = \Gamma(H)$ und $|\Gamma| \geqslant 3$. Gilt $|G'| = |H'|$, dann ist $G_0 \cong H_0$. Ist außerdem $|G| = |H|$, dann besitzen G und H die gleichen Kompositionsfaktoren, inklusive ihrer Multiplizitäten.*

Um die Satz zu beweisen, wird zunächst gezeigt, dass die π_i-Hallgruppen bereits im nicht-abelschen Kompositionsfaktor auftauchen (Lemma 1.12). Die Hauptarbeit beim Beweis beruht dann auf dem Vergleich der Primgraphkomponenten, bzw. der Ordnungen der von den Komponenten induzierten Hallgruppen. Hierbei geht wesentlich die Klassifikation der Primgraphkomponenten der endlichen einfachen Gruppen ein. Diese wurde von J. S. Williams für die alternierenden Gruppen, die sporadisch-einfachen Gruppen und Gruppen vom Lietyp in ungerader Charakteristik angegeben. Für Gruppen vom Lietyp in Charakteristik 2 wurde die Klassifikation einerseits von A. S. Kondrat'ev und andererseits von N. Iiyori und H. Yamaki

parallel gefunden. In allen Fällen geht maßgeblich die Klassifikation der endlichen einfachen Gruppen ein. Es sei hier erwähnt, dass die im ersten Kapitel auftretenden einfachen Gruppen in der Lie-Notation angegeben sind, da dies der üblichen Notation in der Literatur über Primgraphen entspricht. In den Kapiteln 3 und 4 werden einfache Gruppen dann mit ihren klassischen Namen benannt.

In den meisten Fällen ist der Vergleich der Ordnungen der involvierten π_i-Hallgruppen ausreichend, um den Satz zu beweisen. Ist das nicht der Fall, so werden die Ordnungen von G' und H' zu Hilfe genommen. In Tabelle 1.1 sind diese Fälle speziell gekennzeichnet.

Der Beweis gestaltet sich insgesamt durch eine Vielzahl von Rechnungen sehr technisch, verwendet aber hauptsächlich elementare Zahlentheorie. Die Schwierigkeit liegt dabei in der Vielzahl der Fälle, die oft verschiedene Arten der Betrachtungen erfordern.

Eine wichtige Folgerung der Proposition liefert die Anwendung auf Burnsideringe.

Sind G und H Gruppen mit isomorphen Burnsideringen, dann stellt sich die Frage, ob auch G und H isomorph sind. Im Allgemeinen ist dies nicht wahr: In engem Zusammenhang mit dem Burnsidering $\mathsf{B}(\mathsf{G})$ einer Gruppe steht die Markentafel $\mathsf{MT}(\mathsf{G})$. Die Markentafel $\mathsf{MT}(\mathsf{G})$ einer Gruppe G kann zur Konstruktion des Burnsiderings $\mathsf{B}(\mathsf{G})$ verwendet werden. Die Isomorphie der Marktentafeln der Gruppen G und H liefert demnach auch einen Isomorphismus der Burnsideringe. Die Umkehrung ist ein offenes Problem.

W. Kimmerle konnte zeigen, dass ein ordnungs- und konjugationserhaltender Verbandsisomorphismus der Untergruppenverbände zweier Gruppen isomorphe Markentafeln, und demnach auch isomorphe Burnsideringe impliziert. Bereits von A. Rottlaender wurden aber nichtisomorphe Gruppen mit identischen Untergruppenverbänden beschrieben, also nicht-isomorphe Gruppen mit isomorphen Burnsideringen.

Die Markentafel einer Gruppe bestimmt die Gruppe also nicht bis auf Isomorphie. W. Kimmerle zeigte aber, dass sie deren Haupt- und Kompositionsfaktoren bis auf Permutation festlegt (s. Satz 1.22).

Für Burnsideringe ist man bislang weit von einem solchen Resultat entfernt. Bisher ist noch nicht einmal bewiesen (auch wenn man dem Beweis wohl recht nahe ist, s. Satz 1.21), ob der Burnsidering einer einfachen Gruppe diese bis auf Isomorphie bestimmt.

Satz 1.10 kann dazu verwendet werden, einen ersten Schritt in Richtung von Satz 1.22 für Burnsideringe zu machen: Sind G und H Gruppen mit isomorphen Burnsideringen, dann stimmen auch ihre Primgraphen überein. Ist dieser gemeinsame Primgraph mehrfach zerfallend, dann erfüllen G und H die Voraussetzungen von Satz 1.10 und man erhält:

> **Satz 1.24.** *Seien* G *und* H *endliche Gruppen mit* $\mathsf{B}(\mathsf{G}) \cong \mathsf{B}(\mathsf{H})$ *und* $|\Gamma| = |\Gamma(\mathsf{G})| = |\Gamma(\mathsf{H})| \geqslant 3$. *Dann besitzen* G *und* H *die gleichen Kompositionsfaktoren, inklusive deren Vielfachheiten.*

Kapitel 2

Der zweite Teil der Arbeit konzentriert sich auf den ganzzahligen Gruppenring $\mathbb{Z}G$ einer endlichen Gruppe G. Eine zentrale Frage beim Studium des Rings $\mathbb{Z}G$ ist die Beschreibung der Einheitengruppe $\mathcal{U}(\mathbb{Z}G)$, bzw. ohne Einschränkung, die Beschreibung der Gruppe der normierten Einheiten $\mathcal{V}(\mathbb{Z}G)$.

Mit der Gruppe $\mathcal{V}(\mathbb{Z}G)$ beschäftigen sich die bekannten Vermutungen von H. Zassenhaus, die besagen, dass Elemente und Untergruppen endlicher Ordnung von $\mathcal{V}(\mathbb{Z}G)$ jeweils zu Elementen und Untergruppen von G rational, d.h. in $\mathbb{Q}G$, konjugiert sind. Die Vermutungen, dass jede Gruppenbasis (zweite Vermutung von Zassenhaus ($\mathcal{ZC}$·2)) und jede endliche Untergruppe (dritte Vermutung von Zassenhaus ($\mathcal{ZC}$·3)) von $\mathcal{V}(\mathbb{Z}G)$ rational zu einer Untergruppe von G konjugiert ist, wurde von K. W. Roggenkamp und L. L. Scott widerlegt. Die erste Zassenhaus-Vermutung ($\mathcal{ZC}$·1), dass jedes Element endlicher Ordnung aus $\mathcal{V}(\mathbb{Z}G)$ rational zu einem Gruppenelement konjugiert ist, ist immer noch offen.

Da sich der allgemeine Zugang zu ($\mathcal{ZC}$·1) bisher schwierig gestaltet, werden, speziell in jüngster Zeit, schwächere Formulierungen von ($\mathcal{ZC}$·1) untersucht. Eine Frage, die sich unmittelbar stellt und im Allgemeinen unbeantwortet ist, ist die, ob es zu jeder in $\mathcal{V}(\mathbb{Z}G)$ vorkommenden Elementordnung ein Element entsprechender Ordnung in der Gruppe G gibt. Schwächt man dies weiter ab, so taucht in natürlicher Weise die Frage auf, ob der Primgraph von G mit dem von $\mathcal{V}(\mathbb{Z}G)$ übereinstimmt.

Bei der Untersuchung einer Gruppe hinsichtlich ($\mathcal{ZC}$·1), haben sich in der Vergangenheit die partiellen Augmentationen als sehr hilfreich erwiesen, da mit ihrer Hilfe eine äquivalente Formulierung von ($\mathcal{ZC}$·1) möglich ist.

In Kapitel 2 werden partiellen Augmentationen maßgeblich dazu beitragen, die folgende Proposition zu beweisen.

Proposition 2.9. *Es sei G eine endliche Gruppe mit $\Gamma(G) = \Gamma(\mathcal{V}(\mathbb{Z}G))$ und*

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

eine kurze exakte Sequenz von Gruppen. Ist A eine $\mathfrak{p}$-Gruppe, dann ist

$$\Gamma(E) = \Gamma(\mathcal{V}(\mathbb{Z}E))\,.$$

Als Konsequenz erhält man unmittelbar, dass der Primgraph einer auflösbaren Gruppe E mit dem von $\mathcal{V}(\mathbb{Z}E)$ übereinstimmt. Die Ergebnisse in Kapitel 2 entstanden aus gemeinsamer Arbeit mit W. Kimmerle.

In der Zwischenzeit wurde von M. Hertweck gezeigt, dass für auflösbares E nicht nur $\Gamma(E)$ und $\Gamma(\mathcal{V}(\mathbb{Z}E))$ übereinstimmen, sondern dass sogar für jede in $\mathcal{V}(\mathbb{Z}E)$ auftretende (endliche) Elementordnung ein Element gleicher Ordnung in E existiert.

Kapitel 3

Im Falle einer auflösbaren Gruppe G weiß man also, dass das Spektrum von $V(\mathbb{Z}G)$ mit dem von G übereinstimmt. Es ist in diesem Fall auch bekannt, dass jede endliche Untergruppe von $V(\mathbb{Z}G)$ wiederum auflösbar ist. Insbesondere ist also jeder Kompositionsfaktor einer endlichen Untergruppe von $V(\mathbb{Z}G)$ isomorph zu einem Kompositionsfaktor einer Untergruppe von G. Ist G nicht-auflösbar, so weiß man nicht, ob jeder nicht-auflösbare Kompositionsfaktor einer endlichen Untergruppe von $V(\mathbb{Z}G)$ auch als Kompositionsfaktor einer Untergruppe von G auftritt.

In Kapitel 3 wird diese Frage für die minimal-einfachen Gruppen beantwortet, d.h. Gruppen, die keine echten nicht-auflösbaren Untergruppen enthalten. Es wird gezeigt:

> **Satz 3.3.** *Ist G eine endliche, minimal-einfache Gruppe und H eine endliche Untergruppe von $V(\mathbb{Z}G)$ mit $|H| < |G|$, dann ist H auflösbar.*

Zunächst sei an den Satz von S. D. Berman erinnert, nachdem die Ordnung einer endlichen Untergruppe H von $V(\mathbb{Z}G)$ die Ordnung von G teilt. Satz 3.3 zeigt also insbesondere, dass jede endliche nicht-auflösbare Untergruppe von $V(\mathbb{Z}G)$ isomorph zur minimal-einfachen Gruppe G ist.

Grundlage für den Beweis ist die von J. G. Thompson bewiesene Klassifikation der minimal-einfachen Gruppen. Danach ist jedes minimal-einfache G isomorph zu einer der folgenden Gruppen (in Lie-Notation und klassischer Notation):

- $A_1(2^p) = PSL(2, 2^p)$, mit p prim.
- $A_1(3^p) = PSL(2, 3^p)$, mit p ungerade und prim.
- $A_1(p) = PSL(2, p)$, mit $p \neq 3$ prim und $p^2 + 1 \equiv 0 \bmod 5$.
- $A_2(3) = PSL(3, 3)$.
- ${}^2B_2(2^p) = Sz(2^p)$, mit $p \geqslant 3$ prim.

(Man beachte, dass die Gruppe $PSL(3, 3)$ die einzige der obigen Gruppen ist, deren Primgraph nicht mehrfach zerfällt.)

Der Beweis von Satz 3.3 wird dann mit der Methode des kleinsten Verbrechers geführt. Zunächst wird die Struktur eines kleinsten Gegenbeispiels $H \leqslant V(\mathbb{Z}G)$ untersucht. Es zeigt sich, dass H einen auflösbaren Normalteiler A besitzt, so dass der Quotient $H_0 := H/A$ ebenfalls minimal-einfach ist. Es müssen also lediglich alle „kleineren“ minimal-einfachen Gruppen H_0 als Sektion einer Untergruppe von $V(\mathbb{Z}G)$ ausgeschlossen werden. Dafür werden alle möglichen Typen von G mit allen möglichen Typen H_0 verglichen.

In Abbildung 3.1 ist schematisch dargestellt, mit welcher Methode ein jeweiliges H_0 als Sektion in $V(\mathbb{Z}G)$ ausgeschlossen wird.

Zum Ausschluss von H_0 als Sektion in $V(\mathbb{Z}G)$ werden zunächst die Bedingungen geprüft, die der Satz von Berman liefert. So kann z.B. aufgrund der Tatsache, dass die Ordnung einer

Suzukigruppe $\mathsf{Sz}(2^p)$ nicht von 3 geteilt wird, und dass die Suzukigruppen die einzigen nicht-abelschen einfachen Gruppen mit dieser Eigenschaft sind, unmittelbar gefolgert werden, dass mit G auch H_0 eine Suzukigruppe sein muss.

Der nächste Schritt ist die Verwendung neuerer Resultate von W. Kimmerle und M. Hertweck, die zeigen, dass es im ganzzahligen Gruppenring einer endlichen Gruppe G genau dann elementar-abelsche Untergruppen von Primzahlquadrat-Ordnung gibt, wenn es solche Gruppen auch in G gibt. Dabei nutzt man aus, dass man insbesondere die Untergruppen von $\mathsf{PSL}(n, p^f)$ nach dem Satz von L. E. Dickson genau kennt.

Verwendet man diese beiden ersten Methoden, so kann man sowohl G als auch H_0 auf den Typ $\mathsf{PSL}(2, *)$ einschränkten. Durch Ergebnisse von R. Wagner und M. Hertweck ist in diesen Fällen einiges über die Einheiten in $\mathsf{V}(\mathbb{Z}G)$ bekannt. Insbesondere weiß man für viele Elemente von Primzahlordnung, dass sie rational zu Gruppenelementen konjugiert sind. Diese Tatsache ermöglicht das Zählen von Konjugiertenklassen. Es stellt sich für manche Primzahlen r heraus, dass H_0 mindestens soviele Konjugiertenklassen mit Elementen der Ordnung r besitzen muss wie G. Auf diese Art lässt sich z.B. $H_0 = \mathsf{PSL}(2, r)$ mit primem $r \geqslant 7$ als Sektion in $\mathsf{V}(\mathbb{Z}G)$ mit $G = \mathsf{PSL}(2, 2^p)$ ausschließen: Wenn es in $\mathsf{V}(\mathbb{Z}G)$ Elemente der Ordnung r gibt, dann sind diese jeweils rational zu Elementen aus G konjugiert. Außerdem gibt es dann in G mehr als zwei Konjugiertenklassen mit Elementen der Ordnung r. In H_0 existieren aber nur zwei solcher Klassen.

Nach Betrachtungen dieser Art verbleibt der Fall $G \cong \mathsf{PSL}(2, q)$ mit primem q und $H_0 \cong \mathsf{PSL}(2, 2^p)$ mit primem p. Hier versagen die bislang erwähnten Methoden. Abhilfe schafft die Verwendung von Charakteren: Ein gewöhnlicher irreduzibler Charakter χ von G kann zu einem Charakter von $\mathsf{V}(\mathbb{Z}G)$ erweitert und dann wiederum auf die Untergruppe H eingeschränkt werden. Das Standardskalarprodukt $\langle \cdot, \cdot \rangle$ auf dem Raum der Klassenfunktionen von H muss also, ausgewertet an den Charakteren $\chi\big|_H$ und $\psi \in \mathrm{Irr}(H)$, einen nicht-negativen ganzzahligen Wert annehmen.

Diese Bedingung kann mit Hilfe der generischen Charaktertafeln der Gruppen $\mathsf{PSL}(n, p^f)$ überprüft werden. Dabei ist es aber wichtig, dass man die Charakterwerte für die einzelnen Elemente von H kennt. Auch hier ist also das bekannte Wissen über den ganzzahligen Gruppenring von $\mathsf{PSL}(n, p^f)$ entscheidend. Insbesondere ist der Charakter χ von G so zu wählen, dass möglichst alle Charakterwerte auf H bekannt sind. Ist nämlich für die Gruppe G die Vermutung (ZC·1) nicht verifiziert, dann kann der Charakterwert für ein Element aus $\mathsf{V}(\mathbb{Z}G)$ in der Regel nur in Abhängigkeit seiner partiellen Augmentationen angegeben werden.

Verwendet man nun geeignete Charaktere, dann kann man zeigen:

> **Proposition 3.11.** *Ist $G = \mathsf{PSL}(2, p^f)$, dann ist jede endliche abelsche 2-Untergruppe von $\mathsf{V}(\mathbb{Z}G)$ isomorph zu einer Untergruppe von G. Ist p=2, dann gilt das für jede 2-Untergruppe.*

Aus dieser Proposition kann man dann mit elementarer Theorie von p-Gruppen leicht folgern:

> **Korollar 3.12.** *Ist* $G = PSL(2, p^f)$ *mit* $p \neq 2$ *und* $S \leqslant V(\mathbb{Z}G)$ *eine endliche 2-Gruppe, dann ist* $S \leqslant D_4$ *oder aber jeder abelsche Normalteiler von* S *ist zyklisch. In jedem Fall enthält* S *einen zyklischen Normalteiler vom Index 2.*

Der Fall $G \cong PSL(2, q)$ mit primem q und $H_0 \cong PSL(2, 2^p)$ scheidet somit auch aus, da für $p \geqslant 3$ die 2-Sylowgruppen von H_0 von mindestens 3 Elementen erzeugt werden, was im Widerspuch zu Korollar 3.12 steht.

Kapitel 4

Im abschließenden Kapitel 4 werden die endlichen Untergruppen ganzzahliger Gruppenringe der Gruppen $PSL(2, p^f)$ noch genauer untersucht. Im Folgenden ist stets $G = PSL(2, p^f)$.

Zunächst sind die endlichen 2-Untergruppen in $V(\mathbb{Z}G)$ von Interesse. In Proposition 3.11 wurde gezeigt, dass sich die abelschen endlichen 2-Untergruppen von $V(\mathbb{Z}G)$, bis auf Isomorphie, nicht von denen von G unterscheiden. Es wird nun gezeigt, dass das auch für nicht-abelsche 2-Gruppen gilt.

Die Hauptschwierigkeit dabei ist zu zeigen, dass die Quaternionengruppe Q_8 der Ordnung 8 nicht als Untergruppe von $V(\mathbb{Z}G)$ auftritt. Dies wird in Proposition 4.1 bewiesen.

Die Idee dabei ist, dass die irreduzible 4-dimensionale reelle Darstellung von Q_8 über $\mathbb{C}$ in zwei 2-dimensionale Darstellungen zerfällt. In einer komplexen Q_8-Darstellung, die reell realisierbar ist, muss die irreduzible 2-dimensionale gewöhnliche Darstellung daher, wenn überhaupt, paarweise auftreten. Von einer geeigneten gewöhnlichen Darstellung von G kann man zeigen, dass sie, eingeschränkt auf eine potentielle Quaternionengruppe in $V(\mathbb{Z}G)$, eine ungerade Anzahl von Kopien der irreduziblen 2-dimensionalen Darstellung enthält. Mit Hilfe des Frobenius-Schur-Indikators der Darstellung sieht man, dass sie reell realisierbar ist. Das steht aber im Widerspruch zur obigen Überlegung. Die Quaternionengruppe scheidet demnach als mögliche Untergruppe von $V(\mathbb{Z}G)$ aus.

Die entscheidende Idee - die Verwendung reeller Darstellungen - erhielt ich von Martin Hertweck. Ich möchte ihm dafür herzlich danken.

Da man nun weiß, dass die Quaternionengruppe nicht in $V(\mathbb{Z}G)$ auftaucht, kann man zeigen:

> **Proposition 4.2.** *Ist* $G = PSL(2, p^f)$*, dann ist jede endliche 2-Gruppe* $H \leqslant V(\mathbb{Z}G)$ *isomorph zu einer Untergruppe von* G*.*

Dieses Wissen kann man nun dazu verwenden, um in den Fällen $p = 2$ oder $p^f \equiv 3, 5 \bmod 8$, also den Fällen in denen die 2-Sylowgruppen von G abelsch sind, zu zeigen, dass jede nicht-auflösbare Untergruppe von $V(\mathbb{Z}G)$ einen eindeutig bestimmten nicht-abelschen Kompositionsfaktor besitzt, der zu einer Untergruppe von G isomorph ist (Proposition 4.3). Dieses Resultat kann als erste Verallgemeinerung der Ergebnisse aus Kapitel 3 angesehen werden.

Die Methoden aus Kapitel 3 können auch dazu verwendet werden, zu zeigen, dass im Falle $\mathsf{f} = 1$ jede endliche Gruppe $\mathsf{H} \leqslant \mathsf{V}(\mathbb{Z}\mathsf{G})$ deren Ordnung von p geteilt wird, isomorph zu einer Untergruppe von G ist (Proposition 4.4).

Obwohl dieses Ergebnis sehr einschränkende Forderungen an die Gruppe G stellt, kann es dennoch dazu verwendet werden, für „kleine“ G weiterführende Resultate zu erzielen.

In den beiden letzten Abschnitten wird bewiesen:

> **Satz 4.5.** *Ist* $\mathsf{G} = \mathsf{PSL}(2,7)$*, dann ist jede endliche Untergruppe von* $\mathsf{V}(\mathbb{Z}\mathsf{G})$ *rational zu einer Untergruppe von* G *konjugiert.*

und

> **Proposition 4.8.** *Ist* $\mathsf{G} = \mathsf{PSL}(2,11)$ *oder* $\mathsf{G} = \mathsf{PSL}(2,13)$*, dann ist jede endliche Untergruppe in* $\mathsf{V}(\mathbb{Z}\mathsf{G})$ *isomorph zu einer Untergruppe von* G*.*

Die letzte Proposition ergibt sich relativ schnell, indem man eine Fallunterscheidung nach den möglichen minimalen Normalteilern einer endlichen Untergruppe $\mathsf{H} \leqslant \mathsf{V}(\mathbb{Z}\mathsf{G})$ durchführt. Dabei ist zu beachten, dass die Ordnungen der Gruppen $\mathsf{PSL}(2,11)$ und $\mathsf{PSL}(2,13)$ nicht von 8 geteilt werden, man also die möglichen 2-Untergruppen bereits kennt.

Für Satz 4.5 beruht der Beweis der Isomorphie von endlichen Untergruppen von $\mathsf{V}(\mathbb{Z}\mathsf{G})$ mit Untergruppen von G wiederum auf einer Fallunterscheidung aller möglichen minimalen Normalteiler solcher Untergruppen.

Der Beweis der rationalen Konjugiertheit verwendet dann die Charaktertafel von G und ein Lemma (Lemma 4.7), das die rationale Konjugiertheit mit Charakterwerten verbindet.

Damit ist die Gruppe $\mathsf{PSL}(2,7)$, nach der alternierenden Gruppe $\mathsf{A}_5 \cong \mathsf{PSL}(2,5) \cong \mathsf{PSL}(2,2^2)$ die zweite nicht-abelsche einfache Gruppe, für die die dritte Zassenhausvermutung verifiziert wurde.

Danksagung

Zuallererst möchte ich mich bei Herrn Prof. Dr. Wolfgang Kimmerle herzlich bedanken. Ich danke ihm für die sehr gute Betreuung, die er mir vor und während meiner Zeit als Doktorand zukommen ließ und für die vielen Diskussionen und Anregungen. Ich danke ihm auch für den Freiraum zum selbstständigen Arbeiten und nicht zuletzt für viele motivierende Worte.

Herrn PD Dr. Martin Hertweck danke ich für die vielen konstruktiven Gespräche und Hinweise, die mir geholfen haben, die Arbeit abzurunden. Außerdem danke ich ihm für die Erstellung des Gutachtens.

Auch Herrn Prof. Dr. Eric Jespers danke ich für seine Bereitschaft, die vorliegende Arbeit zu begutachten.

Den Mitarbeitern am Lehrstuhl für Geometrie und Topologie sowie dem Team von Mathematik Online danke ich für die angenehme Arbeitsatmosphäre.

Meinen Eltern danke ich für die umfassende Unterstützung während meines Studiums.

Danke Steffi!

KAPITEL 1

Kompositionsfaktoren von endlichen Gruppen mit mehrfach zerfallendem Primgraphen

In diesem ersten Kapitel sollen endliche Gruppen mit mehrfach zerfallendem Primgraphen untersucht werden. Die Ergebnisse werden dann auf die Theorie der Burnsideringe angewendet. Es wird sich zeigen, dass der Burnsidering einer Gruppe mit mehrfach zerfallendem Primgraphen die Kompositionsfaktoren der Gruppe festgelegt.

1.1 Allgemeines über Primgraphen

Definition 1.1. Es sei $n \in \mathbb{N} \setminus \{0\}$ und X eine beliebige, nicht notwendigerweise endliche Gruppe.

- Die Menge aller Primteiler von n wird mit $\pi(n) := \{p \text{ prim } ; \ p \mid n\}$ bezeichnet. Für die Gruppe X setzt man $\pi(X) := \{p \text{ prim } ; \text{ in } X \text{ existiert ein Element der Ordnung } p\}$. Ist X endlich, dann ist also $\pi(X) = \pi(|X|)$.
- Für eine Primzahl p wird die größte p-Potenz, die n teilt, wie folgt notiert:

$$p^a \,\|\, n \iff p^a \mid n \text{ und } p^{a+1} \nmid n\,.$$

Definition 1.2. Der Primgraph, oder auch Gruenberg–Kegel–Graph, $\Gamma(G)$ einer Gruppe G ist der ungerichtete schleifenfreie Graph, der als Eckenmenge die Menge $\pi(G)$ besitzt, und bei dem es zwischen zwei verschiedenen Ecken p und q genau dann eine Kante gibt, wenn es in G ein Element der Ordnung pq gibt. Die Gruppe G muss dabei nicht endlich sein.

Mit $|\Gamma(G)|$ wird die Anzahl der Zusammenhangskomponenten von $\Gamma(G)$ bezeichnet. Besitzt der Primgraph mehr als eine Zusammenhangskomponente, so sagt man, dass der Graph zerfällt. Gilt sogar $|\Gamma(G)| \geqslant 3$, dann nennt man den Graphen mehrfach zerfallend.

Mit $\Gamma_i(G)$ $(i \leqslant 1 \leqslant |\Gamma(G)|)$ werden die Zusammenhangskomponenten von $\Gamma(G)$ benannt. Die Eckenmenge von $\Gamma_i(G)$ wird dann mit $\pi_i(G)$ bezeichnet. Die $\pi_i(G)$ liefern eine disjunkte Zerlegung von $\pi(G)$. Ist $2 \in \pi(G)$, dann wird die Nummerierung der Komponenten von $\Gamma(G)$ so gewählt, dass $2 \in \pi_1(G)$ ist.

Ist G endlich, dann setze man für $1 \leqslant i \leqslant |\Gamma(G)|$

$$\gamma_i(G) := \prod_{\substack{p \in \pi_i(G) \\ p^a \,\|\, |G|}} p^a \,,$$

sowie

$$\gamma_1'(G) := \prod_{i=2}^{|\Gamma(G)|} \gamma_i(G) \,.$$

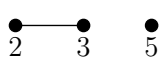
Es gilt dann offensichtlich

$$|G| = \prod_{i=1}^{|\Gamma(G)|} \gamma_i(G) = \gamma_1(G) \cdot \gamma_1'(G) \,.$$

Bemerkung 1.3. Ist S eine Sektion der endlichen Gruppe G, d.h. ein Quotient einer Untergruppe, dann ist $\Gamma(S) \subseteq \Gamma(G)$.

Beispiele 1.4.

- Der Primgraph der symmetrischen Gruppe S_5 ist der folgende zerfallende Graph:

  Der Primgraph $\Gamma(A_5)$ der alternierenden Gruppe A_5 ist sogar mehrfach zerfallend:

- Ist G eine nilpotente Gruppe, dann ist der Primgraph $\Gamma(G)$ der vollständige Graph auf der Eckenmenge $\pi(G)$, d.h. jede Ecke ist mit jeder anderen Ecke durch eine Kante verbunden. Ebenso ist für jede beliebige Gruppe G der Graph $\Gamma(G \times G)$ vollständig auf $\pi(G)$.
- Besitzt die Gruppe G ein nicht-triviales Zentrum $Z(G)$ und gilt $p \,\big|\, |Z(G)|$, dann ist jede Ecke von $\Gamma(G)$ mit p verbunden.

- Die Primgraphen der sporadisch-einfachen Gruppen und ihrer jeweiligen Automorphismengruppe sind in Anhang B dargestellt.
- Die Anzahl der Primgraphkomponenten ist im Allgemeinen nicht begrenzt. Es gilt sogar, dass der Primgraph jede beliebige Gestalt annehmen kann. Sei nämlich Γ ein beliebiger schleifenfreier und ungerichteter Graph, dessen Eckenmenge V aus lauter Primzahlen besteht. Die Kantenmenge E von Γ ist dann $E \subseteq V \times V$. Definiert man eine Menge natürlicher Zahlen $K := \{p \cdot q \ ; \ (p,q) \in E\}$, dann ist das freie Produkt

  $$G = \left(\underset{p \in V}{*} C_p \right) * \left(\underset{k \in K}{*} C_k \right)$$

  eine Gruppe, für die offensichtlich $\Gamma(G) = \Gamma$ gilt. Im Fall einer endlichen Gruppe ist die Anzahl der Primgraphkomponenten jedoch auf 6 beschränkt [60], [43].
- Typische Beispiele für Gruppen mit zerfallendem Primgraphen sind Frobeniusgruppen und 2-Frobeniusgruppen. Eine Gruppe G heißt 2-Frobeniusgruppe, wenn G eine Normalreihe $1 < N < T < G$ besitzt, wobei T eine Frobeniusgruppe mit Kern N und G/N eine Frobeniusgruppe mit Kern T/N ist.

  Ein einfaches Beispiel für eine 2-Frobeniusgruppe ist die Gruppe $G = S_4$. Dabei ist $N = V_4$ und $T = A_4$. Der Primgraph von S_4 besteht aus den beiden isolierten Ecken 2 und 3.

Es gilt sogar

Satz 1.5. *[60, Corollary] Sei G eine endliche, auflösbare Gruppe mit zerfallendem Primgraphen. Dann ist $|\Gamma(G)| = 2$ und G ist eine Frobeniusgruppe oder eine 2-Frobeniusgruppe.*

Auch für eine nicht-auflösbare Frobeniusgruppe G gilt $|\Gamma(G)| = 2$. Ist G eine 2-Frobeniusgruppe, dann ist G, nach den Struktursätzen über Frobeniusgruppen, auflösbar (siehe z.B. [32, V, 8.7]).

Satz 1.5 sowie der folgende Struktursatz über endliche, nicht-auflösbare Gruppen mit zerfallendem Primgraphen wurde von K. W. Gruenberg und O. Kegel bewiesen und erstmals in [60] von J. S. Williams veröffentlicht. Die hier angegebene Formulierung des Struktursatzes ist aus [37] abgeleitet.

Satz 1.6. *[60, Theorem A] Sei G eine endliche, nicht-auflösbare Gruppe mit $|\Gamma(G)| \geqslant 2$. Ist G keine Frobeniusgruppe, dann besitzt G eine Normalreihe der Form*

$$1 \leqslant N < M \leqslant G\,,$$

wobei N ein nilpotenter $\pi_1(G)$-Normalteiler von G ist und M/N eine nicht-abelsche einfache Gruppe. G/M ist eine auflösbare $\pi_1(G)$-Gruppe. Dabei können N und G/M trivial sein. Die Gruppe G/N kann mit einer Gruppe T mit $M/N \leqslant T \leqslant \mathrm{Aut}(M/N)$ identifiziert werden.

Williams zeigte darüber hinaus, dass die Primgraphkomponenten, die 2 nicht als Ecke enthalten, in engem Zusammenhang zu sogenannten isolierten Untergruppen von G stehen.

Definition 1.7. Sei G eine endliche Gruppe und U eine echte Untergruppe von G. Gilt $U^g \cap U \in \{1, U\}$ für jedes $g \in G$, und ist für jedes nicht-triviale Element $u \in U$ der Zentralisator $C_G(u)$ in U enthalten, dann heißt U isoliert in G.

Beispiele für Gruppen mit isolierten Untergruppen sind Frobeniusgruppen. Einerseits ist der Frobeniuskern isoliert, andererseits sind auch die Frobeniuskomplemente isolierte Untergruppen von G.

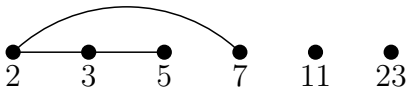
Besitzt die Gruppe G eine isolierte Untergruppe U, dann sind die Elemente in $\pi(U)$ die Ecken einer Zusammenhangskomponente von $\Gamma(G)$ (siehe z.B. [37, Satz 1.3]). Der Primgraph von G zerfällt also in mindestens zwei Komponenten. Ist G nicht auflösbar und gilt $|\Gamma(G)| \geqslant 2$, dann gilt

Satz 1.8. *[60, Theorem 3] Sei G eine nicht-auflösbare endliche Gruppe mit zerfallendem Primgraphen. Dann besitzt G für jedes $i \geqslant 2$ eine isolierte, nilpotente $\pi_i(G)$-Hallgruppe.*

Der folgende Satz von Chigira, Iiyori und Yamaki [11] zeigt, dass die isolierten $\pi_i(G)$-Hallgruppen (mit $i \geqslant 2$) sogar abelsch sind:

Satz 1.9. *Jede nicht-abelsche Sylowgruppe einer endlichen Gruppe gerader Ordnung besitzt mindestens ein Element, das mit einer Involution vertauscht.*

Die Resultate zeigen insbesondere, dass die $\Gamma_i(G)$-Komponenten mit $i \geqslant 2$ jeweils aus vollständigen Graphen bestehen. Für die Komponente $\Gamma_1(G)$ ist dies im Allgemeinen falsch. Es ist nicht einmal die Ecke 2 mit jeder anderen Ecke von $\Gamma_1(G)$ verbunden, wie das Beispiel der Primgraphen der sporadisch-einfachen Matthieu-Gruppe M_{23}

$\Gamma(M_{23}) =$ 

zeigt.

1.2 Endliche Gruppen mit mehrfach zerfallendem Primgraphen

Im vorangegangenen Abschnitt wurde die von Gruenberg, Kegel und Williams gezeigte Klassifikation der Gruppen mit zerfallendem Primgraphen angegeben. Die Resultate zeigen insbesondere, dass eine Gruppe G mit mehrfach zerfallendem Primgraphen genau einen nicht-abelschen einfachen Hauptfaktor besitzt. Dieser Faktor wird im Folgenden mit G_0 bezeichnet. Außerdem besitzt G einen maximalen nilpotenten Normalteiler N, so dass der Quotient $G' := G/N$ isomorph zu einer Gruppe X mit $G_0 \leqslant X \leqslant \mathrm{Aut}(G_0)$ ist. Insbesondere ist also G'/G_0 isomorph zu einer Untergruppe von $\mathrm{Out}(G_0)$.

Ziel ist zunächst der Beweis des folgenden Satzes.

Satz 1.10. *Seien G und H endliche Gruppen mit $\Gamma = \Gamma(G) = \Gamma(H)$ und $|\Gamma| \geqslant 3$. Gilt $|G'| = |H'|$, dann ist $G_0 \cong H_0$. Ist außerdem $|G| = |H|$, dann besitzen G und H die gleichen Kompositionsfaktoren, inklusive ihrer Multiplizitäten.*

Nachdem gezeigt ist, dass unter den Voraussetzungen von Satz 1.10 der nicht-auflösbare Kompositionsfaktor eindeutig bestimmt ist, ist es klar, dass im speziellen Fall $|G| = |H|$ die Kompositionsfaktoren inklusive ihrer Multiplizitäten übereinstimmen.

Der Beweis der Proposition verwendet hauptsächlich die Klassifikation der Primgraphkomponenten von endlichen einfachen Gruppen. Diese Klassifikation wurde von Williams [60] für sporadisch-einfache, alternierende und Gruppen vom Lietyp in ungerader Charakteristik angegeben. Die Primgraphkomponenten der Gruppen vom Lietyp in Charakteristik 2 wurden parallel von Kondrat'ev [43], bzw. Iiyori und Yamaki [35] beschrieben. Die Primgraphkomponenten der sporadisch-einfachen Gruppen sind in Tabelle A.3 angegeben, die Komponenten der einfachen Gruppen mit mehrfach zerfallendem Primgraphen in den Tabellen A.4 und A.5. Nach Satz 1.8 besitzt jede der Gruppen G_0 in den Tabellen A.3 - A.5 für $i \geqslant 2$ eine $\pi_i(G_0)$-Hallgruppe der Ordnung $\gamma_i(G_0)$.

Genauer ist in den Tabellen für $i \geqslant 2$ die Ordnung $\gamma_i(G_0)$ der isolierten $\pi_i(G_0)$-Hallgruppen, sowie $\gamma_1(G_0)$ angegeben. Zur Indizierung der Komponenten siehe Bemerkung 1.13.

In [60], [43] und [35] sind nur die Mengen $\pi_i(G_0)$ von Interesse. Die Tabellen A.3 - A.5 wurden deshalb durch Vergleichen der Tabellen in [60], [43] und [35] mit den in [13] angegebenen Ordnungen von G_0 bestimmt. Es sei erwähnt, dass die Tabellen in [60] einige Notationsfehler enthalten. Diese wurden in den Tabellen A.3 - A.5 korrigiert.

In Tabelle A.3 sind darüber hinaus die Ordnungen der äußeren Automorphismengruppen aufgelistet. Auch diese wurden [13] entnommen.

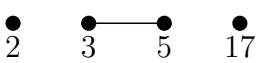
Ist S eine Sektion der Gruppe G, dann wurde schon in Bemerkung 1.3 erwähnt, dass der

Primgraph $\Gamma(S)$ ein Teilgraph von $\Gamma(G)$ ist. Insbesondere ist eine Kante von $\Gamma(S)$ auch eine Kante von $\Gamma(G)$. Zusammenhangskomponenten von $\Gamma(S)$ können aber in $\Gamma(G)$ verschmelzen. Das folgende Lemma zeigt, dass diese Verschmelzung für Kompositionsfaktoren von G nicht willkürlich sein kann.

Lemma 1.11. *Sei G eine endliche nicht-auflösbare Gruppe und $N \trianglelefteq G$. Weiter sei $X = N$ oder $X = G/N$. Sind $\Gamma_i(X)$ und $\Gamma_j(X)$ verschiedene Komponenten von $\Gamma(X)$ mit $\Gamma_i(X) \cup \Gamma_j(X) \subseteq \Gamma_k(G)$ für ein $k \geqslant 1$, dann ist $k = 1$.*

Beweis. Es seien $\Gamma_i(X)$ und $\Gamma_j(X)$ (mit $i, j \neq 1$) zwei verschiedene Komponenten von $\Gamma(X)$ mit $\Gamma_i(X) \cup \Gamma_j(X) \subseteq \Gamma_k(G)$. Angenommen $k \neq 1$, dann besitzt G nach Satz 1.8 eine nilpotente $\pi_k(G)$-Hallgruppe, und damit auch eine nilpotente $\pi_i(X) \cup \pi_j(X)$-Hallgruppe H. Im Fall $X = N$ ist $H \cap X$, und im Fall $X = G/N$ ist HN/N eine nilpotente $\pi_i(X) \cup \pi_j(X)$-Hallgruppe von X (siehe z.B. [32, IV, Hilfssatz 7.2]). In jedem Fall sind also die Komponenten $\Gamma_i(X)$ und $\Gamma_j(X)$ verbunden, im Widerspruch zur Voraussetzung. □

Die Aussage des Lemmas gilt nicht für beliebige Untergruppen oder Sektionen. Ist z.B. $G = A_1(2^4)$ und $U = A_1(2^2) \cong A_5$, dann kann U als Untergruppe von G aufgefasst werden. Für die Primgraphen von G und U gilt aber:

$\Gamma(A_1(2^4)) =$  und $\Gamma(A_1(2^2)) =$ 

Es fusionieren in $\Gamma(G)$ also zwei der Komponenten von $\Gamma(H)$ zu einer Komponente, die 2 nicht als Ecke enthält.

Als Folgerung aus Satz 1.6 und Lemma 1.11 erhält man, unabhängig von der Nummerierung der Primgraphkomponenten die nicht die Ecke 2 enthalten:

Lemma 1.12. *Es seien G und H endliche nicht-auflösbare Gruppen mit zerfallendem Primgraphen und keine Frobeniusgruppen. G_0 und H_0 seien die zugehörigen, eindeutig bestimmten, nicht-auflösbaren Kompositionsfaktoren. Dann gilt:*

a) Für jeden Index $i \geqslant 2$ existiert ein Index $k \geqslant 2$ mit $\Gamma_i(G) = \Gamma_k(G_0)$ und $\gamma_i(G) = \gamma_k(G_0)$.

b) Ist $\Gamma(G) = \Gamma(H)$ und gilt $|X| = |Y|$ für einen nicht-auflösbare Normalteiler oder Quotienten X von G und einen nicht-auflösbare Normalteiler oder Quotienten Y von H, dann gibt es für jeden Index $i \geqslant 2$ Indices $j, k, l \geqslant 2$ mit

$$\Gamma_k(G_0) = \Gamma_i(G) = \Gamma_j(H) = \Gamma_l(H_0)$$

und

$$\gamma_k(G_0) = \gamma_i(G) = \gamma_j(H) = \gamma_l(H_0)\,.$$

Beweis.

a) Nach Satz 1.6 folgt $\pi_i(G) \subset \pi(G_0)$. Also muss $\Gamma_i(G)$ durch Fusion von Komponenten von $\Gamma(G_0)$ entstehen. Nach Lemma 1.11 sind fusionierte Komponenten von $\Gamma(G_0)$ aber Teilgraphen von $\Gamma_1(G)$. Es gilt also $\pi_i(G) = \pi_k(G_0)$ für ein $k \geqslant 2$. Da sowohl $\Gamma_k(G)$, als auch $\Gamma_k(G_0)$ ein vollständiger Graph ist, gilt die Gleichheit. Die Gleichung $\gamma_i(G) = \gamma_k(G_0)$ folgt aus Satz 1.6, da $\frac{|G|}{|G_0|}$ eine $\pi_1(G)$-Zahl ist.

b) Die Gleichheit der Primgraphkomponenten folgt aus Teil a) mit der Gleichheit der Primgraphen. Außerdem folgt $\gamma_i(G) = \gamma_k(G_0)$ sowie $\gamma_j(H) = \gamma_l(H_0)$. Da X und Y nichtauflösbare Gruppen sind gilt nach Satz 1.6 $|G_0| \,\big|\, |X| \,\big|\, |G|$ und $|H_0| \,\big|\, |Y| \,\big|\, |H|$. Aus $|X| = |Y|$ folgt dann die Behauptung, da $\frac{|G|}{|X|}$ und $\frac{|H|}{|Y|}$ nach Satz 1.6 $\pi_i'(G)$-Zahlen sind.

□

Im Fall von Satz 1.10 bedeutet das also, dass jede Komponente Γ_i von Γ mit $i \geqslant 2$ in den Faktoren G_0 und H_0 nilpotente Hallgruppen gleicher Ordnung induzieren. Die Ordnungen dieser Hallgruppen werden jeweils durch geeignete $\gamma_k(G_0)$, bzw. $\gamma_l(H_0)$ beschrieben.

Bemerkung 1.13.

- Für eine endliche Gruppe X wird die Indizierung der Komponenten von $\Gamma(X)$ so gewählt, dass stets $\gamma_i(X) < \gamma_j(X)$ für $2 \leqslant i < j$ gilt. Von dieser Regel wird nur im Fall der Gruppen $E_8(q)$ abgewichen, wenn der Primgraph fünf Komponenten besitzt. In diesem Fall ist $\gamma_2 < \gamma_5 < \gamma_3 < \gamma_4$. Besitzt $E_8(q)$ nur 4 Komponenten, dann gilt $\gamma_2 < \gamma_3 < \gamma_4$. Diese Notation wird gewählt, da so bei allen Gruppen vom Typ $E_8(q)$ die Werte γ_2, γ_3 und γ_4 mit den gleichen Formeln beschrieben werden können, unabhängig von der Anzahl der Primgraphkomponenten.

  Für einen zerfallenden Primgraphen $\Gamma(X)$ bezeichne $\gamma_u(X) := \min\{\gamma_i(X) \;;\; i \geqslant 2\}$ und $\gamma_o(X) := \max\{\gamma_i(X) \;;\; i \geqslant 2\}$.

  Im Fall von Satz 1.10 gilt dann stets (für geeignete Indices $i, j, k, l \geqslant 2$)

$$\gamma_u := \gamma_u(G) = \gamma_i(G_0) = \gamma_j(H_0) = \gamma_u(H) \text{ und}$$
$$\gamma_o := \gamma_o(G) = \gamma_k(G_0) = \gamma_l(H_0) = \gamma_o(H)\,.$$

  Ist insbesondere $|\Gamma| = |\Gamma(G_0)|$, bzw. $|\Gamma| = |\Gamma(H_0)|$, dann gilt $\gamma_u = \gamma_u(G_0)$, bzw. $\gamma_u = \gamma_u(H_0)$ und $\gamma_o = \gamma_o(G_0)$, bzw. $\gamma_o = \gamma_o(H_0)$.
- Die Gruppen $E_7(2), E_7(3), A_2(2), {}^2A_5(2), A_2(4)$ und ${}^2E_6(2)$ sind, neben den sporadisch-einfachen Gruppen, genau die einfachen Gruppen mit $|\Gamma| \geqslant 3$, die keiner Serie von einfachen Gruppen mit $|\Gamma| \geqslant 3$ angehören (siehe Tabellen A.4 und A.5). Diese sechs Gruppen werden daher im Folgenden als Ausnahmegruppen bezeichnet.
- Ist G_0 sporadisch-einfach oder eine Ausnahmegruppe, dann ist $\gamma_o(G_0) \leqslant 1093$.
- In den Tabellen A.4 und A.5 tauchen neben den Ausnahmegruppen auch spezielle alternierende Gruppen und einige Serien einfacher Gruppen vom Lietyp auf, wobei die

zugehörigen Primgraphen nur dann mehrfach zerfallend sind, wenn die Ordnung des zugehörigen Körpers, bzw. der Lierang der Gruppe die in den Tabellen angegebenen Bedingungen erfüllt. Im Folgenden stehe X für einen dieser Typen, und mit $X(q)$ mit $q = p^f$ sei dann eine der Gruppen dieses Typs bezeichnet. Betrachtet man für $i \geqslant 2$ die $\gamma_i(X(q))$ als reellwertige Funktionen in q auf dem Intervall $[2, \infty)$, dann sind all diese Funktionen $\geqslant 0$ und streng monoton wachsend.

Steht X für die alternierenden Gruppen bzw. eine der Serien A_1, ${}^2D_p(3)$ und ${}^2D_{p+1}(2)$, ist dies offensichtlich.

Steht X für eine der anderen Serien, dann kann man jedes der $\gamma_i(X(q))$ als Summe von nicht-negativen, streng monoton wachsenden Funktionen auffassen. Es ist nämlich jedes auftretende $\gamma_i(X(q))$ eine Summe von Funktionen der Form $\pm\sqrt{r}q^j$ mit $r \in \{1, 2, 3\}$ und $2j \in \mathbb{N}$. In der Summe sind die Summanden entweder alle positiv, oder aber das Vorzeichen wechselt alternierend, wenn die Summanden nach der auftretenden q-Potenz absteigend sortiert sind. Sind alle diese Summanden positiv, und damit streng monoton wachsend, dann ist sicherlich auch $\gamma_i(X(q))$ streng monoton wachsend. Im alternierenden Fall kann jeder negative Summand mit seinem direkten Vorgänger verrechnet werden. Es gilt dann $\sqrt{r_a}q^a - \sqrt{r_b}q^b = q^b(\sqrt{r_a}q^{a-b} - \sqrt{r_b})$ mit $a - b \geqslant 1/2$. Ist $r_b \leqslant 2$, dann ist wegen $q \geqslant 2$ sicherlich $\sqrt{r_a}q^{a-b} \geqslant \sqrt{r_b}$. Der Fall $r_b > 2$ tritt nur für den Typ $X = {}^2G_2$ auf. Es gilt dann $r_b = 3$ und weiter ist $r_a = 1$, $a = 2$ und $b = 1$. Auch hier gilt also $q = 1 \cdot q^{2-1} = \sqrt{r_a}q^{a-b} \geqslant \sqrt{r_b} = \sqrt{3}$ für $q \geqslant 2$.

Auch $\gamma_1(X(q))$ kann als Funktion auf $[2, \infty)$ aufgefasst werden. Als Produkt positiver, streng monoton wachsender Funktionen ist $\gamma_1(X(q))$ aber offensichtlich positiv und streng monoton wachsend.

Man erhält also für alle der in den Tabellen A.4 und A.5 vorkommenden Serien von Gruppen

- $\gamma_i(X(q)) > \gamma_i(X(\bar{q})) \iff q > \bar{q}$ für alle $i \geqslant 1$, und damit
- $|X(q)| > |X(\bar{q})| \iff q > \bar{q}$.

1.3 Beweisstrategie von Satz 1.10

Für den Beweis von Satz 1.10 wird $H_0 \ncong G_0$ angenommen. Diese Annahme wird dann in jedem der möglichen Fälle für G_0 und H_0 zu einem Widerspruch geführt. Die Proposition wird in Abschnitt 1.4 zunächst für den Fall von $|\Gamma| > 3$ bewiesen, dann in Abschnitt 1.5 für $|\Gamma| = 3$.

Man kann auf der Menge der Isomorphieklassen einfacher Gruppen mit mehrfach zerfallendem Primgraphen eine totale Ordnung $\prec$ erklären. Zunächst wird die Ordnung zwischen den verschiedenen Typen durch

$$\begin{gathered}\text{sporadisch} \prec \text{Ausnahmegruppen} \prec \text{alternierend} \prec A(q)\ (q \equiv 1 \bmod 4) \prec \\ A(q)\ (q \equiv 3 \bmod 4) \prec A(q)\ (q \equiv 0 \bmod 2) \prec G_2(q) \prec {}^2G_2(q) \prec {}^2D_p(3) \prec {}^2D_{p+1} \prec \\ F_4(q) \prec {}^2F_4(q) \prec E_8(q) \prec {}^2B_2(q)\end{gathered}$$

willkürlich festgelegt. Gruppen, bei denen Ausnahmeisomorphismen vorliegen (siehe dazu [13]), werden dem „kleinsten“ Typ X zugewiesen. Innerhalb eines Typs X wird die Ordnung via $G_1 \prec G_2 \iff |G_1| < |G_2|$ für $G_1, G_2 \in X$ erklärt (man beachte dabei, dass für zwei Gruppen G_1 und G_2 desselben Typs stets $|G_1| \neq |G_2|$ gilt). Sind also G_0 und H_0 einfache Gruppen mit mehrfach zerfallendem Primgraphen vom Typ X bzw. Y, dann gilt

$$H_0 \prec G_0 \iff \begin{cases} X \prec Y & \text{wenn } X \neq Y \\ |H_0| < |G_0| & \text{wenn } X = Y \end{cases}.$$

Für den Beweis der Proposition kann dann o.B.d.A. stets $H_0 \prec G_0$ angenommen werden.

Der Beweis wird so geführt, dass zunächst nur die arithmetischen Bedingungen an die Ordnungen der π_i-Hallgruppen (mit $i \geqslant 2$) ausgenutzt werden. Reicht dies aus, um den Beweis für den Fall $G_0 \in X(q)$ und $H_0 \in Y(\bar{q})$ zu führen, so ist dies in Tabelle 1.1 mit dem Eintrag γ_1' gekennzeichnet.

Die Gruppenordnung von G' wird zu Hilfe genommen, wenn die Ordnungen der Hallgruppen nicht zu einem Widerspruch führen. Diese Fälle sind in der Tabelle mit $|G'|$ gekennzeichnet, und vervollständigen den Beweis.

Insgesamt wird der Beweis also nur unter Verwendung der arithmetischen Bedingungen geführt, die die Ordnungen der isolierten Hallgruppen von G_0 und H_0, bzw. die Ordnungen von G' und H' liefern.

$\lvert\Gamma\rvert \geqslant 3$	sporadisch	Ausnahmegruppen	A_p	$A_1(q); q \equiv 1(4)$	$A_1(q); q \equiv 3(4)$	$A_1(q); q \equiv 0(2)$	$G_2(q)$	${}^2G_2(3^x)$	${}^2D_p(3^2)$	${}^2D_{p+1}(2)$	$F_4(q)$	${}^2F_4(q)$	$E_8(q)$	${}^2B_2(q)$
sporadisch	$\lvert G'\rvert$	$\lvert G'\rvert$	$\lvert G'\rvert$	γ_1'	$\lvert G'\rvert$	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'
Ausnahmegruppen		$\lvert G'\rvert$	$\lvert G'\rvert$	γ_1'	$\lvert G'\rvert$	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'
$A_{\bar{p}}$			γ_1'	γ_1'	γ_1'	$\lvert G'\rvert$	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'
$A_1(\bar{q}); \bar{q} \equiv 1(4)$				γ_1'	γ_1'	γ_1'	$\lvert G'\rvert$	$\lvert G'\rvert$	$\lvert G'\rvert$	$\lvert G'\rvert$	γ_1'	γ_1'	γ_1'	$\lvert G'\rvert$
$A_1(\bar{q}); \bar{q} \equiv 3(4)$					γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'
$A_1(\bar{q}); \bar{q} \equiv 0(2)$						γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'
$G_2(\bar{q})$							γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	$\lvert G'\rvert$
${}^2G_2(\bar{q})$								γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'
${}^2D_{\bar{p}}(3)$									γ_1'	γ_1'	γ_1'	γ_1'	γ_1'	γ_1'
${}^2D_{\bar{p}+1}(2)$										γ_1'	γ_1'	γ_1'	γ_1'	γ_1'
$F_4(\bar{q})$											γ_1'	γ_1'	γ_1'	γ_1'
${}^2F_4(\bar{q})$												γ_1'	γ_1'	γ_1'
$E_8(\bar{q})$													γ_1'	γ_1'
${}^2B_2(\bar{q})$														γ_1'

Tabelle 1.1: Zum Beweis von Satz 1.10; (horizontal ist G_0, vertikal ist H_0 angegeben)

Zum Beweis werden die folgenden zahlentheoretischen Beobachtungen benötigt (siehe [61] oder auch [44]).

Satz 1.14 (Zsigmondy)**.** *Ist* p *eine Primzahl und* $n \geqslant 2$*, dann gibt es eine Primzahl* z*, so dass* $z \mid (p^n - 1)$ *und* $z \nmid (p^m - 1)$ *für* $1 \leqslant m < n$*, bis auf die Fälle*

(a) $p = 2$ *und* $n = 6$ *oder*

(b) $p = 2^s - 1$ *ist eine Mersenne-Primzahl (insbesondere ist also auch* s *prim) und* $n = 2$.

Als Folgerung aus dem Satz von Zsigmondy erhält man [34, Lemma 1.2]:

Lemma 1.15. *Seien* p *und* r *zwei Primzahlen und* $1 \leqslant m < n \in \mathbb{N}$*, so dass*

$$p^m = r^n + 1$$

ist. Dann entsprechen die Zahlen einem der folgenden Fälle:

(a) $r = 2$*,* $p = 3$*,* $n = 3$ *und* $m = 2$*.*

(b) $r = 2$*,* $m = 1$*,* n *ist eine Potenz von 2 und* $p = r^n + 1$ *ist eine Fermat-Primzahl.*

(c) $p = 2$*,* $n = 1$ *und* $r = p^m - 1$ *ist eine Mersenne-Primzahl. Insbesondere ist also* m *prim.*

1.4 Beweis von Satz 1.10 für $|\Gamma| > 3$.

Ist $|\Gamma| > 3$, dann sind die nicht-auflösbaren Faktoren G_0 und H_0 nach den Tabellen A.3 - A.5 entweder sporadisch-einfach, Ausnahmegruppen, $E_8(q)$ oder ${}^2B_2(q)$.

- Ist sowohl G_0 als auch H_0 sporadisch-einfach oder eine Ausnahmegruppe, dann kann man aus den Tabellen A.3 und A.5 sofort ablesen, dass $G_0 \cong H_0$ gelten muss, da für nicht-isomorphe Gruppen G_0 und H_0 stets $|\pi_1'(G_0) \cap \pi_1'(H_0)| \leqslant 2$ gilt.
- Ist $G_0 \cong E_8(q)$, dann ist $|\Gamma| = 4$ oder $|\Gamma| = 5$. Die beiden Fälle können gemeinsam behandelt werden. Für kleine q-Werte erhält man:

q	2	3	4
$\gamma_2(G_0)$	151	4561	$49981 = 151 \cdot 331$
$\gamma_3(G_0)$	241	6481	$65281 = 97 \cdot 673$
$\gamma_4(G_0)$	331	$8401 = 31 \cdot 271$	$80582 = 61 \cdot 1321$
$\gamma_5(G_0)$	–	–	61681

  Ist H_0 sporadisch-einfach bzw. eine Ausnahmegruppe, dann folgt wegen $\gamma_o(H_0) \leqslant 1093$, dass $q = 2$ sein muss. Keine der sporadisch-einfachen Gruppen und Ausnahmegruppen nimmt aber die entsprechenden $\gamma_i(G_0)$-Werte an.

  Es ist also $H_0 \cong E_8(\bar{q})$. Die Bedingungen, die dieser Fall liefert, treten später (in Abschnitt 1.5.13) als Spezialfall beim Beweis für $|\Gamma| = 3$ wieder auf. Dort werden sie behandelt und zu einem Widerspruch geführt.

- Ist $G_0 \cong {}^2B_2(q)$, dann nehmen die $\gamma_i(G_0)$ für kleine q mit $q = 2^{2m+1}$ und $m \geqslant 1$ die folgenden Werte an:

q	2^3	2^5	2^7	2^9	2^{11}
$\gamma_2(G_0)$	5	5^2	113	$481 = 13 \cdot 37$	$1985 = 5 \cdot 397$
$\gamma_3(G_0)$	7	31	127	$511 = 7 \cdot 73$	$2047 = 23 \cdot 89$
$\gamma_4(G_0)$	13	41	$145 = 5 \cdot 29$	$545 = 5 \cdot 109$	2113

Ist H_0 sporadisch-einfach oder eine Ausnahmegruppe, dann ist wegen $\gamma_o(H_0) \leqslant 1093$ nur $q \leqslant 2^9$ möglich. Vergleicht man die auftretenden $\gamma_i(G_0)$-Werte jedoch mit den möglichen $\gamma_i(H_0)$-Werten in Tabelle A.3 und Tabelle A.5, dann stellt man fest, dass keine der sporadisch-einfache Gruppen bzw. der Ausnahmegruppen den $\gamma_i(G_0)$ entsprechende $\gamma_i(H_0)$-Werte besitzt.

Der Fall $H_0 \cong E_8(\bar{q})$ ist ebenfalls nicht möglich. Es ist nämlich $\bar{q}^4-1 \equiv 1^4-1 \equiv 0 \bmod 5$. Da $\bar{q}^4 - 1$ den Wert $\gamma_1(H_0)$ teilt, ist $5 \in \pi_1(H_0)$. Die Zahl 5 teilt aber auch den Wert $\gamma_2(G_0) \cdot \gamma_4(G_0)$, denn es gilt

$$\begin{aligned} \gamma_2(G_0) \cdot \gamma_4(G_0) &= \left(q - \sqrt{2q} + 1\right)\left(q + \sqrt{2q} + 1\right) = q^2 + 1 = 4^{2m+1} + 1 \\ &\equiv -1^{2m+1} + 1 \equiv 0 \bmod 5\,. \end{aligned}$$

Wegen $|\Gamma(G_0)| = 4 \leqslant |\Gamma|$ können in Γ keine der $\Gamma(G_0)$-Komponenten fusionieren und es muss $\gamma_i(G) = \gamma_i(G_0)$ für alle $i \geqslant 2$ gelten. Damit müsste 5 aber in zwei Komponenten liegen, was unmöglich ist.

Ist $H_0 \cong {}^2B_2(\bar{q})$, dann folgt aus $\gamma_4(G_0) = \gamma_o = \gamma_4(H_0)$ unmittelbar $q = \bar{q}$.

1.5 Beweis von Satz 1.10 für $|\Gamma| = 3$.

1.5.1 G_0 sporadisch-einfach

Wegen $H_0 \prec G_0$ ist H_0 ebenfalls sporadisch-einfach mit $|H_0| < |G_0|$. Es ist also $|\mathrm{Out}(G_0)|, |\mathrm{Out}(H_0)| \leqslant 2$ und wegen $|G'| = |H'|$ ist also $|H_0| = |G_0|$ oder $2|H_0| = |G_0|$. Aus Tabelle A.3 kann man dann unmittelbar ablesen, dass $G_0 \cong H_0$ sein muss.

1.5.2 G_0 Ausnahmegruppe

Dann ist $G_0 \in \{E_7(2), E_7(3), {}^2E_6(2), A_2(2), A_2(4), {}^2A_5(2)\}$.

- H_0 sporadisch-einfach

In nachfolgender Tabelle sind für alle möglichen G_0 die Werte $\gamma_1'(G_0)$ angegeben, sowie die sporadisch-einfachen Gruppen für die $\pi_1'(G_0) \subseteq \pi_1'(H_0)$ oder $\pi_1'(G_0) \supseteq \pi_1'(H_0)$ gilt. Diese Gruppen kommen als H_0 in Betracht.

G_0	$E_7(2)$	$E_7(3)$	${}^2E_6(2)$	$A_2(2)$	$A_2(4)$	${}^2A_5(2)$
$\gamma_1'(G_0)$	$73 \cdot 127$	$757 \cdot 1093$	$13 \cdot 17 \cdot 19$	$3 \cdot 7$	$3^2 \cdot 5 \cdot 7$	$7 \cdot 11$
H_0	–	–	–	–	M_{22}	M_{22}, HS, J_1

Der Fall $G_0 \cong A_2(4)$ scheidet aus, denn es ist $11 \in \pi(M_{22})$ aber $11 \nmid |\mathrm{Aut}(A_2(4))|$. Also muss $G_0 \cong {}^2A_5(2)$ gelten und 2^{15} teilt die Ordnung von G'. Für $H_0 \in \{M_{22}, HS, J_1\}$ gilt aber stets, dass 2^{15} den Wert $|H_0| \cdot |\mathrm{Out}(H_0)|$ nicht teilt.

- H_0 Ausnahmegruppe

Obige Tabelle zeigt, dass nur die Kombination $G_0 \cong A_2(4)$ und $H_0 \cong A_2(2)$ in Frage kommt. Es ist aber $|\mathrm{Out}(A_2(2))| = 2$ und damit $|H'| \leqslant 2|H_0| = 2^4 \cdot 3 \cdot 7 < |G_0| \leqslant |G'|$.

1.5.3 G_0 alternierend

Es ist dann $G_0 \cong A_n$ mit $n \in \{5, 6, p\}$, wobei p und $p-2$ prim sind. Ist $n \neq 6$, dann ist $\gamma_o = \gamma_o(G_0) \in \{5, p\}$ der größte Primteiler von $|G'|$, da $\mathrm{Out}(G_0)$ nur für $G_0 \cong A_6$ nicht-trivial ist (genauer gilt $\mathrm{Out}(A_6) \cong C_2$). Außerdem gilt immer, dass alle Primzahlen, die kleiner als n sind, die Ordnung von G' teilen.

- H_0 sporadisch-einfach

Wegen $|\mathrm{Out}(H_0)| \leqslant 2$ sind die maximalen Primteiler von $|H'|$ und $|H_0|$ identisch. Unter den in Frage kommenden sporadisch-einfachen Gruppen gibt es nur zwei Gruppen, deren Ordnung einen maximalen Primteiler p enthalten, so dass auch $p-2$ prim ist, nämlich

H_0	Suz	J_3
$(p, p-2)$	$(13, 11)$	$(19, 17)$

Der Fall $H_0 \cong J_3$ scheidet aus, da es Primzahlen kleiner $\gamma_o = \gamma_o(H_0) = 19$ gibt, die die Ordnung von H' nicht teilen. Es gilt nämlich $7, 11, 13 \notin \pi(\mathrm{Aut}(J_3))$. Ist $H_0 \cong Suz$, dann ist $p = 13$ und damit $G_0 \cong A_{13}$. Wegen $|\Gamma(Suz.2)| = 2$ folgt $H' \cong Suz$ und somit $2^{13} \,\|\, |H'|$, im Widerspruch zu $2^9 \,\|\, |G'| = |G_0| = |A_{13}|$.

- H_0 Ausnahmegruppe

Die Tabelle in Abschnitt 1.5.2 zeigt, dass nur der Fall $G_0 \cong A_7$ und $H_0 \cong A_2(4)$ möglich ist. Es ist dann aber $G' = G_0$ und somit $2^3 \,\|\, |G'|$, im Widerspruch zu $2^6 \mid |H_0|$.

- H_0 alternierend

Für $G_0 \cong A_6$ und $H_0 \cong A_5$ ist $\Gamma(G_0) = \Gamma(H_0)$. Wegen $\mathrm{Out}(A_5) = 1$ gilt aber $|H'| = |H_0| < |G_0| \leqslant |G'|$, im Widerspruch zu $|G'| = |H'|$. Ist $G_0 \cong A_p$ mit $p \geqslant 7$ und $H_0 \cong A_{\bar{p}}$, dann folgt aus $p \neq \bar{p}$ unmittelbar $|G'| = |G_0| \neq |H_0| = |H'|$. Ist $H_0 \cong A_6$, dann ist p kein Teiler von $|H'|$, im Widerspruch zu $p \mid |G_0|$.

1.5.4 G_0 vom Typ $A_1(q)$ mit $q \equiv 1 \bmod 4$

Es ist $\gamma_u = \gamma_u(G_0) = \frac{q+1}{2}$ und $\gamma_o = \gamma_o(G_0) = q$.

- H_0 sporadisch-einfach bzw. Ausnahmegruppe

Es gilt $\gamma_o = \gamma_o(H) \leqslant \gamma_o(H_0) \leqslant 1093$. Die folgende Tabelle zeigt die nach Tabelle A.3 möglichen $\gamma_o = \gamma_o(H)$-Werte, sowie die daraus rechnerisch resultierenden Werte für $\gamma_u = \gamma_u(G_0)$.

$\gamma_o = q$	7	9	11	13	19	23	29	31	37	43	47	59	67	71	127	1093
$\gamma_u = \frac{q+1}{2}$	4	5	6	7	10	12	15	16	19	22	24	30	34	36	64	547

Die einzige Gruppe H_0, die ein entsprechendes Paar (γ_u, γ_o) liefert, ist $H_0 \cong A_2(4)$ mit $\gamma_u(H) = 5$ und $\gamma_o(H) = 9$ (es muss dann $\Gamma_3(H_0) \subset \Gamma_1(H)$ gelten). Entsprechend ist dann $\gamma_o = q = 9$, also $G_0 \cong A_1(9)$. Dann gilt $|\mathrm{Out}(G_0)| = 4$ und damit aber $7 \nmid |G'|$, im Widerspruch zu $7 \mid |H_0| = 2^6 \cdot 3^2 \cdot 5 \cdot 7$.

- H_0 alternierend

Ist $H_0 \cong A_6$, dann gilt $\gamma_o = 3^2 = q$ und damit $G_0 \cong A_1(9)$. Die Gruppen A_6 und $A_1(9)$ sind aber isomorph [13]. Ist $H_0 \cong A_{\bar{p}}$, dann ist $q = \gamma_o = \gamma_o(H_0) = \bar{p}$ und $\frac{q+1}{2} = \gamma_u = \gamma_u(H_0) = \bar{p} - 2$. Man erhält:

$$\bar{p} - 2 = q - 2 = \frac{q+1}{2} \implies q = 5\,.$$

Daraus folgt $G_0 \cong A_1(5)$ und $H_0 \cong A_5$. Auch diese beiden Gruppen sind isomorph [13]. Man erhält also im Fall einer alternierenden Gruppe H_0 genau die Ausnahmeisomorphismen.

- H_0 vom Typ $A_1(\bar{q})$ mit $\bar{q} \equiv 1 \bmod 4$

Für $H_0 \cong A_1(\bar{q})$ mit $\bar{q} \equiv 1 \bmod 4$ folgt aus $q = \gamma_o = \gamma_o(H_0) = \bar{q}$ sofort $H_0 \cong G_0$.

1.5.5 G_0 vom Typ $A_1(q)$ mit $q \equiv 3 \bmod 4$

Es ist $\gamma_u = \gamma_u(G_0) = \frac{q-1}{2}$ und $\gamma_o = \gamma_o(G_0) = q$.

- H_0 sporadisch-einfach bzw. Ausnahmegruppe

Es gilt $\gamma_o = \gamma_o(H) \leqslant \gamma_o(H_0) \leqslant 1093$. Die folgende Tabelle zeigt wieder die nach Tabelle A.3 möglichen $\gamma_o(H)$-Werte, sowie die daraus rechnerisch resultierenden Werte für $\gamma_u = \gamma_u(G_0)$.

$\gamma_o = q$	7	9	11	13	19	23	29	31	37	43	47	59	67	71	127	1093
$\gamma_u = \frac{q-1}{2}$	3	4	5	6	9	11	14	15	18	21	23	29	33	35	63	546

Als mögliche Paare (G_0, H_0) ergeben sich

$$\begin{aligned}
&\text{für } q = 7 \quad : \quad (A_1(7), A_2(2)) \quad , \quad (A_1(7), A_2(4)) \quad , \\
&\text{für } q = 11 \quad : \quad (A_1(11), M_{11}) \quad , \quad (A_1(11), M_{22}) \quad , \\
&\text{für } q = 23 \quad : \quad (A_1(23), M_{23}) \quad , \quad (A_1(23), M_{24}) \quad , \quad (A_1(23), Co_2)
\end{aligned}$$

Für die Gruppenordnungen von G_0 ergibt sich in den einzelnen Fällen:

G_0	$A_1(7)$	$A_1(11)$	$A_1(23)$
$\lvert G_0\rvert$	$2^3 \cdot 3 \cdot 7$	$2^2 \cdot 3 \cdot 5 \cdot 11$	$2^3 \cdot 3 \cdot 11 \cdot 23$

In allen Fällen gilt $|\mathrm{Out}(G_0)| = 2$ und damit $3 \,\|\, |G'|$. Für jede mögliche Gruppe H_0 gilt jedoch $3^2 \,|\, |H_0|$, im Widerspruch zu $|G'| = |H'|$.

- H_0 alternierend

Ist $H_0 \cong A_6$, dann gilt $q = \gamma_o = \gamma_o(H_0) = 3^2$, im Widerspruch zu $q \equiv 3 \bmod 4$. Für $H_0 \cong A_{\bar{p}}$ ist $q = \gamma_o = \gamma_o(H_0) = \bar{p}$ und $\frac{q-1}{2} = \gamma_u = \gamma_u(H_0) = \bar{p} - 2$. Es gilt:

$$\bar{p} - 2 = q - 2 = \frac{q-1}{2} \implies q = 3\,.$$

Damit ist $G_0 \cong A_1(3) \cong A_4$ und $H_0 \cong A_3$. Beide Gruppen sind aber auflösbar.

- H_0 vom Typ $A_1(\bar{q})$ mit $\bar{q} \equiv 1 \bmod 4$

Für $H_0 \cong A_1(\bar{q})$ mit $\bar{q} \equiv 1 \bmod 4$ ist $q = \gamma_o = \gamma_o(H_0) = \bar{q}$. Es ist dann aber $\bar{q} = q \equiv 3 \bmod 4$, im Widerspruch zu $\bar{q} \equiv 1 \bmod 4$.

- H_0 vom Typ $A_1(\bar{q})$ mit $\bar{q} \equiv 3 \bmod 4$

Für $H_0 \cong A_1(\bar{q})$ mit $\bar{q} \equiv 3 \bmod 4$ folgt aus $q = \gamma_o = \gamma_o(H_0) = \bar{q}$ sofort $H_0 \cong G_0$.

1.5.6 G_0 vom Typ $A_1(q)$ mit $q \equiv 0 \bmod 2$

Es ist $\gamma_u = \gamma_u(G_0) = q - 1$ und $\gamma_o = \gamma_o(G_0) = q + 1$. Also gilt $\gamma_o - \gamma_u = 2$. Weiter gilt $\mathrm{Out}(G_0) \cong C_f$, wobei f durch $q = p^f$ definiert ist.

• H_0 sporadisch-einfach bzw. Ausnahmegruppe

In diesem Fall gilt $H_0 \in \{J_4, Suz, A_2(4), {}^2E_6(2)\}$. Alle anderen sporadisch-einfachen Gruppen, bzw. Ausnahmegruppen liefern kein Zahlenpaar $(\gamma_o, \gamma_u) = (\gamma_o(H), \gamma_u(H))$ mit $\gamma_o - \gamma_u = 2$. Es liegen dann die folgenden $\gamma_o(H)$-Werte vor:

H_0	J_4	Suz	$A_2(4)$	${}^2E_6(2)$
$\gamma_o(H)$	31	13	9 oder 7	19

Mit $\gamma_o = q + 1$ sieht man, dass lediglich $H_0 \cong A_2(4)$ mit $\gamma_o(H) = \gamma_4(H_0) = 9 = q + 1$ die Bedingung $q \equiv 0 \bmod 2$ mit $q = 8$ erfüllt. Es ist dann also $G_0 \cong A_1(8)$ und somit $|\mathrm{Aut}(G_0)| = 2^3 \cdot 3^3 \cdot 7$. Damit ist aber 5 kein Teiler von $|G'|$, im Widerspruch zu $5 \in \pi(H_0)$.

• H_0 alternierend

Für $H_0 \cong A_5$ folgt $q = 4$ und damit $G_0 = A_1(4)$. Es ist dann aber $G_0 \cong H_0$, da $A_5 \cong A_1(4)$ gilt. Im Fall $H_0 \cong A_6$ ist $\gamma_o - \gamma_u = \gamma_o(H_0) - \gamma_u(H_0) = 9 - 5 \neq 2$. Es ist also $H_0 \cong A_{\bar{p}}$, mit $\bar{p}$ prim. Da sowohl $\gamma_o = \gamma_o(H_0) = \bar{p}$ als auch $\gamma_u = \gamma_u(H_0) = \bar{p} - 2$ Primzahlen sind, müssen auch $q + 1$ und $q - 1$ prim sein. Die Bedingung $\gamma_o - \gamma_u = 2$ ist immer erfüllt. Nach Satz 1.14 und Lemma 1.15 folgt, dass $\bar{p} = q + 1 = p^f + 1$ eine Fermat-Primzahl ist, und damit $f = 2^n$ gilt. Andererseits folgt, dass $\bar{p} - 2 = q - 1 = p^f - 1$ eine Mersenne-Primzahl und f damit prim sein muss. Insgesamt erhält man $f = 2$, $q = 4$, $p = 5$ und somit wiederum $G_0 \cong A_1(4) \cong A_5 \cong H_0$.

• H_0 vom Typ $A_1(\bar{q})$

Ist $\bar{q} \equiv 0 \bmod 2$, so folgt aus $\bar{q}+1 = \gamma_o(H_0) = \gamma_o = q+1$ unmittelbar $\bar{q} = q$. Ist $q \not\equiv 0 \bmod 2$ gilt $q + 1 = \gamma_o = \gamma_o(H_0) = \bar{q}$. Also ist $\bar{q} - 1 = q$ eine 2-Potenz und $\bar{q} \equiv 1 \bmod 4$. Weiter gilt dann $q - 1 = \gamma_u = \gamma_u(H_0) = \frac{1}{2}(\bar{q} + 1)$ und mit $\bar{q} = q + 1$ folgt:

$$\frac{1}{2}(\bar{q} + 1) = \frac{1}{2}(q + 1 + 1) = q - 1 \implies q = 4\,.$$

Also ist $\bar{q} = 5$. Einmal mehr ist dann aber $G_0 \cong A_1(4) \cong A_1(5) \cong H_0$.

1.5.7 G_0 vom Typ $G_2(q)$

Es ist $q = 3^f$, $\gamma_o = \gamma_o(G_0) = q^2 + q + 1$, $\gamma_u = \gamma_u(G_0) = q^2 - q + 1$ und $\gamma_o - \gamma_u = 2 \cdot q$. Für kleine f ergeben sich folgende γ_o, γ_u-Werte.

f	1	2	3	4
γ_o	13	$91 = 7 \cdot 13$	757	$6643 = 7 \cdot 13 \cdot 73$
γ_u	7	73	$703 = 19 \cdot 37$	6481

- H_0 sporadisch-einfach bzw. Ausnahmegruppe

Anhand der Tabellen A.3 - A.5 sieht man leicht, dass keine sporadisch-einfache Gruppe bzw. Ausnahmegruppe ein Paar $(\gamma_o, \gamma_u) = (\gamma_o(H), \gamma_u(H))$ liefert, das obiger Tabelle entspricht.

- H_0 alternierend

Ist H_0 alternierend, so ist $\gamma_o(H_0) - \gamma_u(H_0) = 2^\varepsilon \neq 2 \cdot q = 2 \cdot 3^f = \gamma_o - \gamma_u$ (dabei ist $\varepsilon = 2$, wenn $H_0 \cong A_6$ ist, sonst ist $\varepsilon = 1$).

- H_0 vom Typ $A_1(\bar{q})$

Ist $H_0 \cong A_1(\bar{q})$ und $\bar{q} \equiv 0 \bmod 2$, dann ist $\gamma_o(H_0) - \gamma_u(H_0) = 2 \neq 2 \cdot q = \gamma_o - \gamma_u$. Es gilt also $\bar{q} \not\equiv 0 \bmod 2$, und damit $\bar{q} = \gamma_o(H_0) = \gamma_o = q^2 + q + 1$.

- Im Fall $\bar{q} \equiv 1 \bmod 4$ ist $\bar{q} + 1 = 2\gamma_u(H_0) = 2\gamma_u = 2(q^2 - q + 1)$, also folgt:

$$\bar{q} = q^2 + q + 1 = 2(q^2 - q + 1) - 1 = 2q^2 - 2q + 1 \implies q^2 = 3q \implies q = 3$$

  Damit ist $\bar{q} = 13$. Man erhält also $G_0 \cong G_2(3)$ und $H_0 \cong A_1(13)$ mit $|G_0| = 2^6 \cdot 3^6 \cdot 7 \cdot 13$ und $|H_0| = 2^2 \cdot 3 \cdot 7 \cdot 13$. Wegen $|\mathrm{Out}(H_0)| = 2$ ist aber stets $|H'| \leqslant 2 \cdot |H_0| < |G_0| \leqslant |G'|$ und damit $|G'| \neq |H'|$.
- Ist $\bar{q} \equiv 3 \bmod 4$, so ist $\bar{q} - 1 = 2\gamma_u(H_0) = 2\gamma_u = 2(q^2 - q + 1)$, also folgt:

$$\bar{q} = q^2 + q + 1 = 2(q^2 - q + 1) + 1 = 2q^2 - 2q + 3 \implies q^2 = 3q - 2\,.$$

  Da q eine 3-Potenz ist, ist das unmöglich.

- H_0 vom Typ $G_2(\bar{q})$

In diesem Fall folgt aus $2q = \gamma_o(H_0) - \gamma_u(H_0) = \gamma_o - \gamma_u = 2\bar{q}$ unmittelbar $q = \bar{q}$ und damit $G_0 \cong H_0$.

1.5.8 G_0 vom Typ ${}^2G_2(q^2)$

Es ist $q^2 = 3^{2m+1}$ mit $m \geqslant 1$. Weiter gilt $\gamma_o = \gamma_o(G_0) = q^2 + \sqrt{3q^2} + 1$ sowie $\gamma_u = \gamma_u(G_0) = q^2 - \sqrt{3q^2} + 1$ und damit $\gamma_o - \gamma_u = 2\sqrt{3q^2} = 2 \cdot 3^{m+1}$. Für kleine Werte von m erhält man die folgenden γ_o, γ_u-Werte:

m	1	2	3
γ_o	37	271	2269
γ_u	19	$217 = 7 \cdot 31$	$2107 = 7^2 \cdot 41$

• H_0 sporadisch-einfach bzw. Ausnahmegruppe

Anhand der Tabellen A.3 - A.5 sieht man leicht, dass keine der sporadisch-einfachen Gruppen bzw. Ausnahmegruppen ein Paar $(\gamma_o(H), \gamma_u(H)) = (\gamma_o, \gamma_u)$ liefert, das obiger Tabelle entspricht.

• H_0 alternierend

Ist H_0 alternierend, dann ist $\gamma_o(H_0) - \gamma_u(H_0) = 2^\varepsilon \neq 2 \cdot 3^{m+1} = \gamma_o - \gamma_u$ (dabei ist wiederum $\varepsilon = 2$ für $H_0 \cong A_6$, sonst ist $\varepsilon = 1$).

• H_0 vom Typ $A_1(\bar{q})$

Sei $H_0 \cong A_1(\bar{q})$ und $\bar{q} \equiv 0 \bmod 2$, dann ist $\gamma_o(H_0) - \gamma_u(H_0) = 2 \neq 2 \cdot 3^{m+1} = \gamma_o - \gamma_u$. Es gilt also $\bar{q} \not\equiv 0 \bmod 2$, und damit $\bar{q} = \gamma_o(H_0) = \gamma_o = q^2 + \sqrt{3q^2} + 1$.

- Im Fall $\bar{q} \equiv 1 \bmod 4$ ist $\bar{q} + 1 = 2\gamma_u(H_0) = 2\gamma_u = 2\left(q^2 - \sqrt{3q^2} + 1\right)$. Es folgt:

$$\begin{aligned} \bar{q} &= q^2 + \sqrt{3q^2} + 1 = 2\left(q^2 - \sqrt{3q^2} + 1\right) - 1 = 2q^2 - 2\sqrt{3q^2} + 1 \\ &\implies 3^{2m+1} = q^2 = 3\sqrt{3q^2} = 3^{m+2} \implies m = 1\,. \end{aligned}$$

  Damit ist $q = 3^3$ sowie $\bar{q} = 37$, also $G_0 \cong {}^2G_2(3^3)$ und $H_0 \cong A_1(37)$ mit

$$|G_0| = 2^3 \cdot 3^9 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \text{ und } |H_0| = 2^2 \cdot 3^2 \cdot 19 \cdot 37\,.$$

  Wegen $\mathrm{Out}(H_0) \cong C_2$ gilt $7, 13 \notin \pi(H')$, im Widerspruch zu $7 \cdot 13 \,\big|\, |G_0|$.

- Ist $\bar{q} \equiv 3 \bmod 4$, dann ist $\bar{q} - 1 = 2\gamma_u(H_0) = 2\gamma_u = 2\left(q^2 - \sqrt{3q^2} + 1\right)$ und es folgt:

$$\bar{q} = q^2 + \sqrt{3q^2} + 1 = 2\left(q^2 - \sqrt{3q^2} + 1\right) + 1 = 2q^2 - 2\sqrt{3q^2} + 3 \implies q^2 = 3\sqrt{3q^2} - 2\,.$$

  Da q eine 3-Potenz ist, ist das unmöglich.

• H_0 vom Typ $G_2(\bar{q})$

Es muss dann gelten:

$$\gamma_1'(H_0) = \bar{q}^4 + \bar{q}^2 + 1 = q^4 - q^2 + 1 = \gamma_1'(G_0) \implies \bar{q}^2(\bar{q}^2 + 1) = q^2(q^2 - 1)\,.$$

Da $\bar{q}$ und q Potenzen von 3 sind, liefern die Faktoren vor der Klammer $\bar{q} = q$. Die Werte in den Klammern stimmen dann aber nicht überein, und es ist $\gamma_1'(G_0) \neq \gamma_1'(H_0)$.

• H_0 vom Typ ${}^2G_2(\bar{q}^2)$

In diesem Fall folgt aus $2\sqrt{3q^2} = \gamma_o - \gamma_u = \gamma_o(H_0) - \gamma_u(H_0) = 2\sqrt{3\bar{q}^2}$ unmittelbar $q = \bar{q}$ und damit $G_0 \cong H_0$.

1.5.9 G_0 vom Typ ${}^2D_p(3)$

Es ist $p = 2^m + 1$ mit $m \geqslant 2$ eine Fermat-Primzahl, insbesondere ist also m eine Potenz von 2. Weiter gilt $\gamma_o = \gamma_o(G_0) = \frac{1}{4}(3^p + 1)$, $\gamma_u = \gamma_u(G_0) = \frac{1}{2}(3^{p-1} + 1)$ und $\gamma_o - \gamma_u = \frac{1}{4}(3^{p-1} - 1)$. Für kleine m-Werte ergibt sich:

m	2	4
p	5	17
γ_o	61	$32285041 = 103 \cdot 307 \cdot 1021$
γ_u	41	21523361

- H_0 sporadisch-einfach bzw. Ausnahmegruppe

Anhand der Tabellen A.3 - A.5 sieht man leicht, dass keine der sporadisch-einfachen Gruppen bzw. Ausnahmegruppen ein Paar $(\gamma_o(H), \gamma_u(H)) = (\gamma_o, \gamma_u)$ liefert, das obiger Tabelle entspricht.

- H_0 alternierend

Ist $H_0 \cong A_6$, dann folgt aus $\gamma_o(H_0) - \gamma_u(H_0) = 4 = \frac{1}{4}(3^{p-1} - 1) = \gamma_o - \gamma_u$, dass $3^{p-1} = 17$ gelten muss, was unmöglich ist. Ist $H_0 \cong A_{\bar{p}}$, dann ist $\gamma_o(H_0) - \gamma_u(H_0) = 2$ und es folgt aus $\gamma_o(H_0) - \gamma_u(H_0) = 2 = \frac{1}{4}(3^{p-1} - 1) = \gamma_o - \gamma_u$, dass $p = 3$ gelten muss, im Widerspruch zu $p \geqslant 5$.

- H_0 vom Typ $A_1(\bar{q})$

Ist $H_0 \cong A_1(\bar{q})$ und $\bar{q} \equiv 0 \bmod 2$, dann ist $\gamma_o(H_0) - \gamma_u(H_0) = 2$. Daraus folgt wie im alternierenden Fall, dass $p = 3$ sein muss, was im Widerspruch zu $p \geqslant 5$ steht. Es ist also $\bar{q} \not\equiv 0 \bmod 2$ und damit $\bar{q} = \gamma_o(H_0) = \gamma_o = \frac{1}{4}(3^p + 1)$.

- Im Fall $\bar{q} \equiv 1 \bmod 4$ ist $\frac{1}{2}(\bar{q} + 1) = \gamma_u(H_0) = \gamma_u = \frac{1}{2}(3^{p-1} + 1)$. Es gilt also:

$$\bar{q} = 3^{p-1} = \frac{1}{4}(3^p + 1) = \frac{1}{4}(3 \cdot 3^{p-1} + 1) \implies 3^{p-1} = 1\,.$$

  Das ist aber unmöglich.

- Im Fall $\bar{q} \equiv 3 \bmod 4$ ist $\frac{1}{2}(\bar{q} - 1) = \gamma_u(H_0) = \gamma_u = \frac{1}{2}(3^{p-1} + 1)$. Also folgt:

$$\bar{q} = 3^{p-1} + 2 = \frac{1}{4}(3^p + 1) = \frac{1}{4}(3 \cdot 3^{p-1} + 1) \implies 3^{p-1} = -7\,.$$

  Das ist aber ebenfalls unmöglich.

• H_0 vom Typ $G_2(\bar{q})$

Ist $H_0 \cong G_2(\bar{q})$ mit $\bar{q} = 3^{\bar{f}}$, so muss

$$\gamma_o(H_0) - \gamma_u(H_0) = 2\bar{q} = \frac{1}{4}(3^{p-1} - 1) = \gamma_o - \gamma_u$$

gelten. Daraus folgt aber $8\bar{q} = 8 \cdot 3^{\bar{f}} = 3^{p-1} - 1$. Die rechte Seite ist aber, im Gegensatz zur linken Seite, nicht durch 3 teilbar.

• H_0 vom Typ ${}^2G_2(\bar{q}^2)$

Ist $H_0 \cong {}^2G_2(\bar{q}^2)$ mit $\bar{q}^2 = 3^{2\bar{m}+1}$ und $m \geqslant 1$, dann muss

$$\gamma_o(H_0) - \gamma_u(H_0) = 2\sqrt{3\bar{q}^2} = \frac{1}{4}(3^{p-1} - 1) = \gamma_o - \gamma_u$$

gelten. Daraus folgt aber nun $8\sqrt{3\bar{q}^2} = 8 \cdot 3^{\bar{m}+1} = 3^{p-1} - 1$. Wiederum ist die linke Seite durch 3 teilbar, die rechte aber nicht.

• H_0 vom Typ ${}^2D_{\bar{p}}(3)$

In diesem Fall folgt aus $\frac{1}{4}(3^{\bar{p}} + 1) = \gamma_o(H_0) = \gamma_o = \frac{1}{4}(3^p + 1)$ unmittelbar $\bar{p} = p$, und damit $G_0 \cong H_0$.

1.5.10 G_0 vom Typ ${}^2D_{p+1}(2)$

Es ist $p = 2^m - 1$ mit $m \geqslant 2$ eine Mersenne-Primzahl. Weiter ist $\gamma_o = \gamma_o(G_0) = 2^{p+1} + 1$, $\gamma_u = \gamma_u(G_0) = 2^p + 1$ und damit $\gamma_o - \gamma_u = 2^p$. Für kleine m- bzw. p-Werte ergibt sich folgende Tabelle:

m	2	3	5
p	3	5	31
γ_o	17	257	$4294967297 = 641 \cdot 6700417$
γ_u	3^2	$129 = 3 \cdot 43$	$2147483649 = 3 \cdot 715827883$

• H_0 sporadisch-einfach bzw. Ausnahmegruppe

Anhand der Tabellen A.3 - A.5 sieht man unmittelbar, dass keine der Gruppen als H_0 in Frage kommt, da keine der sporadisch-einfachen Gruppen bzw. Ausnahmegruppen ein Paar $(\gamma_o, \gamma_u) = (\gamma_o(H), \gamma_u(H))$ liefert, das obiger Tabelle entspricht.

- H_0 alternierend

Ist $H_0 \cong A_6$, dann folgt aus $\gamma_o(H_0) - \gamma_u(H_0) = 4 = 2^p = \gamma_o - \gamma_u$, dass $p = 2$ ist, im Widerspruch zu $p \geqslant 3$. Ist $H_0 \cong A_{\bar{p}}$, so folgt aus $\gamma_o(H_0) - \gamma_u(H_0) = 2 = 2^p = \gamma_o - \gamma_u$, dass $p = 1$ sein muss. Das ist aber ebenfalls unmöglich.

- H_0 vom Typ $A_1(\bar{q})$

  - Ist $\bar{q} \equiv 1 \bmod 4$, dann ist $\bar{q} = \bar{p}^{\bar{f}} = \gamma_o(H_0) = \gamma_o = 2^{p+1} + 1$. Nach [34, Lemma 1.2] hat diese Gleichung die Lösungen

    (1) $\bar{p} = 3$, $\bar{f} = 2$ und $p + 1 = 3$ oder

    (2) $\bar{f} = 1$, $p + 1 = 2^x$ und $\bar{p}$ ist eine Fermat-Primzahl.

    Im Fall (1) ist $p = 2$. Das ist aber wegen $m \geqslant 2$, d.h. $p \geqslant 3$ nicht möglich. Im Fall der zweiten Lösung ist $H_0 \cong A_1(\bar{p})$. Es ist dann $|H_0|/(\gamma_u\gamma_o) = \bar{p} - 1 = 2^{p+1}$ eine Potenz von 2. Da $|\mathrm{Out}(H_0)| = 2$ ist, ist auch $|H'|/(\gamma_u\gamma_o)$ eine 2-Potenz. Die Ordnung von G_0 ist

    $$|G_0| = 2^{p(p+1)}(2^p - 1)\underbrace{(2^p + 1)(2^{p+1} + 1)}_{\gamma_u\gamma_o}\prod_{i=1}^{p-1}(2^{2i} - 1)\,.$$

    Damit ist $|G_0|/(\gamma_u\gamma_o) = 2^{p(p+1)}(2^p-1)\prod_{i=1}^{p-1}(2^{2i}-1)$ keine 2-Potenz, und es gilt sicherlich $|G'| \neq |H'|$.

  - Ist $\bar{q} \equiv 3 \bmod 4$, dann ist $\bar{q} = \gamma_o(H_0) = \gamma_o = 2^{p+1} + 1$ und daher

    $$\gamma_u(H_0) = \frac{1}{2}(\bar{q} - 1) = \frac{1}{2}(2^{p+1}) = 2^p \neq 2^p + 1 = \gamma_u\,.$$

  - Ist $\bar{q} \equiv 0 \bmod 2$, dann gilt:

    $$\gamma_o(H_0) - \gamma_u(H_0) = \bar{q} + 1 - (\bar{q} - 1) = 2 = 2^p = \gamma_o - \gamma_u \implies p = 1\,.$$

    Das ist aber unmöglich.

- H_0 vom Typ $G_2(\bar{q})$

Ist $H_0 \cong G_2(\bar{q})$, gilt $\bar{q}^2 + \bar{q} + 1 = \gamma_o(H_0) = \gamma_o = 2^{p+1} + 1$. Damit folgt $\bar{q}(\bar{q} + 1) = 2^{p+1}$. Das ist unmöglich, da die linke Seite sicherlich keine 2-Potenz ist.

- H_0 vom Typ ${}^2G_2(\bar{q}^2)$

Ist $H_0 \cong {}^2G_2(\bar{q}^2)$ mit $\bar{q}^2 = 3^{2\bar{m}+1}$ und $\bar{m} \geqslant 1$, dann ist

$$\bar{q}^2 + \sqrt{3\bar{q}^2} + 1 = \gamma_o(H_0) = \gamma_o = 3^{2\bar{m}+1} + 3^{\bar{m}+1} + 1 = 2^{p+1} + 1\,.$$

Daraus folgt $3^{\bar{m}+1}(3^{\bar{m}}+1) = 2^{p+1}$. Da die linke Seite wiederum keine 2-Potenz ist, ist dies unmöglich.

• H_0 vom Typ ${}^2D_{\bar{p}}(3)$

Ist $H_0 \cong {}^2D_{\bar{p}}(3)$, dann gilt:

$$\frac{1}{4}(3^{\bar{p}}+1) = \gamma_o(H_0) = \gamma_o = 2^{p+1}+1 \implies 3^{\bar{p}} - 3 = 4 \cdot 2^{p+1} = 2^{p+3}.$$

Auch hier ist die linke Seite keine 2-Potenz, und der Fall ist unmöglich.

• H_0 vom Typ ${}^2D_{\bar{p}+1}(2)$

In diesem Fall folgt aus $\gamma_o(H_0) = \frac{1}{4}(3^{\bar{p}}+1) = \frac{1}{4}(3^p+1) = \gamma_o$ unmittelbar $\bar{p} = p$, und damit $G_0 \cong H_0$.

1.5.11 G_0 vom Typ $F_4(q)$

Es ist $q = 2^m$, $\gamma_o = \gamma_o(G_0) = q^4+1$ und $\gamma_u = \gamma_u(G_0) = q^4 - q^2 + 1$. Insbesondere ist $\gamma_o - \gamma_u = q^2$. Für kleine q-Werte ergibt sich die folgende Tabelle für γ_o bzw. γ_u.

q	2^1	2^2	2^3	2^4
γ_o	17	257	$4097 = 17 \cdot 241$	65537
γ_u	13	241	$4033 = 37 \cdot 109$	$65281 = 97 \cdot 673$

• H_0 sporadisch-einfach bzw. Ausnahmegruppe

Vergleicht man obige Tabelle mit den Tabellen A.3 - A.5, so sieht man, dass nur $H_0 \cong {}^2E_6(2)$ mit $G_0 \cong F_4(2)$ in Frage kommt. Es gilt dann

$$|G_0| = 2^{24} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 17 \quad \text{und} \quad |H_0| = 2^{36} \cdot 3^{10} \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19\,.$$

Weiter gilt $|\mathrm{Out}(G_0)| = 2$ und damit $11, 19 \notin \pi(G')$, im Widerspruch zu $11 \cdot 19 \,\big|\, |H_0|$.

• H_0 alternierend

Ist $H_0 \cong A_6$, dann ist $4 = \gamma_o(H_0) - \gamma_u(H_0) = \gamma_o - \gamma_u = q^2$, und damit muss $q = 2$ gelten. Wie im vorherigen Fall ist dann $|G_0| = 2^{24} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 17$. Wegen $|\mathrm{Aut}(H_0)| = 2^4 \cdot 3^2 \cdot 5$ gilt stets $|H'| < |G'|$. Ist $H_0 \cong A_{\bar{p}}$, so gilt stets $\gamma_o - \gamma_u = 2 \neq q^2$.

- H_0 vom Typ $A_1(\bar{q})$

  - Ist $\bar{q} \equiv 0 \bmod 2$, so muss $\bar{q}+1-(\bar{q}-1) = 2 = \gamma_o(H_0)-\gamma_u(H_0) = \gamma_o-\gamma_u = q^2$ gelten, was unmöglich ist.
  - Ist $q \equiv 1 \bmod 4$, dann ist $\bar{q} = \gamma_o(H_0) = \gamma_o = q^4+1$ und es folgt:

    $$\frac{1}{2}(\bar{q}+1) = \gamma_u(H_0) = \gamma_u = \frac{1}{2}(q^4+2) = q^4-q^2+1 \implies q^4 = 2q^2 \implies q^2 = 2\,.$$

    Das ist aber ebenfalls nicht möglich.
  - Ist $q \equiv 3 \bmod 4$, dann ist $\bar{q} = \gamma_o(H_0) = \gamma_o = q^4+1$ und es folgt:

    $$\frac{1}{2}(\bar{q}-1) = \gamma_u(H_0) = \gamma_u = \frac{1}{2}(q^4) = q^4-q^2+1 \implies q^4 = 2q^2-2 = 2(q^2-1)\,.$$

    Auch dieser Fall ist also unmöglich.

- H_0 vom Typ $G_2(\bar{q})$

Ist $H_0 \cong G_2(\bar{q})$ mit $\bar{q} = 3^{\bar{f}}$, dann muss $\bar{q}^2+\bar{q}+1 = \gamma_o(H_0) = \gamma_o = q^4+1$ und damit $\bar{q}(\bar{q}+1) = q^4$ gelten. Das ist aber nicht möglich, da die linke Seite, im Gegensatz zur rechten, von 3 geteilt wird.

- H_0 vom Typ ${}^2G_2(\bar{q}^2)$

In diesem Fall ist $\bar{q}^2 = 3^{2\bar{m}+1}$ und es muss

$$\bar{q}^2+\sqrt{3\bar{q}}+1 = \gamma_o(H_0) = \gamma_o = 3^{2\bar{m}+1}+3^{\bar{m}+1}+1 = 3^{\bar{m}+1}(3^{\bar{m}}+1)+1 = q^4+1\,,$$

und damit $3^{\bar{m}+1}(3^{\bar{m}}+1) = q^4$ gelten. Das ist aber wiederum wegen $q \equiv 0 \bmod 2$ unmöglich.

- H_0 vom Typ ${}^2D_{\bar{p}}(3)$

Hier gilt $\frac{1}{4}(3^{\bar{p}}+1) = \gamma_o(H_0) = \gamma_o = q^4+1$ und damit $3^{\bar{p}}-3 = 4q^4$. Auch hier ist die rechte Seite wegen $q \equiv 0 \bmod 2$ nicht durch 3 teilbar.

- H_0 vom Typ ${}^2D_{\bar{p}+1}(2)$

Es muss $2^{\bar{p}} = \gamma_o(H_0)-\gamma_u(H_0) = \gamma_o-\gamma_u = q^2 = 2^{2f}$ gelten. Also folgt $\bar{p} = 2f$, was wegen $\bar{p} \geqslant 3$ prim unmöglich ist.

- H_0 vom Typ $F_4(\bar{q})$

In diesem Fall folgt aus $q^2 = \gamma_o-\gamma_u = \gamma_o(H_0)-\gamma_u(H_0) = \bar{q}^2$ unmittelbar $q = \bar{q}$ und damit $H_0 \cong G_0$.

1.5.12 G_0 vom Typ ${}^2F_4(q)$

Es ist $q = 2^{2m+1}$ mit $m \geqslant 1$. Weiter ist $\gamma_o = \gamma_o(G_0) = q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1$ und $\gamma_u = \gamma_u(G_0) = q^2 - \sqrt{2q^3} + q - \sqrt{2q} + 1$, also $\gamma_o - \gamma_u = 2\left(\sqrt{2q^3} + \sqrt{2q}\right) = 2^{m+2}(2^{2m+1}+1)$. Für kleine Werte von q ergeben sich die folgenden γ_o- und γ_u-Werte :

q	2^3	2^5	2^7
γ_o	109	1321	$18577 = 13 \cdot 1429$
γ_u	37	$793 = 13 \cdot 61$	14449

- H_0 sporadisch-einfach bzw. Ausnahmegruppe

Durch vergleichen der obigen Tabelle mit den Tabellen A.3 - A.5 sieht man unmittelbar, dass keine sporadisch-einfache Gruppe bzw. Ausnahmegruppe als H_0 in Frage kommt.

- H_0 alternierend

Ist H_0 alternierend, dann ist $2^\varepsilon = \gamma_o(H_0) - \gamma_u(H_0) \neq \gamma_o - \gamma_u = 2^{m+2}(2^{2m+1} + 1)$, da die rechte Seite keine Potenz von 2 ist (dabei ist wieder $\varepsilon = 2$ für $H_0 \cong A_6$ und $\varepsilon = 1$ in den übrigen Fällen).

- H_0 vom Typ $A_1(\bar{q})$

  - Ist $\bar{q} \equiv 0 \bmod 2$, dann muss
    $$\bar{q} + 1 - (\bar{q} - 1) = 2 = \gamma_o(H_0) - \gamma_u(H_0) = \gamma_o - \gamma_u = 2\left(\sqrt{2q^3} + \sqrt{2q}\right)$$
    gelten, was unmöglich ist.
  - Ist $\bar{q} \equiv 1 \bmod 4$, dann ist
    $$\frac{1}{2}(\bar{q} - 1) = \gamma_o(H_0) - \gamma_u(H_0) = \gamma_o - \gamma_u = 2\left(\sqrt{2q^3} + \sqrt{2q}\right).$$
    Damit muss
    $$\bar{q} = 4\left(\sqrt{2q^3} + \sqrt{2q}\right) + 1 = q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1$$
    gelten, und es folgt
    $$3\left(\sqrt{2q^3} + \sqrt{2q}\right) = q^2 + q = q(q+1).$$
    Mit $q = 2^{2m+1}$ ergibt sich dann:
    $$3\left(\sqrt{2^{6m+3+1}} + \sqrt{2^{2m+1+1}}\right) = 3(2^{3m+2} + 2^{m+1}) = 2^{2m+1}(2^{2m+1} + 1)$$
    $$\implies \quad 3(2^{2m+1} + 1) = 2^m(2^{2m+1} + 1).$$
    Die linke Seite ist aber offensichtlich ungleich der rechten Seite.

- Ist $\bar{q} \equiv 3 \bmod 4$, dann ist

$$\frac{1}{2}(\bar{q}+1) = \gamma_o(H_0) - \gamma_u(H_0) = \gamma_o - \gamma_u = 2\left(\sqrt{2q^3} + \sqrt{2q}\right).$$

  Damit muss

$$\bar{q} = 4\left(\sqrt{2q^3} + \sqrt{2q}\right) - 1 = q^2 + \sqrt{2q^3} + q + \sqrt{2q} + 1$$

  gelten, und es folgt

$$3\left(\sqrt{2q^3} + \sqrt{2q}\right) - 2 = q^2 + q = q(q+1).$$

  Mit $q = 2^{2m+1}$ ergibt sich dann:

$$\begin{aligned} & 3\left(\sqrt{2^{6m+3+1}} + \sqrt{2^{2m+1+1}}\right) - 2 = 3(2^{3m+2} + 2^{m+1}) - 2 = 2^{2m+1}(2^{2m+1}+1) \\ \Longrightarrow\ & 3(2^{3m+1} + 2^m) - 1 = 2^{2m}(2^{2m+1}+1). \end{aligned}$$

  Liest man diese Gleichung modulo 2, dann gilt $1 = 1\cdot(0+0)+1 = 0\cdot(0+1) = 0$. Dieser Fall ist also ebenfalls nicht möglich.

- H_0 vom Typ $G_2(\bar{q})$

Es ist $\bar{q} \equiv 0 \bmod 3$, und es muss

$$2\bar{q} = \gamma_o(H_0) - \gamma_u(H_0) = \gamma_o - \gamma_u = 2^{m+2}(2^{2m+1}+1)$$

gelten. Da $\bar{q}$ ungerade ist, ist dies nicht möglich, da die linke Seite nicht durch 4 teilbar ist.

- H_0 vom Typ ${}^2G_2(\bar{q}^2)$

Wiederum ist $\bar{q} \equiv 0 \bmod 3$, und es muss

$$2\sqrt{3\bar{q}^2} = \gamma_o(H_0) - \gamma_u(H_0) = \gamma_o - \gamma_u = 2^{m+2}(2^{2m+1}+1)$$

gelten. Da $\bar{q}$ ungerade ist, wird auch hier die linke Seite nicht von 4 geteilt. Damit ist auch dieser Fall nicht möglich.

- H_0 vom Typ ${}^2D_{\bar{p}}(3)$

Es muss

$$\frac{1}{4}(3^{\bar{p}-1} - 1) = \gamma_o(H_0) - \gamma_u(H_0) = \gamma_o - \gamma_u = 2^{m+2}(2^{2m+1}+1)$$

gelten, also

$$3^{\bar{p}-1} - 1 = 2^{m+4}(2^{2m+1}+1).$$

Andererseits ist

$$\frac{1}{2}(3^{\bar{p}-1}+1) = \gamma_u(H_0) = \gamma_u = 2^{4m+2} - 2^{3m+2} + 2^{2m+1} - 2^{m+1} + 1\,.$$

Dies liefert

$$3^{\bar{p}-1} - 1 = 2(2^{4m+2} - 2^{3m+2} + 2^{2m+1} - 2^{m+1} + 1) - 2 = 2^{m+2}(2^{3m+1} - 2^{2m+1} + 2^m - 1)\,.$$

Zusammengefasst muss also

$$2^{m+4}(2^{2m+1}+1) = 2^{m+2}(2^{3m+1} - 2^{2m+1} + 2^m - 1)$$

sein, was offensichtlich unmöglich ist.

- H_0 vom Typ ${}^2D_{\bar{p}+1}(2)$

Es muss

$$2^{\bar{p}} = \gamma_o(H_0) - \gamma_u(H_0) = \gamma_o - \gamma_u = 2\left(\sqrt{2q^3} + \sqrt{2q}\right)$$

gelten. Mit $q = 2^{2m+1}$ folgt

$$2^{\bar{p}} = 2(2^{3m+2} + 2^{m+1}) = 2^{m+2}(2^{2m}+1)\,.$$

Das ist aber unmöglich.

- H_0 vom Typ $F_4(\bar{q})$

Es muss

$$\bar{q}^2 = \gamma_o(H_0) - \gamma_u(H_0) = \gamma_o - \gamma_u = 2\left(\sqrt{2q^3} + \sqrt{2q}\right)$$

gelten. Mit $\bar{q} = 2^{\bar{f}}$ und $q = 2^{2m+1}$ folgt

$$2^{\bar{f}} = 2(2^{3m+2} + 2^{m+1}) = 2^{m+2}(2^{2m}+1)\,.$$

Das ist aber unmöglich.

- H_0 vom Typ ${}^2F_4(\bar{q})$

In diesem Fall folgt aus

$$2^{m+2}(2^{2m+1}+1) = \gamma_o(H_0) - \gamma_u(H_0) = \gamma_o - \gamma_u = 2^{\bar{m}+2}(2^{2\bar{m}+1}+1)$$

unmittelbar $m = \bar{m}$, und damit $H_0 \cong G_0$.

1.5.13 G_0 vom Typ $E_8(q)$

Für $q \equiv 2, 3 \bmod 5$ gilt $|\Gamma(G_0)| = 4$ und im Fall $q \equiv 0, 1, 4 \bmod 5$ ist $|\Gamma(G_0)| = 5$. Im letzteren Fall ist die Nummerierung der $\gamma_i(G_0)$ nicht mehr nach der Größe aufsteigend gewählt! Die Nummerierung der $\gamma_i(G_0)$ ist mit

$$\begin{aligned}
\gamma_2(G_0) &= q^8 - q^7 + q^5 - q^4 + q^3 - q + 1\,,\\
\gamma_3(G_0) &= q^8 - q^4 + 1\,,\\
\gamma_4(G_0) &= q^8 + q^7 - q^5 - q^4 - q^3 + q + 1\,,\\
\gamma_5(G_0) &= q^8 - q^6 + q^4 - q^2 + 1 \qquad\qquad (\text{im Fall } \ q \equiv 0, 1, 4 \bmod 5)\,,
\end{aligned}$$

also

$$\gamma_2(G_0) < \gamma_5(G_0) < \gamma_3(G_0) < \gamma_4(G_0)\,,$$

so gewählt, dass die Fälle $|\Gamma(G_0)| = 4$ und $|\Gamma(G_0)| = 5$ gemeinsam behandelt werden können. Es gilt dann

$$\begin{aligned}
\gamma_4(G_0) - \gamma_3(G_0) &= q^7 - q^5 - q^3 + q &&= q(q-1)^2(q+1)^2(q^2+1)\\
\gamma_4(G_0) - \gamma_5(G_0) &= q^7 + q^6 - q^5 - 2q^4 - q^3 + q^2 + q &&= q(q-1)^2(q+1)^2(q^2+q+1)\\
\gamma_4(G_0) - \gamma_2(G_0) &= 2q^7 - 2q^5 - 2q^3 - 2q &&= 2q(q-1)^2(q+1)^2(q^2+1)\\
\\
\gamma_3(G_0) - \gamma_5(G_0) &= q^6 - 2q^4 + q^2 &&= q^2(q-1)^2(q+1)^2\\
\gamma_3(G_0) - \gamma_2(G_0) &= q^7 - q^5 - q^3 + q &&= q(q-1)^2(q+1)^2(q^2+1)\\
\\
\gamma_5(G_0) - \gamma_2(G_0) &= q^7 - q^6 - q^5 + 2q^4 - q^3 - q^2 + q &&= q(q-1)^2(q+1)^2(q^2-q+1)\,.
\end{aligned}$$

Es gilt sicherlich $(q-1, q+1) = 2$. Damit sind $\frac{q-1}{2}$ und $\frac{q+1}{2}$ teilerfremd und $\gamma_o - \gamma_u$ wird in jedem Fall von mindestens drei verschiedenen Primzahlen geteilt, d.h. $|\pi(\gamma_o - \gamma_u)| \geqslant 3$.

Für kleine Werte von q ergibt sich die folgende Tabelle.

q	2	3	4	5	7
γ_2	151	4561	$49981 = 151 \cdot 331$	$315121 = 181 \cdot 1741$	$4956001 = 31 \cdot 159871$
γ_3	241	6481	$65281 = 97 \cdot 673$	390001	$5762401 = 73 \cdot 193 \cdot 409$
γ_4	331	$8401 = 31 \cdot 271$	$80582 = 61 \cdot 1321$	$464881 = 61 \cdot 7621$	6568801
γ_5	–	–	61681	$375601 = 41 \cdot 9161$	–

In Γ muss nach Lemma 1.11 eine, bzw. zwei der Komponenten $\Gamma_i(G_0)$ $(i \geqslant 2)$ mit der Komponente $\Gamma_1(G_0)$ fusionieren. Den beiden verbleibenden Komponenten, die 2 nicht enthalten, kann dann γ_o und γ_u zugeordnet werden.

• H_0 sporadisch-einfach bzw. Ausnahmegruppe

Durch Vergleichen der obigen Tabelle mit den Tabellen A.3 - A.5 sieht man wiederum unmittelbar, dass keine sporadisch-einfache Gruppe, bzw. Ausnahmegruppe für H_0 in Betracht kommt.

• H_0 alternierend

Ist H_0 alternierend, dann gilt $\gamma_o - \gamma_u = \gamma_o(H_0) - \gamma_u(H_0) = 2^x$. Obige Rechnung zeigt aber, dass $\gamma_o - \gamma_u$ stets von mindestens drei verschiedenen Primzahlen geteilt wird, im Widerspruch zu einem alternierenden H_0.

• H_0 vom Typ $A_1(\bar{q})$

- Ist $\bar{q} \equiv 0 \bmod 2$, dann muss $\gamma_o - \gamma_u = \gamma_o(H_0) - \gamma_u(H_0) = \bar{q} + 1 - (\bar{q} - 1) = 2$ gelten, was nach dem vorangegangenen Argument unmöglich ist.
- Ist $\bar{q} \equiv 1 \bmod 4$, dann ist $\gamma_u = \gamma_u(H_0) = \frac{1}{2}(\bar{q} + 1)$ und $\gamma_o = \gamma_o(H_0) = \bar{q}$.
  - Ist $\gamma_o = \gamma_4(G_0) = q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$, dann ist

    $$\frac{1}{2}(\bar{q} + 1) = \gamma_2(H_0) = \gamma_u \geqslant \gamma_2(G_0) = q^8 - q^7 + q^5 - q^4 + q^3 - q + 1\,.$$

    Wegen $2\gamma_u - 1 = \gamma_o$ ist dann

    $$q^8 + q^7 - q^5 - q^4 - q^3 + q + 2 = \gamma_o + 1 = 2\gamma_u \geqslant 2(q^8 - q^7 + q^5 - q^4 + q^3 - q + 1)\,,$$

    und damit folgt:

    $$-q^8 + 3q^7 - 3q^5 + q^4 - 3q^3 + 3q \geqslant 0 \implies q < 3\,.$$

    Es ist also $q = 2$ und damit $\gamma_o = 331$ sowie $\gamma_u = 166 \equiv 0 \bmod 2$, im Widerspruch zu einem ungeradem γ_u.
  - Ist $\gamma_o = \gamma_3(G_0) = q^8 - q^4 + 1$, dann ist

    $$\frac{1}{2}(\bar{q} + 1) = \gamma_2(H_0) = \gamma_u \geqslant \gamma_2(G_0) = q^8 - q^7 + q^5 - q^4 + q^3 - q + 1\,.$$

    Wegen $2\gamma_u - 1 = \gamma_o$ ist dann

    $$q^8 - q^4 + 2 = \gamma_o + 1 = 2\gamma_u \geqslant 2(q^8 - q^7 + q^5 - q^4 + q^3 - q + 1)\,,$$

    und damit folgt

    $$-q^8 + q^7 - 2q^5 + q^4 - 2q^3 + q \geqslant 0\,,$$

    was aber nicht möglich ist.

- Ist $\gamma_o = \gamma_5(G_0) = q^8 - q^6 + q^4 - q^2 + 1$, dann ist
$$\frac{1}{2}(\bar{q} + 1) = \gamma_2(H_0) = \gamma_u = \gamma_2(G_0) = q^8 - q^7 + q^5 - q^4 + q^3 - q + 1\,.$$
Wegen $2\gamma_u - 1 = \gamma_o$ ist dann
$$q^8 - q^6 + q^4 - q^2 + 2 = \gamma_o + 1 = 2\gamma_u \geqslant 2(q^8 - q^7 + q^5 - q^4 + q^3 - q + 1)\,,$$
und damit folgt
$$-q^8 + q^7 - q^6 - 2q^5 + 3q^4 - 2q^3 - q^2 + 2q \geqslant 0\,,$$
was aber ebenfalls unmöglich ist.

- Ist $\bar{q} \equiv 3 \bmod 4$, dann ist $\gamma_u = \gamma_u(H_0) = \frac{1}{2}(\bar{q} - 1)$ und $\gamma_o = \gamma_o(H_0) = \bar{q}$.
  - Ist $\gamma_o = \gamma_4(G_0) = q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$, dann ist
  $$\frac{1}{2}(\bar{q} - 1) = \gamma_2(H_0) = \gamma_u \geqslant \gamma_2(G_0) = q^8 - q^7 + q^5 - q^4 + q^3 - q + 1\,.$$
  Wegen $2\gamma_u + 1 = \gamma_o$ ist dann
  $$q^8 + q^7 - q^5 - q^4 - q^3 + q = \gamma_o - 1 = 2\gamma_u \geqslant 2(q^8 - q^7 + q^5 - q^4 + q^3 - q + 1)\,,$$
  und damit folgt:
  $$-q^8 + 3q^7 - 3q^5 + q^4 - 3q^3 + 3q - 2 \geqslant 0 \implies q < 3\,.$$
  Also ist $q = 2$ und damit $\gamma_o = 331$ und $\gamma_u = 166 \equiv 0 \bmod 2$, im Widerspruch zu einem ungeradem γ_u.
  - Ist $\gamma_o = \gamma_3(G_0) = q^8 - q^4 + 1$, dann ist
  $$\frac{1}{2}(\bar{q} - 1) = \gamma_2(H_0) \geqslant \gamma_u = \gamma_2(G_0) = q^8 - q^7 + q^5 - q^4 + q^3 - q + 1\,.$$
  Wegen $2\gamma_u + 1 = \gamma_o$ gilt dann
  $$q^8 - q^4 + 2 = \gamma_o - 1 = 2\gamma_u \geqslant 2(q^8 - q^7 + q^5 - q^4 + q^3 - q + 1)\,,$$
  und damit folgt
  $$-q^8 + q^7 - 2q^5 + q^4 - 2q^3 + q - 2 \geqslant 0\,,$$
  was aber nicht möglich ist.
  - Ist $\gamma_o = \gamma_5(G_0) = q^8 - q^6 + q^4 - q^2 + 1$, dann ist
  $$\frac{1}{2}(\bar{q} - 1) = \gamma_2(H_0) = \gamma_u = \gamma_2(G_0) = q^8 - q^7 + q^5 - q^4 + q^3 - q + 1\,,$$
  und wegen $2\gamma_u + 1 = \gamma_o$ folgt
  $$q^8 - q^6 + q^4 - q^2 = \gamma_o - 1 = 2\gamma_u \geqslant 2(q^8 - q^7 + q^5 - q^4 + q^3 - q + 1)\,.$$
  Damit ist
  $$-q^8 + q^7 - q^6 - 2q^5 + 3q^4 - 2q^3 - q^2 + 2q - 2 \geqslant 0\,,$$
  was aber ebenfalls unmöglich ist.

- H_0 vom Typ $G_2(\bar{q})$

Es ist $\bar{q} = 3^{\bar{f}}$, $\gamma_o = \gamma_o(H_0) = \bar{q}^2 + \bar{q} + 1$, $\gamma_u = \gamma_u(H_0) = \bar{q}^2 - \bar{q} + 1$ und damit $\gamma_o - \gamma_u = 2\bar{q}$. Insbesondere gilt also $|\pi(\gamma_o - \gamma_u)| = 2$. Das steht aber im Widerspruch zu obiger Betrachtung, nach der in jedem Fall $|\pi(\gamma_o - \gamma_u)| \geqslant 3$ ist.

- H_0 vom Typ ${}^2G_2(\bar{q}^2)$

Es ist $\bar{q}^2 = 3^{2\bar{m}+1}$, $\gamma_o = \gamma_o(H_0) = \bar{q}^2 + \sqrt{3\bar{q}^2} + 1$ und $\gamma_u = \gamma_u(H_0) = \bar{q}^2 - \sqrt{3\bar{q}^2} + 1$. Wegen $\gamma_o - \gamma_u = 2\sqrt{3\bar{q}^2} = 2 \cdot 3^{\bar{m}+1}$ gilt auch hier wieder $|\pi(\gamma_o - \gamma_u)| = 2$, was im Widerspruch zu $|\pi(\gamma_o - \gamma_u)| \geqslant 3$ steht.

- H_0 vom Typ ${}^2D_{\bar{p}}(3)$

Es gilt $\gamma_o = \gamma_o(H_0) = \frac{1}{4}(3^{\bar{p}} + 1)$, $\gamma_u = \gamma_u(H_0) = \frac{1}{2}(3^{\bar{p}-1} + 1)$ und $\gamma_o - \gamma_u = \frac{1}{4}(3^{\bar{p}-1} - 1)$.

- Ist $\gamma_u = \gamma_3(G_0) = q^8 - q^4 + 1$, dann ist $\gamma_o = \gamma_4(G_0)$, und es gilt

$$\gamma_o - \gamma_u = \frac{1}{4}(3^{\bar{p}-1} - 1) = q(q^6 - q^4 - q^2 + 1)$$

und damit

$$3^{\bar{p}-1} + 1 = 4q(q^6 - q^4 - q^2 + 1) + 2\,.$$

Es ist dann aber

$$\gamma_u = q^8 - q^4 + 1 = \frac{1}{2}(3^{\bar{p}-1} + 1) = 2q(q^6 - q^4 - q^2 + 1) + 1$$

und damit

$$q^4(q^4 - 1) = 2q(q^6 - q^4 - q^2 + 1)\,,$$

was unmöglich ist.

- Ist $\gamma_u = \gamma_5(G_0) = q^8 - q^6 + q^4 - q^2 + 1$, dann ist $\gamma_o \in \{\gamma_4(G_0), \gamma_3(G_0)\}$.
  Ist $\gamma_o = \gamma_4(G_0)$, dann gilt

$$\gamma_o - \gamma_u = \frac{1}{4}(3^{\bar{p}-1} - 1) = q(q^6 + q^5 - q^4 - 2q^3 - q^2 + q + 1)$$

und damit

$$3^{\bar{p}-1} + 1 = 4q(q^6 + q^5 - q^4 - 2q^3 - q^2 + q + 1) + 2\,.$$

Es ist dann aber

$$\gamma_u = q^8 - q^6 + q^4 - q^2 + 1 = \frac{1}{2}(3^{p-1} + 1) = 2q(q^6 + q^5 - q^4 - 2q^3 - q^2 + q + 1) + 1\,,$$

d.h.

$$q^2(q^6 - q^4 + q^2 - 1) = 2q(q^6 + q^5 - q^4 - 2q^3 - q^2 + q + 1)\,.$$

Das ist aber unmöglich.

Ist $\gamma_o = \gamma_3(G_0)$, dann gilt

$$\gamma_o - \gamma_u = \frac{1}{4}(3^{p-1} - 1) = q^2(q^4 - 2q^2 + 1)\,,$$

und damit

$$3^{\bar{p}-1} + 1 = 4q^2(q^4 - 2q^2 + 1) + 2\,.$$

Dann ist aber

$$\gamma_u = q^8 - q^6 + q^4 - q^2 + 1 = \frac{1}{2}(3^{\bar{p}-1} + 1) = 2q^2(q^4 - 2q^2 + 1) + 1\,,$$

und somit folgt:

$$q^2(q^6 - q^4 + q^2 - 1) = 2q^2(q^4 - 2q^2 + 1) \implies q^6 - 3q^4 + 3q^2 - 3 = 0 \implies q = 3^f\,.$$

Insgesamt ist dann

$$0 = 3^{6f-1} - 3^{4f} + 3^{2f} - 1 > 0\,.$$

- Ist $\gamma_u = \gamma_2(G_0) = q^8 - q^7 + q^5 - q^4 + q^3 - q + 1$, dann ist $\gamma_o \in \{\gamma_4(G_0), \gamma_3(G_0), \gamma_5(G_0)\}$.

  Ist $\gamma_o = \gamma_4(G_0)$, dann gilt

  $$\gamma_o - \gamma_u = \frac{1}{4}(3^{\bar{p}-1} - 1) = q^2(2q^5 - 2q^3 - 2q + 2\,,)$$

  und damit

  $$3^{\bar{p}-1} + 1 = 4q^2(2q^5 - 2q^3 - 2q + 2) + 2\,.$$

  Dann ist aber

  $$\gamma_u = q^8 - q^7 + q^5 - q^4 + q^3 - q + 1 = \frac{1}{2}(3^{\bar{p}-1} + 1) = 2q^2(2q^5 - 2q^3 - 2q + 2) + 1\,,$$

  und damit

  $$q(q^7 - q^6 + q^4 - q^3 + q^2 - 1) = 2q^2(2q^5 - 2q^3 - 2q + 2)\,,$$

  was unmöglich ist.

  Ist $\gamma_o = \gamma_3(G_0)$, dann gilt

  $$\gamma_o - \gamma_u = \frac{1}{4}(3^{\bar{p}-1} - 1) = q(q^6 - q^4 - q^2 + 1)\,,$$

  also

  $$3^{\bar{p}-1} + 1 = 4q(q^6 - q^4 - q^2 + 1) + 2\,.$$

  Dann ist aber

  $$\gamma_u = q^8 - q^7 + q^5 - q^4 + q^3 - q + 1 = \frac{1}{2}(3^{\bar{p}-1} + 1) = 2q(q^6 - q^4 - q^2 + 1) + 1\,,$$

und somit folgt:

$$q(q^7-q^6+q^4-q^3+q^2-1) = 2q(q^6-q^4-q^2+1) \Rightarrow q^7-3q^6+3q^4-q^3+3q^2-3 = 0\,.$$

Es muss also $q \leqslant 3$ gelten. Für $q \leqslant 3$ ist die linke Seite aber ungleich 0.
Ist $\gamma_o = \gamma_5(G_0)$, dann gilt

$$\gamma_o - \gamma_u = \frac{1}{4}(3^{\bar{p}-1}-1) = q(q^6-q^5-q^4+2q^3-q^2-q+1)\,,$$

und damit

$$3^{\bar{p}-1}+1 = 4q(q^6-q^5-q^4+2q^3-q^2-q+1)+2\,.$$

Dann ist aber

$$\gamma_u = q^8-q^7+q^5-q^4+q^3-q+1 = \frac{1}{2}(3^{\bar{p}-1}+1) = 2q(q^6-q^5-q^4+2q^3-q^2-q+1)+1\,,$$

und damit

$$q(q^7-q^6+q^4-q^3+q^2-1) = 2q(q^6-q^5-q^4+2q^3-q^2-q+1)\,.$$

Daraus folgt:

$$q^7-3q^6+2q^5+3q^4-5q^3+3q^2+2q-3 = 0 \implies q < 3\,.$$

Für $q = 2$ ist die linke Seite aber ungleich 0.

- H_0 vom Typ ${}^2D_{\bar{p}+1}(2)$

Es ist $\gamma_o = \gamma_o(H_0) = 2^{\bar{p}+1}+1$, $\gamma_u = \gamma_u(H_0) = 2^{\bar{p}}+1$ und $\gamma_o - \gamma_u = 2^{\bar{p}}$. Da $\gamma_o - \gamma_u$ nach obigem aber von mindestens drei verschiedenen Primzahlen geteilt wird, ist dieser Fall nicht möglich.

- H_0 vom Typ $F_4(\bar{q})$

Hier ist $\gamma_o = \gamma_o(H_0) = \bar{q}^4+1$, $\gamma_u = \gamma_u(H_0) = \bar{q}^4-\bar{q}^2+1$ und $\gamma_o - \gamma_u = \bar{q}^2$. Auch dieser Fall ist also wieder unmöglich, da $\gamma_o - \gamma_u$ mindestens drei verschiedene Primteiler besitzt.

- H_0 vom Typ ${}^2\mathsf{F}_4(\bar{\mathfrak{q}})$

Es ist $\bar{\mathfrak{q}} = 2^{2\bar{\mathfrak{m}}+1} > 2$ und für $\gamma_o = \gamma_o(\mathsf{H}_0)$ und $\gamma_u = \gamma_u(\mathsf{H}_0)$ gilt das folgende:

$$\begin{aligned}
\gamma_o - 1 \quad &= \quad \bar{\mathfrak{q}}^2 + \sqrt{2\bar{\mathfrak{q}}^3} + \bar{\mathfrak{q}} + \sqrt{2\bar{\mathfrak{q}}} \quad &= \quad 2^{4\bar{\mathfrak{m}}+2} + 2^{3\bar{\mathfrak{m}}+2} + 2^{2\bar{\mathfrak{m}}+1} + 2^{\bar{\mathfrak{m}}+1} \\
&&= \quad (2^{\bar{\mathfrak{m}}}+1)(2^{3\bar{\mathfrak{m}}+2} + 2^{\bar{\mathfrak{m}}+1}) \\
&&= \quad 2^{\bar{\mathfrak{m}}+1}(2^{\bar{\mathfrak{m}}}+1)(2^{2\bar{\mathfrak{m}}+1}+1) \qquad (1) \\
\gamma_u - 1 \quad &= \quad \bar{\mathfrak{q}}^2 - \sqrt{2\bar{\mathfrak{q}}^3} + \bar{\mathfrak{q}} - \sqrt{2\bar{\mathfrak{q}}} \quad &= \quad 2^{\bar{\mathfrak{m}}+1}(2^{\bar{\mathfrak{m}}}-1)(2^{2\bar{\mathfrak{m}}+1}+1) \qquad (2) \\
\gamma_o + \gamma_u - 2 \quad &= \quad 2(\bar{\mathfrak{q}}^2 + \bar{\mathfrak{q}}) \quad &= \quad 2^{2\bar{\mathfrak{m}}+2}(2^{2\bar{\mathfrak{m}}+1}+1) \qquad (3) \\
&&= \quad 2^{2\bar{\mathfrak{m}}+2}(2^{\bar{\mathfrak{m}}+1}(2^{\bar{\mathfrak{m}}}-1) + 2(2^{\bar{\mathfrak{m}}}-1) + 3) \qquad (4) \\
&&= \quad 2^{2\bar{\mathfrak{m}}+2}(2^{\bar{\mathfrak{m}}+1}(2^{\bar{\mathfrak{m}}}+1) - 2(2^{\bar{\mathfrak{m}}}+1) + 3) \qquad (5)
\end{aligned}$$

Angenommen für ein $\mathfrak{n} \geqslant 1$ gilt:

$$\mathfrak{q}^{2\mathfrak{n}} \,\big|\, (\gamma_u - 1)\ ,\ \mathfrak{q}^{\mathfrak{n}} \,\big|\, (\gamma_o - 1) \ \text{ und } \ \mathfrak{q}^{2\mathfrak{n}} \nmid (\gamma_o - 1)$$

oder

$$\mathfrak{q}^{2\mathfrak{n}} \,\big|\, (\gamma_o - 1)\ ,\ \mathfrak{q}^{\mathfrak{n}} \,\big|\, (\gamma_u - 1) \ \text{ und } \ \mathfrak{q}^{2\mathfrak{n}} \nmid (\gamma_u - 1)\,,$$

dann folgt

$$\mathfrak{q}^{\mathfrak{n}} \,\big|\, (\gamma_o + \gamma_u - 2) \ \text{ und } \ \mathfrak{q}^{2\mathfrak{n}} \nmid (\gamma_o + \gamma_u - 2)\,.$$

Die maximale $\mathfrak{q}$-Potenz, die $\gamma_o + \gamma_u - 2$ teilt, ist das Minimum der maximalen $\mathfrak{q}$-Potenzteiler von $\gamma_o - 1$ und $\gamma_u - 1$, also $\mathfrak{q}^{\mathfrak{n}}$. Für gerades $\mathfrak{q}$ folgt aus den Gleichungen $(1) - (3)$, dass $2^{\bar{\mathfrak{m}}+1} = 2^{2\bar{\mathfrak{m}}+2}$ gelten muss, was unmöglich ist. Also ist $\mathfrak{q}$ ungerade. Dann gilt aber

$$\mathfrak{q}^{\mathfrak{n}} \,\big|\, (2^{2\bar{\mathfrak{m}}+1}+1) \text{ und } \mathfrak{q}^{2\mathfrak{n}} \nmid (2^{2\bar{\mathfrak{m}}+1}+1)\,.$$

Da $\mathfrak{q}^{2\mathfrak{n}}$ entweder $\gamma_o - 1$ oder $\gamma_u - 1$ teilt, folgt aus Gleichung (1) oder (2), dass $\mathfrak{q}^{\mathfrak{n}}$ den Wert $2^{\bar{\mathfrak{m}}}+1$ oder $2^{\bar{\mathfrak{m}}}-1$ teilt. Dann liefert aber die Gleichung (4) oder (5), dass $\mathfrak{q} = 3$ gelten muss.

Die folgende Tabelle zeigt nochmals (s. Seite 24) die Werte für kleine $\bar{\mathfrak{q}} = 2^{2\bar{\mathfrak{m}}+1}$.

$\bar{\mathfrak{q}}$	2^3	2^5	2^7
γ_o	109	1321	$18577 = 13 \cdot 1429$
γ_u	37	$793 = 13 \cdot 61$	14449

Man sieht leicht, dass für $\mathfrak{q} = 3$ kein passendes $\bar{\mathfrak{m}}$ gewählt werden kann.

Der einzige Fall, der nicht den obigen Voraussetzungen entspricht, ist $\gamma_o = \gamma_4(\mathsf{G}_0)$ und $\gamma_u = \gamma_2(\mathsf{G}_0)$. Daraus folgt aber:

$$\gamma_o + \gamma_u = 2(\bar{\mathfrak{q}}^2 + \bar{\mathfrak{q}} + 1) = 2(\mathfrak{q}^8 - \mathfrak{q}^4 + 1) \implies \bar{\mathfrak{q}}(\bar{\mathfrak{q}}+1) = \mathfrak{q}^4(\mathfrak{q}^4 - 1)\,.$$

Man erhält also

$$\bar{\mathfrak{q}} = \mathfrak{q}^4 - 1 \implies \gamma_3(\mathsf{H}_0) = (\mathfrak{q}^4-1)^2 + \mathfrak{q}^4 - 1 + 1 = \mathfrak{q}^8 - \mathfrak{q}^4 + 1 \neq \gamma_o\,.$$

• H_0 vom Typ $E_8(\bar{q})$

Wegen $H_0 \prec G_0$ ist $\bar{q} < q$. Abhängig von $\bar{q}$ müssen eine oder zwei der Komponenten von $\Gamma_i(H_0)$ ($i \geqslant 2$) in Γ mit der Komponente $\Gamma_1(H_0)$ verschmelzen. Die beiden verbleibenden Komponenten implizieren die Werte γ_u und γ_o. Gilt $\gamma_o = \gamma_i(H_0) = \gamma_i(G_0)$ oder $\gamma_u = \gamma_j(H_0) = \gamma_j(G_0)$ für ein $i, j \geqslant 2$, dann folgt unmittelbar $\bar{q} = q$. Es gilt also stets $\gamma_u, \gamma_o = \gamma_i(H_0) = \gamma_j(G_0)$ mit $i \neq j$ und die folgenden Fälle sind möglich:

(a)	$\gamma_o = \gamma_4(H_0) = \gamma_3(G_0)$	und	$\gamma_u = \gamma_2(H_0) = \gamma_5(G_0)$	oder
(b)	$\gamma_o = \gamma_4(H_0) = \gamma_3(G_0)$	und	$\gamma_u = \gamma_5(H_0) = \gamma_2(G_0)$	oder
(c)	$\gamma_o = \gamma_4(H_0) = \gamma_3(G_0)$	und	$\gamma_u = \gamma_3(H_0) = \gamma_5(G_0)$	oder
(d)	$\gamma_o = \gamma_4(H_0) = \gamma_3(G_0)$	und	$\gamma_u = \gamma_3(H_0) = \gamma_2(G_0)$	oder
(e)	$\gamma_o = \gamma_4(H_0) = \gamma_5(G_0)$	und	$\gamma_u = \gamma_5(H_0) = \gamma_2(G_0)$	oder
(f)	$\gamma_o = \gamma_4(H_0) = \gamma_5(G_0)$	und	$\gamma_u = \gamma_3(H_0) = \gamma_2(G_0)$	oder
(g)	$\gamma_o = \gamma_3(H_0) = \gamma_5(G_0)$	und	$\gamma_u = \gamma_5(H_0) = \gamma_2(G_0)$	

Wegen $q > \bar{q}$ gilt stets $q \nmid \bar{q}$, $q \nmid \bar{q} - 1$ und $q^2 \nmid \bar{q}^2 + 1$. Liegt die Bedingung $q \mid \bar{q} + 1$ vor, dann folgt $q = \bar{q} + 1$.

In den Fällen (a)-(d) ist

$$\begin{aligned} \gamma_o - 1 &= \gamma_4(H_0) - 1 &&= \bar{q}(\bar{q}-1)(\bar{q}+1)(\bar{q}^2+1)(\bar{q}^3+\bar{q}^2-1) \\ &&&= \bar{q}^8 + \bar{q}^7 - \bar{q}^5 - \bar{q}^4 - \bar{q}^3 + \bar{q} \qquad (*) \\ &= \gamma_3(G_0) - 1 &&= q^4(q^4-1) \qquad . \end{aligned}$$

Gilt $q \mid \bar{q} + 1$, also $q = \bar{q} + 1$, dann ist

$$\begin{aligned} \gamma_o - 1 &= \gamma_3(G_0) - 1 &&= q^4(q^4-1) = (\bar{q}+1)^4((\bar{q}+1)^4-1) \\ &&&= \bar{q}^8 + 8\bar{q}^7 + 28\bar{q}^6 + 56\bar{q}^5 + 69\bar{q}^4 + 52\bar{q}^3 + 22\bar{q}^2 + 4\bar{q} \quad . \end{aligned}$$

Diese Gleichung unterscheidet sich aber offensichtlich von $(*)$. Es gilt also

$$q^4 \mid (\bar{q}^2+1)(\bar{q}^3+\bar{q}^2-1)\,,$$

und wegen $q^2 \nmid (\bar{q}^2+1)$ folgt:

$$q^3 \mid \bar{q}^3+\bar{q}^2-1 \implies q^3 \leqslant \bar{q}^3+\bar{q}^2-1 < \bar{q}^3+\bar{q}^2 = \bar{q}^2(\bar{q}+1) \leqslant \bar{q}^2 q < q^3\,.$$

In den Fällen (e) und (f) ist:

$$\begin{aligned}
\gamma_o - 1 &= \gamma_4(H_0) - 1 &&= \bar{q}(\bar{q}-1)(\bar{q}+1)(\bar{q}^2+1)(\bar{q}^3+\bar{q}^2-1) \\
&&&= \bar{q}^8+\bar{q}^7-\bar{q}^5-\bar{q}^4-\bar{q}^3+\bar{q} \qquad (*) \\
&= \gamma_5(G_0) - 1 &&= q^2(q-1)(q+1)(q^4+1) \\
\gamma_u - 1 &= \gamma_2(G_0) - 1 &&= q(q-1)(q+1)(q^2+1)(q^3-q^2+1) \quad .
\end{aligned}$$

Aus γ_o folgt wie oben $q^2 \mid (\bar{q}^2+1)(\bar{q}^3+\bar{q}^2-1)$. Angenommen $q \mid \bar{q}^2+1$, dann folgt wegen $q^2 \nmid \bar{q}^2+1$, dass

$$q \mid \bar{q}^3+\bar{q}^2-1 = \bar{q}(\bar{q}^2+1)+\bar{q}^2-\bar{q}-1 = \bar{q}(\bar{q}^2+1)(\bar{q}^2+1)-\bar{q}-2$$

gilt. Daraus folgt $q \mid \bar{q}+2$ und damit $q = \bar{q}+2$. Eingesetzt liefert dies:

$$\begin{aligned}
\gamma_o - 1 &= \gamma_5(G_0) - 1 = q^2(q-1)(q+1)(q^4+1) \\
&= (\bar{q}+2)^2((\bar{q}+2)-1)((\bar{q}+2)+1)((\bar{q}+2)^4+1) \\
&= \bar{q}^8+16\bar{q}^7+111\bar{q}^6+436\bar{q}^5+1061\bar{q}^4+1640\bar{q}^3+1575\bar{q}^2+860\bar{q}+204 \quad .
\end{aligned}$$

Diese Gleichung unterscheidet sich aber wiederum sicherlich von $(*)$. Es gilt also $q \nmid \bar{q}^2+1$ und damit $q^2 \mid \bar{q}^3+\bar{q}^2-1$.

Im Fall (e) ist

$$\gamma_u - 1 = \gamma_5(H_0) - 1 = \bar{q}^2(\bar{q}-1)(\bar{q}+1)(\bar{q}^4+1) = q(q-1)(q+1)(q^2+1)(q^3+q^2-1)\,.$$

Es folgt dann:

$$q \parallel \bar{q}^4+1 = \bar{q}(\bar{q}^3+\bar{q}^2-1)-\bar{q}^3+\bar{q}+1 \implies q \parallel \bar{q}^3-\bar{q}-1\,.$$

Wegen $q^2 \mid \bar{q}^3+\bar{q}^2-1$ gilt

$$q \parallel \bar{q}^3+\bar{q}^2-1-(\bar{q}^3-\bar{q}-1) = \bar{q}^2+\bar{q} = \bar{q}(\bar{q}+1)\,,$$

im Widerspruch zu $q \nmid \bar{q}(\bar{q}+1)$.

Im Fall (f) ist $\gamma_u - 1 = \gamma_3(H_0) - 1 = \bar{q}^4(\bar{q}^4-1)q(q-1)(q+1)(q^2+1)(q^3+q^2-1)$. Es folgt dann:

$$q \parallel \bar{q}^4-1 = \bar{q}(\bar{q}^3+\bar{q}^2-1)-\bar{q}^3+\bar{q}-1 \implies q \parallel \bar{q}^3-\bar{q}+1\,.$$

Wegen $q^2 \mid \bar{q}^3+\bar{q}^2-1$ gilt dann:

$$\begin{aligned}
& q \parallel \bar{q}^3+\bar{q}^2-1-(\bar{q}^3-\bar{q}+1) = \bar{q}^2+\bar{q}-2 && \implies q \parallel \bar{q}^2+\bar{q}-2 \\
\implies\ & q \parallel \bar{q}^4-1-(\bar{q}^3+\bar{q}^2-1) = \bar{q}^4-\bar{q}^3-\bar{q}^2 = \bar{q}^2(\bar{q}^2-\bar{q}-1) && \implies q \parallel \bar{q}^2-\bar{q}-1 \\
\implies\ & q \mid \bar{q}^2+\bar{q}-2-(\bar{q}^2-\bar{q}-1) = 2\bar{q}-1\,.
\end{aligned}$$

Die Bedingung $q \mid 2\bar{q} - 1$ liefert $q = 2\bar{q} - 1$ und damit $\bar{q} = \frac{1}{2}(q+1)$ wegen $q > \bar{q}$. Es folgt dann:

$$q \mid \bar{q}^2 + \bar{q} - 2 + (\bar{q}^2 - \bar{q} - 1) = 2\bar{q}^3 - 3 = 2\frac{1}{4}(q+1)^2 - 3 = \frac{1}{2}(q^2 + 2q - 5) \implies q = 5\,.$$

Die Tabelle auf Seite 27 zeigt aber, dass dann $\bar{q}$ nicht entsprechend gewählt werden kann.

Im Fall (g) ist

$$\begin{aligned} \gamma_o - 1 &= \gamma_3(H_0) - 1 &&= \bar{q}^4(\bar{q}^4 - 1) \\ &= \gamma_5(G_0) - 1 &&= q^2(q-1)(q+1)(q^4+1) \\ \gamma_u - 1 &= \gamma_5(H_0) - 1 &&= \bar{q}^2(\bar{q}-1)(\bar{q}+1)\bar{q}^4 + 1) \\ &= \gamma_2(G_0) - 1 &&= q(q-1)(q+1)(q^2+1)(q^3 - q^2 + 1)\,. \end{aligned}$$

Wegen $q \nmid \bar{q}(\bar{q}-1)(\bar{q}+1)$ folgt aus γ_o, dass $q^2 \parallel (\bar{q}^4-1)$ gelten muss. Aus γ_u folgt $q \parallel (\bar{q}^4+1)$. Daraus folgt aber $q \parallel \bar{q}^4 + 1 - (\bar{q}^4 - 1) = 2$ und somit der Widerspruch $\bar{q} < q = 2$.

1.5.14 G_0 vom Typ ${}^2B_2(q)$

Auch in diesem Fall ist $|\Gamma(G_0)| = 4$. Es gilt $q = 2^{2m+1}$ mit $m \geqslant 1$, und es ist

$$\begin{aligned} \gamma_2(G_0) = q - \sqrt{2q} + 1 &= 2^{m+1}(2^m - 1) + 1\,, \\ \gamma_3(G_0) = q - 1 &= 2^{2m+1} - 1\,, \\ \gamma_4(G_0) = q + \sqrt{2q} + 1 &= 2^{m+1}(2^m + 1) + 1\,. \end{aligned}$$

Für kleine Werte von q ergibt sich die folgenden Tabelle:

q	2^3	2^5	2^7	2^9	2^{11}
$\gamma_2(G_0)$	5	5^2	113	$481 = 13 \cdot 37$	$1985 = 5 \cdot 397$
$\gamma_3(G_0)$	7	31	127	511	$2047 = 23 \cdot 89$
$\gamma_4(G_0)$	13	41	$145 = 5 \cdot 29$	$545 = 5 \cdot 109$	2113

Für alle Werte von q gilt $5 \mid \gamma_2 \cdot \gamma_4 = q^2 + 1$, denn es ist $q^2 = 2^{4m+2} = (2^m)^4 \cdot 4 \equiv 1 \cdot (-1) \bmod 5$ und damit $q^2 + 1 \equiv 0 \bmod 5$.

- H_0 sporadisch-einfach bzw. Ausnahmegruppe

Vergleicht man die Werte in Tabelle A.3 mit obiger Tabelle, dann sieht man, dass H_0 nicht sporadisch-einfach sein kann. Aus A.4 und A.5 folgt $H_0 \cong A_2(4)$ und $G_0 \cong {}^2B_2(2^3)$ im Fall, dass H_0 eine Ausnahmegruppe ist. Wegen $|\Gamma| = 3$ ist dann $\Gamma_3(G_0), \Gamma_4(H_0) \subset \Gamma_1$. Es gilt aber $13 \nmid |\mathrm{Aut}(H_0)| = 2^8 \cdot 3^3 \cdot 5 \cdot 7$, im Widerspruch zu $13 \in \pi(G_0)$.

- H_0 alternierend

Ist H_0 alternierend, dann ist $\gamma_o - \gamma_u = \gamma_o(H_0) - \gamma_u(H_0) = 2^x$ mit $x \leqslant 2$. Ist $\gamma_o = \gamma_4(G_0)$, dann ist $\gamma_o - \gamma_u \geqslant \gamma_4(G_0) - \gamma_3(G_0) = \sqrt{2q} + 2 = 2^{m+1} + 2 > 4$. Ist $\gamma_o = \gamma_3(G_0)$, dann ist $\gamma_u = \gamma_2(G_0)$ und es gilt $\gamma_o - \gamma_u = \sqrt{2q} - 2 = 2^{m+1} - 2$. Für $m > 1$ ist die Differenz größer als 4. Für $m = 1$ gilt $\gamma_o - \gamma_u = 2$. Es ist dann $q = 2^3$ und $G_0 \cong {}^2B_2(2^3)$, sowie $\gamma_o = 7$ und $\gamma_u = 5$. Es muss also $H_0 \cong A_7$ gelten. Es gilt aber $13 \nmid |\mathrm{Aut}(A_7)|$, im Widerspruch zu $13 \in \pi(G_0)$.

- H_0 vom Typ $A_1(\bar{q})$

  - Ist $\bar{q} \equiv 0 \bmod 2$, dann muss $\gamma_o - \gamma_u = \gamma_o(H_0) - \gamma_u(H_0) = \bar{q} + 1 - (\bar{q} - 1) = 2$ gelten. Wie im alternierenden Fall ergibt sich $G_0 \cong {}^2B_2(2^3)$ und damit $\gamma_o = 7$ sowie $\gamma_u = 5$. Es muss dann also $\bar{q} = 6$ gelten, was unmöglich ist.
  - Ist $\bar{q} \equiv 1 \bmod 4$, dann gilt $\gamma_o = \gamma_o(H_0) = \bar{q}$ und $\gamma_u = \gamma_u(H_0) = \frac{1}{2}(\bar{q} + 1)$.
    - Ist $\gamma_o = \gamma_4(G_0)$, dann ist $\bar{q} = 2^{m+1}(2^m + 1) + 1$ und damit
    $$\gamma_u = \frac{1}{2}(\bar{q} + 1) = \frac{1}{2}(2^{m+1}(2^m + 1) + 2) = 2^m(2^m + 1) + 1\,.$$
    Damit ist $\gamma_u = \gamma_2(G_0)$ nicht möglich, und es gilt:
    $$\gamma_u = \gamma_3(G_0) = 2^{2m+1} - 1 = 2^m(2^m + 1) + 1 \implies 2^{2m+1} = 2\underbrace{\left(2^{m-1}(2^m + 1) + 1\right)}_{\equiv 1 \bmod 2 \text{ für } m \neq 1}\,.$$
    Für $m \neq 1$ ist die Gleichung also nicht lösbar. Für $m = 1$ ist $\gamma_o = \bar{q} = 13$ und $\gamma_u = 7$, also $H_0 \cong A_1(13)$. Es gilt $5 \nmid |\mathrm{Aut}(H_0)| = 2^3 \cdot 3 \cdot 7 \cdot 13$, im Widerspruch zu $5 \in \pi(G_0)$.
    - Ist $\gamma_o = \gamma_3(G_0)$ und somit $\gamma_u = \gamma_2(G_0)$, dann ist $\bar{q} = 2^{2m+1} - 1$ und damit
    $$\gamma_u = \frac{1}{2}(\bar{q} + 1) = \frac{1}{2}(2^{2m+1}) = 2^{2m} \neq \gamma_2(G_0)\,.$$
  - Ist $\bar{q} \equiv 3 \bmod 4$, dann gilt $\gamma_o = \gamma_o(H_0) = \bar{q}$ und $\gamma_u = \gamma_u(H_0) = \frac{1}{2}(q - 1)$.
    - Ist $\gamma_o = \gamma_4(G_0)$, dann ist $\bar{q} = 2^{m+1}(2^m + 1)$ und damit
    $$\gamma_u = \frac{1}{2}(\bar{q} - 1) = \frac{1}{2}(2^{m+1}(2^m + 1)) = 2^m(2^m + 1)\,.$$
    Also muss γ_u gerade sein, was nicht möglich ist.
    - Ist $\gamma_o = \gamma_3(G_0)$ und somit $\gamma_u = \gamma_2(G_0)$, dann ist $\bar{q} = 2^{2m+1} - 1$ und damit
    $$\gamma_u = \frac{1}{2}(\bar{q} - 1) = \frac{1}{2}(2^{2m+1} - 2) = 2^{2m} - 1 \overset{=}{} 2^{2m+1} - 2^{m+1} + 1 = \gamma_2(G_0)\,.$$
    Es muss also
    $$2^m = 2(2^{2m} - 2^m + 1)$$
    gelten. Die rechte Seite ist aber keine Potenz von 2.

- H_0 vom Typ $G_2(\bar{q})$

Es ist $\bar{q} = 3^{\bar{f}}$, $\gamma_o = \gamma_o(H_0) = \bar{q}^2 + \bar{q} + 1$ und $\gamma_u = \gamma_u(H_0) = \bar{q}^2 - \bar{q} + 1$.

- Ist $\gamma_o = \gamma_4(G_0)$, dann folgt

$$\gamma_o - 1 = \bar{q}^2 + \bar{q} = \bar{q}(\bar{q}+1) = 3^{\bar{f}}(3^{\bar{f}}+1) = 2^{m+1}(2^m+1)\,.$$

  Es gilt also $3^{\bar{f}} \,\big|\, 2^m + 1$ sowie $2^{m+1} \,\big|\, 3^{\bar{f}} + 1$, und damit folgt:

$$3^{\bar{f}} \leqslant 2^m + 1 < 2^{m+1} \leqslant 3^{\bar{f}} + 1 \implies 3^{\bar{f}} = 2^m + 1 \text{ und } 2^{m+1} = 3^{\bar{f}} + 1\,.$$

  Damit ist

$$2^{m+1} = 3^{\bar{f}} + 1 = 2^m + 1 + 1 = 2^m + 2\,.$$

  Also ist $m = \bar{f} = 1$ und damit $G_0 \cong {}^2B_2(2^3)$ und $H_0 \cong G_2(3)$. Es ist dann $\gamma_o = 13$ und $\gamma_u = 7$. Also ist $\gamma_u = \gamma_3(G_0)$. Allerdings gilt $3 \,\big\|\, |\mathrm{Aut}(G_0)| = 2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ im Widerspruch zu $3^6 \,\big\|\, |H_0| = 2^6 \cdot 3^6 \cdot 7 \cdot 13$.

- Ist $\gamma_o = \gamma_3(G_0)$, dann gilt:

$$\gamma_o = \bar{q}^2 + \bar{q} + 1 = q - 1 = 2^{2m+1} - 1 \implies 3^{\bar{f}}(3^{\bar{f}}+1) = 2(2^{2m}-1)\,.$$

  Mit $\gamma_u = \gamma_2(G_0)$ folgt:

$$\bar{q}^2 - \bar{q} + 1 = 2^{2m+1} - 2^{m+1} + 1 \implies 3^{\bar{f}}(3^{\bar{f}}-1) = 2^{m+1}(2^m-1)\,.$$

  Insgesamt muss dann

$$3^{\bar{f}} \leqslant 2^m - 1 < 2^{m+1} \leqslant 3^{\bar{f}} - 1$$

  gelten, was aber unmöglich ist.

- H_0 vom Typ ${}^2G_2(\bar{q}^2)$

Es ist $\bar{q}^2 = 3^{2\bar{m}+1}$, $\gamma_o = \gamma_o(H_0) = \bar{q}^2 + \sqrt{3\bar{q}^2} + 1$ und $\gamma_u = \gamma_u(H_0) = \bar{q}^2 - \sqrt{3\bar{q}^2} + 1$. Wegen $(\bar{q}^4 - 1) \,\big|\, \gamma_1(H_0)$ gilt $5 \in \pi_1(H_0)$ und damit beschreibt $\gamma_3(G_0)$ eine der verbleibenden isolierten Komponenten von Γ.

- Ist $\gamma_3(G_0) = \gamma_u$, dann ist $\gamma_o = \gamma_4(G_0)$, und es gilt

$$\gamma_o - 1 = 2^{m+1}(2^m+1) = 3^{\bar{m}+1}(3^{\bar{m}}+1)\,.$$

  Damit muss aber wegen Teilbarkeitsargumenten

$$2^{m+1} \leqslant 3^{\bar{m}} + 1 < 3^{\bar{m}+1} \leqslant 2^m + 1$$

  gelten, was unmöglich ist.

- Ist $\gamma_3(G_0) = \gamma_o$, dann ist $\gamma_u = \gamma_2(G_0)$, und es gilt

$$\gamma_u - 1 = 2^{m+1}(2^m-1) = 3^{\bar{m}+1}(3^{\bar{m}}-1)\,.$$

  Wiederum liefern Teilbarkeitsargumente den Widerspruch

$$2^{m+1} \leqslant 3^{\bar{m}} - 1 < 3^{\bar{m}+1} \leqslant 2^m - 1\,.$$

- H_0 vom Typ ${}^2D_{\bar{p}}(3)$

Es ist $\bar{p} = 2^{\bar{m}} + 1$, $\gamma_o = \gamma_o(H_0) = \frac{1}{4}(3^{\bar{p}} + 1)$ und $\gamma_u = \gamma_u(H_0) = \frac{1}{2}(3^{\bar{p}-1} + 1)$. Wegen $(3^4 - 1) \,|\, \gamma_1(H_0)$ gilt $5 \in \pi_1(H_0)$ und damit beschreibt $\gamma_3(G_0)$ eine der verbleibenden isolierten Komponenten von Γ.

- Ist $\gamma_3(G_0) = \gamma_u$, dann ist $\gamma_o = \gamma_4(G_0)$, und es gilt:

$$\gamma_u = 2^{2m+1} - 1 = \frac{1}{2}(3^{\bar{p}-1} + 1) \implies 3^{\bar{p}-1} = 2^{2m+1} - 2 - 1 = 2^{2m+2} - 3\,.$$

  Die letzte Gleichung ist aber nicht erfüllbar, da die rechte Seite keine Potenz von 3 ist.

- Ist $\gamma_3(G_0) = \gamma_o$, dann ist $\gamma_u = \gamma_2(G_0)$, und es gilt:

$$\gamma_o = 2^{2m+1} - 1 = \frac{1}{4}(3^{\bar{p}} + 1) \implies 2^{2m+3} - 4 = 3^{\bar{p}} + 1 \implies 3^{\bar{p}} = 2^{2m+3} - 5\,.$$

  Weiter folgt:

$$\gamma_u = 2^{2m+1} - 2^{m+1} + 1 = \frac{1}{2}(3^{\bar{p}-1} + 1) \implies 3^{\bar{p}-1} = 2^{2m+2} - 2^{m+2} + 1\,.$$

  Fasst man die beiden Bedingungen zusammen, so ergibt sich

$$3^{\bar{p}} = 3 \cdot 3^{\bar{p}-1} = 3(2^{2m+2} - 2^{m+2} + 1^{)} = 2^{2m+3} - 5 \implies 3 \cdot 2^{m+2}(2^m - 1) = 2^3(2^{2m} - 1)\,.$$

  Daraus folgt $2^{m+2} = 2^3$ und damit $m = 1$, bzw. $q = 2^3$. Aus $\gamma_o = 7$ folgt dann $\bar{p} = 3$. Es ist also $G_0 \cong {}^2B_2(2^3)$ und $H_0 \cong {}^2D_3(3)$. Allerdings gilt $3 \,\|\, |\mathrm{Aut}(G_0)| = 2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ im Widerspruch zu $3^6 \,\|\, |H_0| = 2^9 \cdot 3^6 \cdot 5 \cdot 7$.

- H_0 vom Typ ${}^2D_{\bar{p}+1}(2)$

Es ist $\bar{p} = 2^{\bar{m}} - 1$ mit $\bar{m} \geqslant 2$, sowie $\gamma_o = \gamma_o(H_0) = 2^{\bar{p}+1} + 1$ und $\gamma_u = \gamma_u(H_0) = 2^{\bar{p}} + 1$. Außerdem gilt $5 \,|\, \gamma_1(H_0)$ und damit $5 \in \pi_1(H_0)$. Damit beschreibt $\gamma_3(G_0)$ eine der verbleibenden isolierten Komponenten von Γ.

- Ist $\gamma_3(G_0) = \gamma_u$, dann ist $\gamma_o = \gamma_4(G_0)$, und es gilt:

$$\gamma_u = 2^{2m+1} - 1 = 2^{\bar{p}} + 1 \implies 2^{\bar{p}} = 2(2^{2m} - 1)\,.$$

  Die letzte Gleichung ist aber nicht erfüllbar, da die rechte Seite keine Potenz von 2 ist.

- Ist $\gamma_3(G_0) = \gamma_o$, dann gilt:

$$\gamma_o = 2^{2m+1} - 1 = 2^{\bar{p}+1} + 1 \implies 2^{\bar{p}+1} = 2(2^{2m} - 1)\,.$$

  Auch diese Gleichung ist wiederum nicht erfüllbar, da die rechte Seite dann keine Potenz von 2 ist.

- H_0 vom Typ $F_4(\bar{q})$

Es ist $\bar{q} = 2^{2\bar{m}+1}$ mit $\bar{m} \geqslant 0$, sowie $\gamma_o = \gamma_o(H_0) = \bar{q}^4 + 1$ und $\gamma_u = \gamma_u(H_0) = \bar{q}^4 - \bar{q}^2 + 1$. Außerdem gilt $\bar{q}^4 - 1 \,|\, \gamma_1(H_0)$ und damit $5 \in \pi_1(H_0)$. Damit beschreibt $\gamma_3(G_0)$ eine der verbleibenden isolierten Komponenten von Γ.

- Ist $\gamma_3(G_0) = \gamma_u$, dann ist $\gamma_o = \gamma_4(G_0)$, und es gilt

$$\gamma_o - 1 = 2^{m+1}(2^m + 1) = 2^{2\bar{m}+1}\,.$$

  Die Gleichung ist nicht erfüllbar, da die linke Seite für positive m keine Potenz von 2 ist.

- Ist $\gamma_3(G_0) = \gamma_o$, dann gilt:

$$\gamma_o = 2^{2m+1} - 1 = 2^{2\bar{m}+1} + 1 \implies 2^{2m+1} = 2(2^{2\bar{m}} + 1)\,.$$

  Die rechte Seite der Gleichung ist nur für $\bar{m} = 0$ eine Potenz von 2. Dann müsste aber $2^{2m+1} = 4$ gelten, was unmöglich ist.

- H_0 vom Typ ${}^2F_4(\bar{q})$

Es ist $\bar{q} = 2^{2\bar{m}+1}$ mit $\bar{m} \geqslant 1$, sowie

$$\begin{aligned}
\gamma_o = \gamma_o(H_0) &= \bar{q}^2 + \sqrt{2\bar{q}^3} + q + \sqrt{2\bar{q}} + 1 &&= 2^{4\bar{m}+2} + 2^{3\bar{m}+2} + 2^{2\bar{m}+1} + 2^{\bar{m}+1} + 1 \\
\gamma_u = \gamma_u(H_0) &= \bar{q}^2 - \sqrt{2\bar{q}^3} + q - \sqrt{2\bar{q}} + 1 &&= 2^{4\bar{m}+2} - 2^{3\bar{m}+2} + 2^{2\bar{m}+1} - 2^{\bar{m}+1} + 1\,.
\end{aligned}$$

Außerdem gilt $\bar{q}^4 - 1 \,|\, \gamma_1(H_0)$ und damit $5 \in \pi_1(H_0)$. Damit beschreibt wiederum $\gamma_3(G_0)$ eine der verbleibenden isolierten Komponenten von Γ.

- Ist $\gamma_3(G_0) = \gamma_u$, dann gilt

$$\gamma_u + 1 = 2^{2m+1} = 2(2^{4\bar{m}+1} - 2^{3\bar{m}+1} + 2^{2\bar{m}} - 2^{\bar{m}} + 1)\,.$$

  Die Gleichung ist nicht erfüllbar, da die rechte Seite für positive $\bar{m}$ keine Potenz von 2 ist.

- Ist $\gamma_3(G_0) = \gamma_o$, dann gilt

$$\gamma_o + 1 = 2^{2m+1} = 2(2^{4\bar{m}+1} + 2^{3\bar{m}+1} + 2^{2\bar{m}} + 2^{\bar{m}} + 1)\,.$$

  Auch diese Gleichung ist für positive $\bar{m}$ nicht erfüllbar, da die rechte Seite keine Potenz von 2 ist.

• H_0 vom Typ ${}^2E_8(\bar{q})$

Auch in diesem Fall gilt wieder $\bar{q}^4 - 1 \,\big|\, \gamma_1(H_0)$ und damit ist $5 \in \pi_1(H_0)$. Damit ist in jedem Fall $|\Gamma| = 3$ und wiederum beschreibt $\gamma_3(G_0)$ eine der verbleibenden isolierten Komponenten von Γ.

Für die $\gamma_i(H_0)$ gilt:

$$\begin{aligned}
\gamma_2(H_0) - 1 &= \bar{q}(\bar{q}-1)(\bar{q}+1)(\bar{q}^2+1)(\bar{q}^3-\bar{q}^2+1)\\
\gamma_3(H_0) - 1 &= \bar{q}^4(\bar{q}-1)(\bar{q}+1)(\bar{q}^2+1)\\
\gamma_4(H_0) - 1 &= \bar{q}(\bar{q}-1)(\bar{q}+1)(\bar{q}^2+1)(\bar{q}^3+\bar{q}^2-1)\\
\gamma_5(H_0) - 1 &= \bar{q}^2(\bar{q}-1)(\bar{q}+1)(\bar{q}^4+1)
\end{aligned}$$

Es muss $\gamma_3(G_0) = \gamma_i(H_0)$ für ein i mit $2 \leqslant i \leqslant 5$ gelten. Für dieses i gilt dann auch

$$\gamma_i(H_0) - 1 = \gamma_3(G_0) - 1 = 2(2^{2m+1} - 1)\,.$$

Für ungerades $\bar{q}$ gilt $2 \,\big|\, \bar{q}^x \pm 1$. Es teilt dann 2^3 den Wert $\gamma_i(H_0) - 1$, im Widerspruch zu $2 \,\big\|\, \gamma_3(G_0) - 1 = 2(2^{2m} - 1)$. Es ist also $\bar{q}$ gerade, und wegen $2 \,\big\|\, \gamma_3(G_0) - 1$ folgt (für $m > 1$) $\bar{q} = 2$ und $i \in \{2, 4\}$.

Ist $\gamma_3(G_0) = \gamma_2(H_0)$, dann muss

$$\frac{1}{2}(\gamma_3(G_0) - 1) + 1 = 2^{2m+1} = \frac{1}{2} \cdot 2 \cdot (2-1)(2+1)(2^2+1)(2^3-2^2+1) = \frac{1}{2}(\gamma_2(H_0) - 1) + 1$$

gelten. Ist $\gamma_3(G_0) = \gamma_4(H_0)$, dann gilt

$$\frac{1}{2}(\gamma_3(G_0) - 1) + 1 = 2^{2m+1} = \frac{1}{2} \cdot 2 \cdot (2-1)(2+1)(2^2+1)(2^3+2^2-1) = \frac{1}{2}(\gamma_2(H_0) - 1) + 1\,.$$

Beides ist aber unmöglich, weil die rechte Seite z.B. von 3 geteilt wird.

Der Fall $m = 0$ ist ebenfalls nicht möglich. Das zeigt der Vergleich der γ_o-, bzw. γ_u-Werte mit denen für kleine $\bar{q}$.

• H_0 vom Typ ${}^2B_2(\bar{q})$

Wegen $|\Gamma| = 3$ muss nach Lemma 1.11 eine der Komponenten $\Gamma_i(G_0)$ ($i \geqslant 2$) mit der Komponente $\Gamma_1(G_0)$ fusionieren. Die zwei verbleibenden Komponenten induzieren γ_o und γ_u. Das gleiche gilt für H_0.

Gilt $\gamma_o = \gamma_i(G_0) = \gamma_i(H_0)$ oder $\gamma_u = \gamma_j(G_0) = \gamma_j(H_0)$, dann folgt wiederum unmittelbar $q = \bar{q}$. Wegen $H_0 \prec G_0$ gilt also

$$\gamma_o = \gamma_4(H_0) = \gamma_3(G_0) \quad \text{und} \quad \gamma_u = \gamma_3(H_0) = \gamma_2(G_0)\,.$$

Aus der ersten Gleichung folgt (mit $\bar{q} = 2^{2\bar{m}+1}$):

$$2^{\bar{m}+1}(2^{\bar{m}}+1)+1 = 2^{2m+1}-1 \implies 2^{\bar{m}}(2^{\bar{m}}+1) = 2^{2m}-1\,.$$

Die linke Seite der Gleichung ist aber wegen $\bar{m} \geqslant 1$ gerade, die rechte jedoch wegen $m \geqslant 1$ ungerade.

□

1.6 Anwendung auf Burnsideringe

Die Ergebnisse des vorangegangenen Abschnitts können auf die Theorie der Burnsideringe angewendet werden.

Definition 1.16. Der Burnsidering $B(G)$ einer endlichen Gruppe G ist die freie abelsche Gruppe auf der Menge der Isomorphieklassen transitiver G-Linksmengen. Die Addition auf $B(G)$ ist durch die disjunkte Vereinigung

$$[S] + [T] = [S \dot\cup T]$$

gegeben. Die Multiplikation auf $B(G)$ wird durch das Bilden kartesischer Produkte

$$[S] \cdot [T] = [S \times T]$$

erklärt. $B(G)$ ist also der Grothendieck-Ring der Kategorie transitiver G-Linksmengen.

Jede transitive G-Linksmenge ist isomorph zur Menge der Nebenklassen G/H für eine Untergruppe H von G. Zwei transitive G-Linksmengen $S = G/H_1$ und $T = G/H_2$ sind genau dann isomorph als G-Linksmengen, wenn H_1 und H_2 in G konjugiert sind.

Das Einselement von $B(G)$ ist $[G/G]$.

Äquivalent zur Definition 1.16 können Burnsideringe auch über die sogenannte Markentafel $MT(G)$ von G definiert werden:

Definition 1.17. Sei G eine Gruppe und U eine Untergruppe von G. Dann bezeichnet $[U]$ die Menge aller zu U in G konjugierten Untergruppen. Man setzt $V(G) := \{[U]; U \leqslant G\}$, sowie $n := |V(G)|$. Weiter steht für eine G-Menge X und eine Untergruppe K von G der Ausdruck X^K für die Fixpunkte von X unter K.

Die Markentafel $MT(G)$ ist eine ganzzahlige $n \times n$-Matrix. Zeilen und Spalten werden von den Elementen aus $V(G)$ indiziert. Genauer werden die Spalten von G/U und die Zeilen von K, mit $[U], [K] \in V(G)$, indiziert. Der Eintrag der Spalte G/U und Zeile K ist der Wert $|(G/U)^K|$.

Der $\mathbb{Z}$-Aufspann der Spalten von $MT(G)$ ist ein Teilring von $\mathbb{Z}^n$. Dieser Teilring ist isomorph zum Burnsidering $B(G)$.

Bemerkung 1.18.

- Für die Einträge von $\mathsf{MT}(G)$ gilt die Formel

$$|(G/U)^K| = \frac{|\{H \in [K]\,;\, H \leqslant U\}| \cdot |N_G(U)|}{|U|}\,.$$

- Sind die Ordnungen von U und K coprim, dann ist $|(G/U)^K| = 0$.

Die Zeilen und Spalten der Markentafel können so geordnet werden, dass Folgendes gilt:

- Die Werte unterhalb der Diagonalen sind Null.
- Die Diagonale besteht aus den Werten $|N_G(U) : U|$.
- Die letzte Spalte besteht nur aus Einsen, sie entspricht der Eins von $B(G)$.

Beispiel 1.19. Für $G = S_3$ ist $V(G) = \{[1], [C_2], [C_3], [S_3]\}$. Es ist also $n = 4$. Die Markentafel hat die Gestalt

$\mathsf{MT}(S_3)$	$S_3/1$	S_3/C_2	S_3/C_3	S_3/S_3
1	6	3	2	1
C_2		1	0	1
C_3			2	1
S_3				1

Aufgrund der Definition ist unmittelbar klar, dass für zwei Gruppen G und H

$$\mathsf{MT}(G) \cong \mathsf{MT}(H) \implies B(G) \cong B(H)$$

gilt. Die Umkehrung ist ein offenes Problem (siehe z.B. [39]).

Es stellt sich die Frage, inwieweit die Markentafel $\mathsf{MT}(G)$ bzw. der Burnsidering $B(G)$ einer Gruppe G die Gruppe selbst bestimmt, ob also aus $\mathsf{MT}(G) \cong \mathsf{MT}(H)$ bzw. $B(G) \cong B(H)$ folgt, dass $G \cong H$ ist. Nach [37, Proposition 7.2] gilt

Satz 1.20. *Gibt es für zwei Gruppen G und H einen Verbandsisomorphismus σ der Untergruppenverbände, der die Konjugiertheit und die Ordnung von Untergruppen bewahrt, dann besitzen G und H identische Markentafeln, also auch identische Burnsideringe.*

Nicht-isomorphe Gruppen mit dieser Eigenschaft wurden bereits 1928 von A. Rottlaender beschrieben [50], d.h. es gibt nicht-isomorphe Gruppen G und H mit identischen Markentafeln und isomorphen Burnsideringen. Das erste, als solches veröffentlichte Beispiel nicht-isomorpher Gruppen mit isomorphem Burnsidering gab J. Thévenaz [55]. Das kleinste Beispiel für ein Paar von nicht-isomorphen Gruppen mit identischen Markentafeln sind zwei Gruppen der Ordnung 96. Es wurde von L. M. Huerta-Aparicio, A. Molina-Rueda, A. G. Raggi-Cárdenas und

L. Valero-Elizondo [30, Abschnitt 5] gefunden. Sie verwendeten dazu die `SmallGroupLibrary` des Computer-Algebra-Systems `GAP` [18].

Obwohl es also im Allgemeinen falsch ist, dass die Markentafel oder der Burnsidering die zugrunde liegende Gruppe bis auf Isomorphie bestimmt, gibt es Klassen von Gruppen für die dies doch der Fall ist. So gilt zum Beispiel, dass wenn zwei Gruppen G und H isomorphe Burnsideringe besitzen, und eine der Gruppen abelsch, hamiltonsch oder minimal-einfach ist, dass dann G isomorph zu H ist [47].

Auch für nahezu alle (nicht minimal-) einfachen Gruppen lässt sich die obige Frage positiv beantworten:

Satz 1.21 (Kimmerle, Luca, Raggi-Cárdenas [39, Theorem 5.3])**.** *Ist G eine endliche einfache Gruppe, die nicht isomorph zu einer symplektischen oder orthogonalen Gruppe der Ordnung $\geqslant 10^8$ ist, dann bestimmt der Burnsidering $B(G)$ die Gruppe G bis auf Isomorphie.*

Wenn auch die Markentafel und der Burnsidering einer Gruppe diese im Allgemeinen nicht bis auf Isomorphie bestimmt, stellt sich dennoch die Frage, welche Eigenschaften der Gruppe G durch ihre Markentafel, bzw. ihren Burnsidering bestimmt sind.

Ein wichtiges Resultat in Hinblick auf diese Fragestellung ist der folgende Satz [37, Satz 7.5].

Satz 1.22 (Kimmerle)**.** *Seien G und H endliche Gruppen mit gleicher Markentafel. Dann gibt es zu jeder Hauptreihe*

$$1 = K_0 < K_1 < \ldots < K_{n-1} < K_n = G$$

von G eine Hauptreihe

$$1 = L_0 < L_1 < \ldots < L_{n-1} < L_n = H$$

von H, so dass für $1 \leqslant i \leqslant n$ die Hauptfaktoren K_i/K_{i-1} und L_i/L_{i-1} isomorph sind.

Insbesondere sind also die Isomorphietypen und Multiplizitäten der Kompositionsfaktoren einer Gruppe durch ihre Markentafel bestimmt. Ob die Kompositionsfaktoren einer Gruppe auch durch ihren Burnsidering bestimmt sind, ist im Allgemeinen ein offenes Problem.

Von einigen wichtigen Eigenschaften von G ist aber bekannt, dass sie durch den Burnsidering $B(G)$ festgelegt sind.

Bemerkung 1.23. Sind G und H endliche Gruppen mit isomorphen Burnsideringen $B(G) \cong B(H)$, dann gilt:

(a) $|G| = |H|$.

(b) $\pi_e(G) = \pi_e(H)$, wobei $\pi_e(X) := \{o(x)\ ;\ x \in X\}$ das Spektrum einer Gruppe X beschreibt [39, Corollary 5.2]. Insbesondere ist also $\Gamma(G) = \Gamma(H)$.

(c) Es gibt eine Bijektion zwischen den Konjugiertenklassen auflösbarer Untergruppen von G und H, die die Ordnung der Untergruppen und die Länge der Konjugiertenklassen erhält [47, Corollary 5.2] (s. auch [39, Corollary 4.4]).

Sind G und H endliche Gruppen mit isomorphen Burnsideringen, und ist N_G ein maximaler auflösbarer Normalteiler von G, dann besitzt H nach obiger Bemerkung einen maximalen auflösbaren Normalteiler N_H von gleicher Ordnung wie N_G. Ist $\Gamma = \Gamma(\mathsf{G}) = \Gamma(\mathsf{H})$ mehrfach zerfallend, dann erfüllen (mit den Bezeichnungen aus Abschnitt 1.2) G und H, bzw. $\mathsf{G}' = \mathsf{G}/\mathsf{N}_\mathsf{G}$ und $\mathsf{H}' = \mathsf{H}/\mathsf{N}_\mathsf{H}$ alle Voraussetzungen von Satz 1.10 und man erhält unmittelbar das folgende Resultat.

Satz 1.24. *Seien* G *und* H *endliche Gruppen mit* $\mathsf{B}(\mathsf{G}) \cong \mathsf{B}(\mathsf{H})$ *und* $|\Gamma| = |\Gamma(\mathsf{G})| = |\Gamma(\mathsf{H})| \geqslant 3$. *Dann besitzen* G *und* H *die gleichen Kompositionsfaktoren, inklusive deren Vielfachheiten.*

KAPITEL 2

Zum Primgraphen der Einheitengruppe im ganzzahligen Gruppenring auflösbarer Gruppen

Es sei $\mathbb{Z}G$ der Gruppenring einer endlichen Gruppe G. Jedes Element $\nu \in \mathbb{Z}G$ lässt sich in der Form

$$\nu = \sum_{g \in G} \alpha_g(\nu) g \quad \text{mit} \quad \alpha_g(\nu) \in \mathbb{Z}$$

schreiben. Die Abbildung

$$\begin{array}{rccc} \varepsilon: & \mathbb{Z}G & \longrightarrow & \mathbb{Z} \\ & \nu & \longmapsto & \sum\limits_{g \in G} \alpha_g(\nu) \end{array}$$

heißt die Augmentationsabbildung. Weiter bezeichne $V(\mathbb{Z}G)$ die Gruppe der normierten Einheiten von $\mathbb{Z}G$, d.h. jene Einheiten $u \in \mathbb{Z}G$ mit Augmentation $\varepsilon(u) = 1$.

Gibt es für zwei Elemente $u, \nu \in V(\mathbb{Z}G)$, bzw. zwei Untergruppen $A, B \leqslant V(\mathbb{Z}G)$ ein Element x aus den Einheiten von $\mathbb{Q}G$ mit $x^{-1}ux = \nu$, bzw. $x^{-1}Ax = B$, so wird dies im Folgenden mit $x \underset{\mathbb{Q}G}{\sim} y$, bzw. $A \underset{\mathbb{Q}G}{\sim} B$ notiert.

Ist G eine Gruppe mit $\Gamma(V(\mathbb{Z}G)) = \Gamma(G)$ und E eine abelsche Erweiterung von G, dann wird in diesem Kapitel gezeigt, dass $\Gamma(V(\mathbb{Z}E)) = \Gamma(E)$ gilt. Als Konsequenz erhält man die Gleichheit der Primgraphen von G und $V(\mathbb{Z}G)$ für jede auflösbare endliche Gruppe G. Die Ergebnisse resultieren aus gemeinsamer Arbeit mit W. Kimmerle [38, Abschnitt 4].

Die Frage, ob für eine endliche Gruppe G der Primgraph $\Gamma(G)$ mit $\Gamma(V(\mathbb{Z}G))$ übereinstimmt, steht im Zusammenhang mit den folgenden Vermutungen von H. Zassenhaus:

- (ZC·1) Ist $u \in V(\mathbb{Z}G)$ ein Element endlicher Ordnung, dann gibt es ein Element g von G mit $u \underset{\mathbb{Q}G}{\sim} g$.
- (ZC·2) Ist H eine Untergruppe von $V(\mathbb{Z}G)$ mit $|H| = |G|$, dann ist $H \underset{\mathbb{Q}G}{\sim} G$.
- (ZC·3) Ist U eine endliche Untergruppe von $V(\mathbb{Z}G)$, gibt es eine Untergruppe U von G mit $H \underset{\mathbb{Q}G}{\sim} U$.

Es ist offensichtlich, dass für eine Gruppe G die Implikationen

$$(ZC·2) \impliedby (ZC·3) \implies (ZC·1) \implies \Gamma(G) = \Gamma(V(\mathbb{Z}G))$$

gelten. Die Vermutungen (ZC·2) und (ZC·3) sind nicht für alle endlichen Gruppen wahr[1]. Ein erstes Gegenbeispiel zu (ZC·2) wurde von K. W. Roggenkamp und L. L. Scott [49], [52] (siehe auch [42]), konstruiert. Das von ihnen konstruierte Gegenbeispiel ist eine metabelsche Gruppe der Ordnung 2880. Mittlerweile sind wesentlich kleinere Gegenbeispiele bekannt. So konstruierte M. Hertweck in [23] und [24] Gegenbeispiele, wobei das kleinste Gegenbeispiel eine Gruppe der Ordnung 144 ist. Von F. D. Blanchard [5], [6] wurden Serien von Gruppen angegeben, für die eine semilokale Version von (ZC·2) nicht gilt. In [7] gibt Blanchard drei semilokale Gegenbeispiele der Ordnung 96 an und zeigt, dass es keine kleineren Gegenbeispiele gibt. M. Hertweck konnte zeigen [25, Theorem 10.1], dass (ZC·2) für eine dieser Gruppen global richtig ist, für die anderen beiden Gruppen ist (ZC·2) auch global falsch.

Obwohl sich also (ZC·2), und damit auch (ZC·3), im Allgemeinen als falsch erwiesen hat, sind die Vermutungen dennoch für viele Gruppen wahr, und es bleibt weiterhin von Interesse, Gruppen zu finden, für die die Vermutungen richtig sind. Eines der wichtigsten positiven Resultate bezüglich der Vermutungen lieferte sicherlich A. Weiss in [59], indem er gezeigt hat, dass (ZC·3) für nilpotente Gruppen wahr ist.

Für nicht-auflösbare einfache Gruppen ist (ZC·3) bislang offen. Lediglich für die alternierende Gruppe A_5 konnte von M. Dokuchaev, S. O. Juriaans und C. P. Milies [15] bisher bewiesen werden, dass (ZC·3) wahr ist. In dieser Arbeit wird die Vermutung auch für die beiden nicht-auflösbaren Gruppen S_5 und $SL(2,5)$ bewiesen.

Im Gegensatz zu (ZC·3) ist die Vermutung (ZC·1) bisher offen. In [45] stellen I. S. Luthar und I. B. S. Passi einen algorithmischen Zugang zur Lösung von (ZC·1) für eine konkret vorgegebene Gruppe G vor, der auf der Verwendung der Charaktertafel von G beruht. Es ist daher auch möglich, die Methode von Luthar und Passi auf Serien von Gruppen mit generischen Charaktertafeln anzuwenden. Auf diese Art wurden erstmals von R. Wagner [57] die Gruppen $PSL(2,p^f)$ bezüglich (ZC·1) untersucht.

Die Luthar-Passi-Methode kann die Frage, ob (ZC·1) für die Gruppe G wahr ist, im Allgemeinen nicht beantworten. Für Gruppen kleiner Ordnung ist sie aber oftmals ausreichend,

[1] Mit „(ZC·i) ist wahr für G“ ist gemeint, dass (ZC·i) für die Einheiten in $V(\mathbb{Z}G)$ richtig ist.

um (ZC·1) zu verifizieren (siehe z.B. [28]). In jedem Fall liefert die Methode aber wertvolle Informationen über die Torsionseinheiten im Gruppenring.

In [27] konnte M. Hertweck zeigen, dass die Methode mit Hilfe von Brauer-Charakteren von G auch p-modular angewendet werden kann. Dies hat die Methode für nicht-auflösbare Gruppen zwar wesentlich verbessert, mit wachsender Ordnung von G ist es aber auch mit der verbesserten Methode nicht mehr möglich, (ZC·1) für G vollständig zu beweisen.

Andere systematische Zugänge zum Beweis von (ZC·1) sind momentan nicht bekannt. Es ist daher sicherlich sinnvoll, schwächere Versionen von (ZC·1) zu untersuchen. Eine der ersten Fragen die sich stellt, ist die, ob es zu jedem Torsionselement u aus $V(\mathbb{Z}G)$ ein Element gleicher Ordnung in G gibt, oder äquivalent, ob es zu jeder endlichen zyklischen Untergruppe C in $V(\mathbb{Z}G)$ eine zu C isomorphe Gruppe in G gibt. Eine noch schwächere Formulierung ist dann die Frage, ob $\Gamma(G) = \Gamma(V(\mathbb{Z}G))$ gilt.

Da man G als Untergruppe von $V(\mathbb{Z}G)$ auffassen kann, ist klar, dass $\Gamma(G) \subseteq \Gamma(V(\mathbb{Z}G))$ ist. Schon das folgende, wohlbekannte Resultat zeigt für eine endliche Gruppe G, dass die Eckenmengen $\pi(G)$ und $\pi(V(\mathbb{Z}G))$ der Primgraphen übereinstimmen. Es gilt nämlich:

Satz 2.1 (Berman [4])**.** *Ist* G *eine endliche Gruppe und* H *eine endliche Untergruppe von* $V(\mathbb{Z}G)$*, dann teilt die Ordnung von* H *die Ordnung von* G*.*

Man weiß aber sogar noch mehr [12]:

Satz 2.2 (Cohn, Livingstone)**.** *Ist* G *eine endliche Gruppe und* H *eine endliche Untergruppe von* $V(\mathbb{Z}G)$*, dann gilt* $\exp(H) \mid \exp(G)$*.*

Nach [53, S.177] und [54, 45.11] gilt auch für unendliche Gruppen, dass die Ecken von $\Gamma(V(\mathbb{Z}G))$ mit den Ecken von $\Gamma(G)$ übereinstimmen. Als Folgerung erhält man daher:

Korollar 2.3. *Sei* G *eine beliebige Gruppe. Dann ist* $\Gamma(G \times G) = \Gamma\left(V\left(\mathbb{Z}(G \times G)\right)\right)$*.*

Es wird nun untersucht, wie sich der Primgraph der Einheitengruppe im Gruppenring unter endlichen, auflösbaren Erweiterungen der zugrunde liegenden Gruppe verhält. Dazu wird zunächst der Begriff der partiellen Augmentation eingeführt:

Für eine Konjugiertenklasse $[x]$ von G ist dann die partielle Augmentation von $v \in \mathbb{Z}G$ bezüglich $[x]$ als

$$\varepsilon_{[x]}(v) := \sum_{g \in [x]} \alpha_g(v)$$

definiert. Die partiellen Augmentationen spielen bei der Untersuchung von (ZC·1) eine wesentliche Rolle, denn es gilt:

Satz 2.4 ([46, Theorem 2.5]). *Sei* G *eine endliche Gruppe und* U *eine endliche Untergruppe von* $V(\mathbb{Z}G)$. *Dann sind äquivalent:*

(a) Jedes Element $u \in U$ *ist rational zu einem Element* $g \in G$ *konjugiert.*

(b) Für jedes $u \in U$ *gibt es genau eine Konjugiertenklasse* $[x]$ *von* G *mit* $\varepsilon_{[x]}(u) \neq 0$.

Dieser Satz führt also zu einer äquivalenten Formulierung von (ZC-1) mit Hilfe partieller Augmentationen:

Satz 2.5 ([46, Theorem 2.6]). (ZC-1) *ist für eine endliche Gruppe* G *genau dann wahr, wenn es für jede Torsionseinheit* $u \in V(\mathbb{Z}G)$ *genau eine Konjugiertenklasse* $[x]$ *von* G *gibt mit* $\varepsilon_{[x]}(u) \neq 0$.

Die partiellen Augmentationen ermöglichen einen algorithmischen Zugang zu (ZC-1). So beruht beispielsweise die oben erwähnte Luthar–Passi–Methode auf der Bestimmung möglicher partieller Augmentationen für Torsionseinheiten. Auch bei den folgenden Betrachtungen bezüglich des Primgraphen von $V(\mathbb{Z}G)$ liefert das Verwenden partieller Augmentationen den Zugang zu den Beweisen.

Ist $\varphi : G \longrightarrow \overline{G}$ ein Homomorphismus von Gruppen, dann bezeichne $\hat{\varphi} : \mathbb{Z}G \longrightarrow \mathbb{Z}\overline{G}$ den von φ induzierten Homomorphismus zwischen den Gruppenringen. Zunächst sei an ein wohlbekanntes Lemma (siehe z.B. [14]) erinnert.

Lemma 2.6. *Sei*

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\varphi} \overline{G} \longrightarrow 1$$

eine kurze exakte Sequenz endlicher Gruppen. Wenn p *die Ordnung von* N *nicht teilt, dann gibt es im Kern von* $\hat{\varphi}$ *keine Einheit der Ordnung* p.

Beweis. Angenommen, es sei $u \in V(\mathbb{Z}G)$ mit $o(u) = p$ und $\hat{\varphi}(u) = 1$. Nach [29], [4] ist $\alpha_1(u) = 0$. Für $\hat{\varphi}(u)$ gilt:

$$\hat{\varphi}(u) = \hat{\varphi}\left(\sum_{g \in G} \alpha_g(u) g\right) = \sum_{g \in G} \alpha_g(u) \varphi(g)\,.$$

Der Einskoeffizient $\alpha_1(\hat{\varphi}(u))$ ist also die Summe aller partieller Augmentationen $\varepsilon_{[x]}(u)$ für die $\varphi(x) = 1$ gilt. Für ein nicht-triviales $x \in G$ mit $\varphi(x) = 1$ gilt aber sicherlich $o(x) \neq p$, und wegen $o(u) = p$ ist dann nach [46, Theorem 2.7] $\varepsilon_{[x]}(u) = 0$. Der Einskoeffizient von $\hat{\varphi}(u)$ verschwindet also, im Widerspruch zu $\hat{\varphi}(u) = 1$. □

Für eine natürliche Zahl $n \in \mathbb{N}$ und ein Element $v \in \mathbb{Z}G$ bezeichne $\sigma_n(v)$ die Summe aller partieller Augmentationen von v bezüglich Konjugiertenklassen von G, die Elemente der Ordnung n enthalten. Setzt man $G(n) := \{g \in G\,;\, o(g) = n\}$ und $G'(n) := G \setminus G(n)$, dann ist also

$$\sigma_n(v) = \sum_{g \in G(n)} \alpha_g(v) \quad \text{und} \quad \varepsilon(v) = \sigma_n(v) + \sum_{g \in G'(n)} \alpha_g(v)\,.$$

Lemma 2.7. *Sei* $u \in V(\mathbb{Z}G)$ *mit* $o(u) = pq$, *wobei* p *und* q *zwei verschiedene Primzahlen sind. Dann ist*

$$\sigma_p(u) \equiv 0 \bmod p\,.$$

Beweis. Man schreibe $\varepsilon(u)$ in der Form

$$\varepsilon(u) = \sigma_p(u) + \sum_{g \in G'(p)} \alpha_g(u)\,.$$

Das Element u^p hat Ordnung q. Daher ist der Einskoeffizient von u^p gleich Null [29], [4].
Mit

$$[\mathbb{Z}G, \mathbb{Z}G] = \{uv - vu\ ;\ u, v \in \mathbb{Z}G\}$$

sei der additive Kommutator von $\mathbb{Z}G$ bezeichnet. Es gilt dann offensichtlich $\varepsilon(x) = 0$ für $x \in [\mathbb{Z}G, \mathbb{Z}G]$, und die Kongruenz (siehe z.B. [53, S.4])

$$u^p \equiv \sum_{g \in G(p)} \alpha(g) \underbrace{g^p}_{=1} + \sum_{g \in G'(p)} \alpha(g) g^p \mod [\mathbb{Z}G, \mathbb{Z}G] + p\mathbb{Z}G$$

liefert die Behauptung; denn für $g \in G'(p)$ gilt $g^p \neq 1$ und damit $\sigma_p(u) = \sigma_1(u^p) \equiv 0 \bmod p$. □

Mit Hilfe der beiden Lemmata kann man zeigen:

Lemma 2.8. *Sei*

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\varphi} \overline{G} \longrightarrow 1$$

eine kurze exakte Sequenz endlicher Gruppen, und seien p *und* q *verschiedene Primzahlen. Dann gilt:*

(i) Wenn $\overline{G}$ *Elemente der Ordnung* pq *besitzt, dann auch* G.

(ii) Die Ordnung von N *werde nicht von* q *geteilt und es sei* $\Gamma(V(\mathbb{Z}\overline{G})) = \Gamma(\overline{G})$. *Dann gilt: Wenn* $V(\mathbb{Z}G)$ *ein Element der Ordnung* pq *besitzt, dann auch* G.

Beweis.

(i) Klar.

(ii) Sei $u \in V(\mathbb{Z}G)$ mit $o(u) = pq$. Nach Lemma 2.6 ist $o(\hat{\varphi}(u)) \in \{q, pq\}$. Ist $o(\hat{\varphi}(u)) = pq$, dann besitzt $V(\mathbb{Z}\overline{G})$, und nach Voraussetzung auch $\overline{G}$, Elemente der Ordnung pq. Nach (i) gibt es dann auch in G solche Elemente. Es sei also $o(\hat{\varphi}(u)) = q$. Der Wert $\sigma_q(\hat{\varphi}(u))$ ist Summe aller partiellen Augmentationen $\varepsilon_{[x]}(u)$ mit $o(\varphi(x)) = q$. Wegen $o(u) = pq$ gilt nach [46, Theorem 2.7] $\varepsilon_{[x]}(u) = 0$ für jedes $x \in G$, dessen Ordnung von einer von p und q verschiedenen Primzahl geteilt wird. Es sei M die Menge aller Konjugiertenklassen $[x]$ von G, mit $o(x) = p^i q$ für ein $i \geqslant 1$ und $o(\varphi(x)) = q$. Da es im Kern von $\hat{\varphi}$ nach Lemma 2.6 keine Elemente der Ordnung q gibt, ist

$$\sigma_q(\hat{\varphi}(u)) = \sigma_q(u) + \sum_{[x] \in M} \varepsilon_{[x]}(u)\,.$$

Nach [12, Theorem 4.1] gilt $\sigma_q(\hat{\varphi}(u)) \not\equiv 0 \bmod q$, und nach Lemma 2.7 ist $\sigma_q(u) \equiv 0 \bmod q$. Es folgt also

$$\sum_{[x]\in M} \varepsilon_{[x]}(u) \not\equiv 0 \bmod q,$$

und damit muss es in G Elemente der Ordnung pq geben.

□

Letztendlich folgt nun

Proposition 2.9. *Es sei G eine endliche Gruppe mit $\Gamma(G) = \Gamma(V(\mathbb{Z}G))$ und*

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

eine kurze exakte Sequenz von Gruppen. Ist A eine p-Gruppe, dann ist

$$\Gamma(E) = \Gamma(V(\mathbb{Z}E)).$$

Beweis. Ist q eine von p verschiedene Primzahl, dann muss lediglich gezeigt werden, dass es in E ein Element der Ordnung pq gibt, wenn es in $V(\mathbb{Z}E)$ solch ein Element gibt. Da q die Ordnung von A nicht teilt, folgt das aber unmittelbar aus Lemma 2.8. □

Durch Induktion folgt für eine auflösbare Gruppe G sofort:

Korollar 2.10. *Ist G eine endliche auflösbare Gruppe, dann ist*

$$\Gamma(G) = \Gamma(V(\mathbb{Z}G)).$$

□

In der Zwischenzeit wurde von M. Hertweck [21] gezeigt, dass es für jedes Torsionselement u in den normierten Einheiten des ganzzahligen Gruppenrings einer endlichen, auflösbaren Gruppe G ein Element entsprechender Ordnung in G gibt.

KAPITEL 3

Zu den Einheiten im ganzzahligen Gruppenring minimal-einfacher Gruppen

3.1 Motivation

Seit den Arbeiten von T. Akasaki [1] und K. W. Roggenkamp [48] über idempotente Ideale im ganzzahligen Gruppenring ist bekannt, dass jede endliche Untergruppe H in der Einheitengruppe des ganzzahligen Gruppenrings einer auflösbaren Gruppe G wiederum auflösbar ist (für einen elementareren Beweis siehe [54, Lemma 7.4]). Jeder Kompositionsfaktor von H tritt also nach Satz 2.1 schon als Kompositionsfaktor von G auf.

Für die Einheiten im ganzzahligen Gruppenring von nicht-auflösbaren bzw. einfachen Gruppen ist man weit von einem solchen Resultat entfernt. Im Fall von Gruppenbasen von $\mathbb{Z}\mathsf{G}$ ist die Situation allerdings bekannt: Ist G eine beliebige endliche Gruppe, und $\mathsf{H} \leqslant \mathsf{V}(\mathbb{Z}\mathsf{G})$ mit $|\mathsf{H}| = |\mathsf{G}|$, dann besitzen G und H nach [40, Theorem 2.3] isomorphe Hauptreihen, d.h. die Hauptfaktoren von G und H stimmen überein. Insbesondere besitzen G und H also isomorphe Kompositionsfaktoren, bei denen auch jeweils die Multiplizitäten übereinstimmen.

Es stellt sich die Frage, ob es für jede endliche Gruppe G und jeden Kompositionsfaktor K einer endlichen Gruppe $\mathsf{H} \leqslant \mathsf{V}(\mathbb{Z}\mathsf{G})$ stets eine Untergruppe U von G gibt, die einen zu K isomorphen Kompositionsfaktor besitzt. Die Frage stellt sich also nur bei nicht-auflösbaren Kompositionsfaktoren bzw. nicht-auflösbaren Gruppen H.

Beschränkt man sich bei der nicht-auflösbaren Gruppe G zunächst auf eine minimal-einfache endliche Gruppe, dann wird im Folgenden gezeigt, dass jede nicht-auflösbare endliche Untergruppe von $\mathsf{V}(\mathbb{Z}\mathsf{G})$ isomorph zu G ist.

Definition 3.1. Eine nicht-abelsche einfache Gruppe G heißt minimal-einfach, wenn jede echte Untergruppe von G auflösbar ist.

Die Definition ist nicht auf endliche Gruppen beschränkt. Im Folgenden sind aber nur endliche minimal-einfache Gruppen von Interesse. Deren Klassifikation geht aus einer fundamentalen, sehr umfangreichen Arbeit von J. G. Thompson hervor:

Satz 3.2 (Thompson [56, 3, Corollary 1])**.** *Eine endliche minimal-einfache Gruppe* G *ist isomorph zu einer der folgenden Gruppen*[1]*:*

- $\mathsf{PSL}(2, 2^p)$*, mit* p *prim.*
- $\mathsf{PSL}(2, 3^p)$*, mit* p *ungerade und prim.*
- $\mathsf{PSL}(2, p)$ *, mit* $p \neq 3$ *prim und* $p^2 + 1 \equiv 0$ *mod* 5*.*
- $\mathsf{PSL}(3, 3)$*.*
- $\mathsf{Sz}(2^p)$*, mit* $p \geqslant 3$ *prim.*

Man beachte dabei, dass $\mathsf{PSL}(2,5) \cong \mathsf{PSL}(2,4) \cong \mathsf{A}_5$ ist. Durch die Bedingung $p^2 + 1 \equiv 0 \bmod 5$ an die Gruppen in der Serie $\mathsf{PSL}(2, p)$ lässt sich also jede endliche minimal-einfache Gruppe genau einem der obigen Typen zuordnen.

Für die endlichen minimal-einfachen Gruppen soll in diesem Kapitel der folgende Satz gezeigt werden.

Satz 3.3. *Ist* G *eine endliche, minimal-einfache Gruppe und* H *eine Untergruppe von* $\mathsf{V}(\mathbb{Z}G)$ *mit* $|H| < |G|$*, dann ist* H *auflösbar.*

3.2 Zutaten zum Beweis

3.2.1 Ordnungsargumente

Einer der wichtigsten Bestandteile des Beweises von Satz 3.3 ist der schon im vorangegangenen Kapitel benutzte Satz 2.1:

Satz 2.1 (Berman)**.** *Ist* G *eine endliche Gruppe und* H *eine endliche Untergruppe von* $\mathsf{V}(\mathbb{Z}G)$*, dann teilt die Ordnung von* H *die Ordnung von* G*.*

Es wird sich zeigen, dass man Satz 3.3 allein aufgrund dieser einfachen Teilbarkeits-Beziehung zwischen den Ordnungen von G und H in den Fällen $G \cong \mathsf{PSL}(3,3)$ und $G \cong \mathsf{Sz}(2^p)$ beweisen kann. Man braucht dazu lediglich noch das folgende wohlbekannte zahlentheoretische Lemma:

[1] In der Lie-Notation entsprechen die Gruppen $\mathsf{PSL}(n, q)$ den Gruppen $\mathsf{A}_{n-1}(q)$ und die Gruppen $\mathsf{Sz}(2^n)$ den Gruppen ${}^2\mathsf{B}_2(2^n)$

Lemma 3.4. *Es seien* $x, n, m \in \mathbb{N}$. *Dann gilt*

$$x^n - 1 \,\big|\, x^m - 1 \iff n \,\big|\, m\,.$$

Beweis. Gilt $n \,\big|\, m$, also $m = an$ für ein $a \in \mathbb{Z}$, dann ist $x^m - 1 = (x^n)^a - 1$. Setzt man $y := x^n$, dann gilt

$$y^a - 1 = (y^{a-1} + \ldots + 1) \cdot (y - 1)\,.$$

Gilt umgekehrt $x^n - 1 \,\big|\, x^m - 1 = x^n \cdot x^{m-n} - 1 = x^{m-n}(x^n - 1) + x^{m-n} - 1$, dann folgt $x^n - 1 \,\big|\, x^{m-n} - 1$. Iteriert man dieses Vorgehen, so folgt nach a Schritten $x^n - 1 \,\big|\, x^{m-an} - 1$. Die Iteration bricht ab, wenn $an \geqslant m$ ist. Wegen der Teilbarkeitsbedingung muss dann $an = m$ gelten. □

3.2.2 Elementar-abelsche Untergruppen in $V(\mathbb{Z}G)$

Für eine beliebige Gruppe G zeigt Satz 2.1, dass eine zyklische Gruppe C_p von Primzahlordnung p nur dann als Untergruppe von $V(\mathbb{Z}G)$ auftreten kann, wenn es auch in G eine solche Gruppe gibt. Für eine beliebige, endliche Gruppe H ist die Frage völlig offen, ob die Existenz von einer zu H isomorphen Gruppe in $V(\mathbb{Z}G)$ die Existenz einer solchen Gruppe in G impliziert. Z. Marciniak regte 2006 an, diese Frage zunächst für die Kleinsche Vierergruppe $C_2 \times C_2$ zu untersuchen. Als Antwort auf diese Frage konnte W. Kimmerle zeigen [36]:

Satz 3.5. *Es sei* G *eine endliche Gruppe. In* $V(\mathbb{Z}G)$ *gibt es genau dann eine zu* $C_2 \times C_2$ *isomorphe Untergruppe, wenn es eine solche Gruppe in* G *gibt.*

Dieses Resultat stellt, neben dem altbekannten Resultat über zyklische Gruppen, das erste allgemeine Ergebnis dieser Art dar. In [22] konnte M. Hertweck den entsprechenden Satz für ungerade Primzahlen zeigen:

Satz 3.6. *Es sei* G *eine endliche Gruppe und* p *eine ungerade Primzahl. In* $V(\mathbb{Z}G)$ *gibt es genau dann eine zu* $C_p \times C_p$ *isomorphe Untergruppe, wenn es eine solche Gruppe in* G *gibt.*

Der Beweis beruht auf der Verwendung von Charakteren einer potentiellen Untergruppe $C_p \times C_p$ von $V(\mathbb{Z}G)$ (vgl. Abschnitt 3.2.4).
Im Beweis von Satz 3.3 wird dieser Satz an einigen Stellen eingehen.

3.2.3 Anzahl von Konjugiertenklassen

Ein anderes Hilfsmittel im Beweis wird die Anzahl von Konjugiertenklassen von Elementen von Primzahlordnung sein. Bezeichnet $\mathrm{ccl}_G(n)$ die Menge der Konjugiertenklassen in G, die Elemente der Ordnung n enthalten, dann kann man unter bestimmten Voraussetzungen für eine ungerade Primzahl p und $H \leqslant V(\mathbb{Z}G)$ zeigen, dass

$$|\mathrm{ccl}_G(p)| \leqslant |\mathrm{ccl}_H(p)|$$

sein muss. Es gilt nämlich:

Lemma 3.7. *Es sei* G *eine Gruppe mit zyklischen* p*-Sylowgruppen und jede Torsionseinheit der Ordnung* p *aus* $V(\mathbb{Z}G)$ *sei rational zu einem Element von* G *konjugiert. Ist* $H \leqslant V(\mathbb{Z}G)$ *eine Torsionsuntergruppe deren Ordnung von* p *geteilt wird, dann gilt* $|\mathrm{ccl}_H(p)| \geqslant |\mathrm{ccl}_G(p)|$.

Beweis. Angenommen $|\mathrm{ccl}_H(p)| < |\mathrm{ccl}_G(p)| =: n$ und es sei $h \in H$ mit $o(h) = p$. Nach Voraussetzung gibt es ein $z \in V(\mathbb{Z}G)$ mit $h^z = x \in G$. Da die p-Sylowgruppen von G zyklisch sind, enthält $\langle x \rangle$ ein Repräsentantensystem von $\mathrm{ccl}_G(p)$. Ein solches System sei durch $\{x = x^{i_1}, x^{i_2}, \ldots, x^{i_n}\}$ gegeben. Für alle i_j mit $1 \leqslant j \leqslant n$ gilt $(h^{i_j})^z = x^{i_j}$. Wegen $|\mathrm{ccl}_H(p)| < |\mathrm{ccl}_G(p)| = n$ gibt es aber mindestens ein Paar s, t mit $h^{i_s} \sim h^{i_t}$ und damit $x^{i_s} \sim x^{i_t}$. Das steht aber im Widerspruch dazu, dass x^{i_s} und x^{i_t} verschiedene Konjugiertenklassen von G repräsentieren. □

Um dieses Lemma später im Beweis anwenden zu können ist noch folgende, häufig verwendete Folgerung aus dem Satz von Schur-Zassenhaus wichtig:

Lemma 3.8. *Es sei* p *eine Primzahl und für eine* p'*-Gruppe* N *sei*

$$1 \longrightarrow N \longrightarrow E \xrightarrow{\kappa} G \longrightarrow 1$$

eine kurze exakte Sequenz. Dann sind Elemente $x, y \in E$ *mit* $o(x) = o(y) = p$ *genau dann konjugiert in* E*, wenn* $\kappa(x)$ *und* $\kappa(y)$ *in* G *konjugiert sind.*

Beweis. Ist x zu y konjugiert, dann sicherlich auch $\kappa(x)$ zu $\kappa(y)$.

Sei also $\kappa(x)$ zu $\kappa(y)$ konjugiert. Es gibt dann ein $g \in G$ mit $\kappa(x)^g = \kappa(y)$. Also gibt es Elemente $e \in E$ und $n \in N$ mit $x^e = yn$. Mit x hat dann auch yn Ordnung p. Für eine Sylowgruppe $\overline{S} \in \mathrm{Syl}_p(G)$ mit $\kappa(y) \in \overline{S}$ ist, nach dem Satz von Schur-Zassenhaus, die kurze exakte Sequenz

$$1 \longrightarrow N \longrightarrow \kappa^{-1}(\overline{S}) \xrightarrow{\kappa} \overline{S} \longrightarrow 1$$

split, und es gilt $\kappa^{-1}(\overline{S}) = S \cdot N$ für eine Sylowgruppe $S \in \mathrm{Syl}_p(E)$ und $y \in S$. Verschiedene Komplemente sind via Elementen aus N konjugiert. Es gibt also ein $m \in N$, so dass y und $(yn)^m$ in S liegen. Die Einschränkung $\kappa|_S$ ist injektiv und daher gilt $y = (yn)^m$. Insgesamt erhält man also $y = (yn)^m = x^m$ und damit ist x konjugiert zu y. □

3.2.4 Zum Gruppenring von $\mathrm{PSL}(2, p^f)$

Der Beweis von Satz 3.3 wird sich größtenteils auf den Fall $G = \mathrm{PSL}(2, p^f)$ reduzieren. In diesem Abschnitt soll daher Bekanntes über diese Gruppen und ihren Gruppenring bereitgestellt werden. Außerdem werden abelsche 2-Gruppen in $V(\mathbb{Z}G)$ genauer untersucht. Dieser

Abschnitt stellt auch die Grundlage für das folgende Kapitel 4 dar.

Ist $G = \mathsf{PSL}(2, p^f)$, dann gilt für die Ordnung von G

$$|G| = \frac{1}{d} p^f (p^f - 1)(p^f + 1) \quad \text{mit} \quad d = \begin{cases} 1 & \text{für } p = 2 \\ 2 & \text{sonst} \end{cases},$$

und G besitzt nach L. E. Dickson genau die folgenden Untergruppen (siehe z.B. [32, II, Satz 8.27]):

(1) Elementar-abelsche p-Gruppen.
(2) Zyklische Gruppen der Ordnung z mit $z \mid \frac{p^f \pm 1}{k}$, wobei $k = (p^f - 1, 2)$ ist.
(3) Diedergruppen D_z der Ordnung $2z$ mit z wie in (2).
(4) Alternierende Gruppen A_4 für $p > 2$ oder $p = 2$ und $f \equiv 0 \bmod 2$.
(5) Symmetrische Gruppen S_4 für $p^{2f} - 1 \equiv 0 \bmod 16$.
(6) Alternierende Gruppen A_5 für $p = 5$ oder $p^{2f} - 1 \equiv 0 \bmod 5$.
(7) Semidirekte Produkte von elementar-abelschen Gruppen der Ordnung p^m mit zyklischen Gruppen der Ordnung t. Dabei teilt t sowohl $p^m - 1$ als auch $\frac{p^f - 1}{k}$, wobei $k = (p^f - 1, 2)$ ist.
(8) Gruppen $\mathsf{PSL}(2, p^m)$ für $m \mid f$ und $\mathsf{PGL}(2, p^m)$ für $2m \mid f$.

Teilt p die Ordnung eines Elements $g \in G$, dann ist $o(g) = p$. Ist $p \neq 2$ dann G gibt es zwei Konjugiertenklassen mit Elementen der Ordnung p.
Ist $g \in G$ mit $p \nmid o(g) = n$, dann gilt $n \mid p^f \pm 1$ und in G gibt es $\frac{\phi(n)}{2}$ Konjugiertenklassen mit Elementen der Ordnung n. Dabei ist ϕ die Eulersche ϕ-Funktion. Ist insbesondere r eine von p verschiedene ungerade Primzahl, dann gibt es genau $\frac{r-1}{2}$ Konjugiertenklassen mit Elementen der Ordnung r. Dabei ist jedes Element der Ordnung r zu seinem Inversen konjugiert. Außerdem gibt es stets genau eine Konjugiertenklasse mit Involutionen.

Zyklische Untergruppen in den Einheiten des Gruppenrings

Die Torsionseinheiten in den normierten Einheiten im ganzzahligen Gruppenring von $\mathsf{PSL}(2, p^f)$ wurden erstmals von R. Wagner [57] mit Hilfe generischer Charaktertafeln untersucht (die Ergebnisse finden sich auch in [10]). Die Ergebnisse wurden von M. Hertweck [27] wesentlich verbessert. Die hier relevanten Ergebnisse von Wagner und Hertweck lauten zusammengefasst:

Satz 3.9. *Ist* $G = PSL(2, p^f)$ *und* $u \in V(\mathbb{Z}G)$ *mit* $o(u) = n$. *Dann gilt*

a) Ist $p \neq 2$, $f \leqslant 2$ *und* $n = p$, *dann ist* $u \underset{\mathbb{Q}G}{\sim} g \in G$.

b) Ist $p \neq 2$, $f = 1$ *und* $p \mid n$, *dann ist* $n = p$.

c) Ist $r \neq p$ *prim und* $n = r$, *dann ist* $u \underset{\mathbb{Q}G}{\sim} g \in G$.

d) Ist $p \neq 2, 3$ *und* $n = 6$, *dann ist* $u \underset{\mathbb{Q}G}{\sim} g \in G$.

e) Gilt $p \nmid n$, *dann gibt es ein* $g \in G$ *mit* $o(g) = n$.

Beweis. Teil a) und b) des Satzes werden in [57], die Teile c) - e) in [27] bewiesen. □

Als Folgerung von [27, Proposition 6.5] erhält man

Korollar 3.10. *Ist* $G = PSL(2, p^f)$ *und* $u \in V(\mathbb{Z}G)$ *mit* $o(u) = 4$. *Dann ist* $u \underset{\mathbb{Q}G}{\sim} g \in G$.

Beweis. Ist $p = 2$, dann ist $2 \parallel \exp(G)$ und nach Satz 2.2 gibt es keine Elemente der Ordnung 4. Ist $p \neq 2$, dann gibt es in G je genau eine Konjugiertenklasse $[i]$ mit Elementen der Ordnung 2 und $[h]$ mit Elementen der Ordnung 4. Sei $u \in V(\mathbb{Z}G)$ mit $o(u) = 4$. Ist $g \in G$ mit $o(g) \neq 2, 4$, dann ist $\varepsilon_{[g]}(u) = 0$. Mit den Bezeichnungen aus Kapitel 2 lässt sich $\varepsilon(u)$ daher als

$$1 = \varepsilon(u) = \sigma_2(u) + \sigma_4(u) = \varepsilon_{[i]}(u) + \varepsilon_{[h]}(u)$$

schreiben. Nach [27, Proposition 6.5] ist $\sigma_2(u) = 0$, und damit $\sigma_4(u) = \varepsilon_{[h]}(u) = 1$. Aus Satz 2.5 folgt dann $u \underset{\mathbb{Q}G}{\sim} g$ für ein $g \in G$. □

Abelsche 2-Untergruppen in den Einheiten des Gruppenrings

Die Idee, die zum Beweis der unten folgenden Proposition 3.11 führt, und auch speziell im Kapitel 4 noch weiter genutzt wird, ist die Verwendung von Charakteren einer Gruppe G als Charaktere einer endlichen Untergruppe H von $V(\mathbb{Z}G)$:

Es sei G eine beliebige endliche Gruppe, $\chi \in \mathrm{Irr}(G)$ ein irreduzibler Charakter und D die zugehörige Darstellung. Durch lineare Ausdehnung wird D dann zu einer Darstellung $D\big|^{V(\mathbb{Z}G)}$ von $V(\mathbb{Z}G)$. Diese kann zu einer Darstellung $D\big|_H^{V(\mathbb{Z}G)}$ der Untergruppe H eingeschränkt werden. Der zugehörige Charakter ist dann $\chi\big|_H^{V(\mathbb{Z}G)}$. Auf diese Art kann also ein Charakter von G als Charakter von H aufgefasst werden, daher wird im Folgenden kurz $\chi\big|_H$ für $\chi\big|_H^{V(\mathbb{Z}G)}$ geschrieben. Verwendet wird der so gewonnene Charakter von H in Kombination mit einem beliebigen irreduziblen gewöhnlichen Charakter $\psi \in \mathrm{Irr}(H)$[2]:

Das Standardskalarprodukt $\langle \chi\big|_H, \psi \rangle$ muss einen nicht-negativen ganzzahligen Wert annehmen.

[2]Die Idee hierfür stammt aus gemeinsamen Diskussionen mit Wolfgang Kimmerle. Sie wird auch in [22] verwendet (χ nicht notwendig irreduzibel).

Bei der Überprüfung dieser Bedingung ist das Verwenden von generischen Charaktertafeln möglich. Die Bereitstellung von generischen Charaktertafeln ist ein Ziel des Computer Algebra Projekts `CHEVIE` [19].

Die hier verwendeten generischen Charaktertafeln der Gruppen $\mathsf{PSL}(2,p^f)$ (Tabellen A.1 und A.2 im Anhang) sind [19] entnommen, wurden aber bereits von G. Frobenius [17] und I. Schur [51] gefunden. Diese Charaktertafeln werden zunächst dazu benutzt, mit Hilfe der obigen Überlegung die folgende Proposition zu beweisen.

Proposition 3.11. *Ist* $G = \mathsf{PSL}(2,p^f)$*, dann ist jede endliche abelsche 2-Untergruppe von* $V(\mathbb{Z}G)$ *isomorph zu einer Untergruppe von* G*. Ist p=2, dann gilt das für jede endliche 2-Untergruppe.*

Beweis. Sei $p = 2$ und $U \leqslant V(\mathbb{Z}G)$ eine endliche 2-Untergruppe. Die Aussage ist dann klar, denn wegen $2 \,\|\, \exp(G)$ ist U elementar-abelsch und somit, wegen $|U| \,\big|\, |G|$, isomorph zu einer Untergruppe von G.

Sei also $p \neq 2$ und $A \leqslant V(\mathbb{Z}G)$ eine endliche abelsche 2-Untergruppe. Die maximalen abelschen 2-Untergruppen von G sind dann isomorph zu $C_2 \times C_2$ und C_{2^n}, mit $2^{n+1} \,\|\, |G|$. Die Aussage folgt dann aus den beiden Behauptungen:

Behauptung 1: A enthält keine elementar-abelsche Untergruppe E_8 der Ordnung 8.

Behauptung 2: A enthält keine Untergruppe der Form $C_2 \times C_4$

Beweis der Behauptungen.

In $V(\mathbb{Z}G)$ sind Involutionen rational zu Elementen von G konjugiert, da es in G nur eine Konjugiertenklasse $[\iota]$ von Involutionen gibt. Ist χ ein Charakter von G und $\tau \in A$ eine Involution, dann gilt also $\chi(\tau) = \chi(\iota)$.

- ad Behauptung 1: O.B.d.A. sei $A = E_8$ und $\psi \in \mathrm{Irr}(E_8)$ ein vom trivialen Charakter verschiedener Charakter.

  Ist $p^f \equiv 1 \bmod 4$, dann gilt $8 \,\big|\, p^f - 1$ (wegen $8 = |A| \,\big|\, |G|$). In Tabelle A.1 wird die Konjugiertenklasse der Involutionen durch den Repräsentanten $a^{\frac{p^f-1}{4}}$, d.h. $l = \frac{p^f-1}{4}$ beschrieben. Beim Charakter δ_2 nehmen die Involutionen den Wert

  $$\delta_2(\iota) = \rho^{\frac{p^f-1}{2}} + \rho^{-\frac{p^f-1}{2}} = -2$$

  an. Es folgt dann

  $$\begin{aligned} |A|\langle \delta_2\big|_A, \psi\rangle &= \sum_{h\in A} \delta_2\big|_A(h)\psi(h^{-1}) = \delta_2\big|_A(1)\psi(1) + \delta_2\big|_A(\iota) \sum_{o(h)=2} \psi(h) \\ &= p^f + 1 + (-2)\cdot(-1) = p^f + 3\,. \end{aligned}$$

Also muss $8 \mid p^f + 3$ gelten, was aber wegen $8 \mid p^f - 1$ unmöglich ist.

Ist $p^f \equiv -1 \bmod 4$, dann gilt $8 \mid p^f + 1$ und der Widerspruch folgt völlig analog zum ersten Fall, wenn man mit Charakter θ_2 aus Tabelle A.2 die Bedingung $\langle \theta_2|_A, \psi \rangle \in \mathbb{Z}$ betrachtet. Die Involutionen werden in diesem Fall von $b^{\frac{p^f+1}{4}}$, d.h. $e = \frac{p^f+1}{4}$ repräsentiert und nehmen auf θ_2 den Charakterwert

$$\theta_2(\iota) = -\sigma^{\frac{p^f+1}{2}} - \sigma^{-\frac{p^f+1}{2}} = 2$$

an. Es folgt dann

$$\begin{aligned} |A|\langle \theta_2|_A, \psi \rangle &= \sum_{h \in A} \theta_2|_A(h)\psi(h^{-1}) = \theta_2|_A(1)\psi(1) + \theta_2|_A(\iota) \sum_{o(h)=2} \psi(h) \\ &= p^f - 1 + 2 \cdot (-1) = p^f - 3\,. \end{aligned}$$

Es muss also $|A| = 8$ den Wert $p^f - 3$ teilen, was im Widerspruch zu $8 \mid p^f + 1$ steht.

- ad Behauptung 2: O.B.d.A. sei $A = C_2 \times C_4$. Die Charakterwerte von Involutionen aus A müssen wiederum mit denen von Involutionen aus G übereinstimmen, da es nur eine Konjugiertenklasse mit Involutionen in G gibt. Auch für Elemente der Ordnung 4 weiß man nach Korollar 3.10, dass (ZC·1) wahr ist. Die Aussage kann aber auch ohne das Verwenden dieses Korollars gezeigt werden. In G gibt es nur eine Konjugiertenklasse $[\omega]$ mit Elementen der Ordnung 4. Für ein Element $x \in A$ der Ordnung 4 und einen Charakter χ von G gilt daher $\chi|_A(x) = \varepsilon_2(x)\chi|_A(\iota) + \varepsilon_4(x)\chi|_A(\omega)$ mit $\varepsilon_2(x) + \varepsilon_4(x) = 1$. Nach [12] gilt $\varepsilon_2(x) \equiv 0 \bmod 2$ und $\varepsilon_4(x) \equiv 1 \bmod 2$.

  Es $y \in A$, $\psi \in \mathrm{Irr}(A)$ der Charakter mit

$$\psi(y) = \begin{cases} -1 & \text{wenn } o(y) = 4 \\ 1 & \text{sonst} \end{cases},$$

  und mit (x_1, x_2) und (x_3, x_4) seien die beiden Paare zueinander inverser Elemente der Ordnung 4 in A bezeichnet.

  In den Tabellen A.1 und A.2 werden die Konjugiertenklassen von Elementen der Ordnung 4 durch $a^{\frac{p^f-1}{8}}$ (d.h. $l = \frac{p^f-1}{8}$), bzw. $b^{\frac{p^f+1}{8}}$ (d.h. $m = \frac{p^f+1}{8}$) beschrieben.

  Betrachtet man für $p^f \equiv 1 \bmod 4$ wiederum den Charakter δ_2, dann gilt

$$\delta_2(a^l) = \rho^{\frac{p^f-1}{8}} + \rho^{-\frac{p^f-1}{8}} = 0\,.$$

  Ein Element $x \in A$ mit $o(x) = 4$ nimmt also den Charakterwert $\delta_2|_A(x) = -2\varepsilon_2(x)$ an. Wegen $\delta_2|_A(x) \in \mathbb{Z}$ gilt $\delta_2|_A(x) = \delta_2|_A(x^{-1})$, und man erhält

$$\begin{aligned} |A|\langle \delta_2|_A, \psi \rangle &= \sum_{h \in A} \delta_2|_A(h)\psi(h^{-1}) \\ &= \delta_2|_A(1)\psi(1) + \delta_2|_A(\iota) \sum_{o(h)=2} \psi(h) + \delta_2|_A(\iota)\,(2\varepsilon_2(x_1) + 2\varepsilon_2(x_3)) \\ &= p^f + 1 - 2 \cdot 3 - 4\,(\varepsilon_2(x_1) + \varepsilon_2(x_3)) = p^f - 5 + 4\,(\varepsilon_2(x_1) + \varepsilon_2(x_3))\,. \end{aligned}$$

Da $\varepsilon_2(x_i) \equiv 0 \bmod 2$ ist, folgt $8 \mid p^f - 5$, was aber wegen $8 \mid p^f - 1$ unmöglich ist.

Für $p^f \equiv -1 \bmod 4$ erhält man, wiederum mit θ_2, einen völlig analogen Widerspruch. Hier gilt

$$\theta_2(b^m) = -\sigma^{\frac{p^f+1}{8}} - \sigma^{-\frac{p^f+1}{8}} = 0\,,$$

und ein Element $x \in A$ mit $o(x) = 4$ nimmt den Charakterwert $\theta_2\big|_A(x) = 2\varepsilon_2(x)$ an. Wegen $\theta_2\big|_A(x) \in \mathbb{Z}$ gilt $\theta_2\big|_A(x) = \theta_2\big|_A(x^{-1})$, und man erhält

$$\begin{aligned} |A|\langle \theta_2\big|_A, \psi\rangle &= \sum_{h\in A} \theta_2\big|_A(h)\psi(h^{-1}) \\ &= \theta_2\big|_A(1)\psi(1) + \theta_2\big|_A(\iota) \sum_{o(h)=2} \psi(h) + \theta_2\big|_A(\iota)\,(2\varepsilon_2(x_1) + 2\varepsilon_2(x_3)) \\ &= p^f - 1 + 2\cdot 3 + 4\,(\varepsilon_2(x_1) + \varepsilon_2(x_3)) = p^f + 5 + 4\,(\varepsilon_2(x_1) + \varepsilon_2(x_3))\ . \end{aligned}$$

Da $\varepsilon_2(x_i) \equiv 0 \bmod 2$ ist, folgt $8 \mid p^f + 5$, was aber wegen $8 \mid p^f + 1$ unmöglich ist.

□

Mit Wissen aus der elementaren Theorie der 2-Gruppen erhält man nun:

Korollar 3.12. *Ist* $G = \mathrm{PSL}(2, p^f)$ *mit* $p \neq 2$ *und* $S \leqslant V(\mathbb{Z}G)$ *eine endliche 2-Gruppe, dann ist* $S \leqslant D_4$ *oder aber jeder abelsche Normalteiler von* S *ist zyklisch. In jedem Fall enthält* S *einen zyklischen Normalteiler vom Index 2.*

Beweis. Sei M ein maximaler abelscher Normalteiler von S. Nach obiger Proposition ist M isomorph zu $C_2 \times C_2$ oder M ist zyklisch. Ist $M \cong C_2 \times C_2$, dann gilt $|S| \leqslant 8$ nach [32, III, Satz 7.2a)]. Da S nicht isomorph zu E_8 sein kann, ist $S \leqslant D_4$ und besitzt einen zyklischen Normalteiler vom Index 2.

Sind alle maximalen abelschen Normalteiler von S zyklisch, dann folgt die Aussage aus [32, III, Satz 7.6]. □

3.3 Beweis des Satzes

Mit Hilfe der vorangestellten Eigenschaften der minimal-einfachen Gruppen und ihrer Gruppenringe kann nun das Hauptresultat dieses Kapitels bewiesen werden:

Satz 3.3. *Ist* G *eine endliche minimal-einfache Gruppe und* H *eine Untergruppe von* $V(\mathbb{Z}G)$ *mit* $|H| < |G|$*, dann ist* H *auflösbar.*

Der Beweis wird unter der Annahme eines kleinsten Gegenbeispiel geführt. Im Folgenden sei G eine minimal-einfache Gruppe und $H \leqslant V(\mathbb{Z}G)$ eine nicht-auflösbare Gruppe mit $|H| < |G|$. Die Gruppen G und H können so gewählt werden, dass H ein minimales Gegenbeispiel bezüglich

der Ordnung ist, d.h. für alle minimal-einfachen Gruppen $\widetilde{G}$ und alle Gruppen $\widetilde{H} \leqslant V(\mathbb{Z}\widetilde{G})$ mit $|\widetilde{H}| < |\widetilde{G}|$ und $|\widetilde{H}| < |H|$ gilt, dass $\widetilde{H}$ auflösbar ist. Besitzt H diese Eigenschaft, dann heißt H kleinster Verbrecher zu Satz 3.3.

Zunächst soll die Struktur eines kleinsten Verbrechers H näher untersucht werden. Es gilt

Lemma 3.13. *H ist eine perfekte Gruppe, die einer kurzen exakten Sequenz*

$$1 \longrightarrow A \longrightarrow H \xrightarrow{\varphi} H_0 \longrightarrow 1$$

genügt. Dabei ist A ein auflösbarer Normalteiler von H und H_0 eine minimal-einfache Gruppe. Ist $A \neq 1$, dann ist die Sequenz nicht-split.

Beweis. Ist

$$1 \trianglelefteq N_n \trianglelefteq N_{n-1} \trianglelefteq \ldots \trianglelefteq N_1 \trianglelefteq H$$

eine Kompositionsreihe von H, dann folgt aus der Minimalität von H, dass N_1 eine auflösbare Gruppe ist und damit $H_0 := H/N_1$ nicht-auflösbar einfach. Ist H_0 nicht minimal-einfach, dann gibt es eine nicht-auflösbare Gruppe $X < H_0$ und $\varphi^{-1}(X)$ enthält eine nicht-auflösbare Untergruppe von H, im Widerspruch zur Minimalität von H. Würde die Sequenz im Fall $A = 1$ zerfallen, dann wäre $H_0 \leqslant V(\mathbb{Z}G)$, wiederum im Widerspruch zur Minimalität von H. □

Im Folgenden bezeichnet H_0 immer den nicht-auflösbaren Kompositonsfaktor von $H \leqslant V(\mathbb{Z}G)$. Der Beweis von Satz 3.3 lässt sich dann durch Betrachten aller Kombinationen von G und H_0 führen, wobei beide Gruppen minimal-einfach sind.

3.3.1 $G = Sz(2^p)$

Ist H_0 keine Suzukigruppe, dann besitzt H_0 - und damit auch H - Elemente der Ordnung 3. Da G keine Elemente der Ordnung 3 besitzt, steht dies im Widerspruch zu Satz 2.1. Es ist also $H_0 \cong Sz(2^n)$ mit ungeradem n. Wegen Satz 2.1 gilt

$$2^{2n}(2^{2n}+1)(2^n-1) = |H_0| \;\Big|\; |H| \;\Big|\; |G| = 2^{2p}(2^{2p}+1)(2^p-1)\,.$$

Insbesondere erhält man

$$2^n - 1 \,\Big|\, (2^{2p}+1)(2^p-1)(2^p+1) = 2^{4p} - 1\,.$$

Nach Lemma 3.4 folgt dann $n \,\big|\, 4p$. Da n ungerade ist gilt $n = p$ und damit $H_0 = G$. Es gibt also keinen Verbrecher.

3.3.2 $G = PSL(3,3)$

Es ist $|G| = 2^4 \cdot 3^3 \cdot 13$, also insbesondere $|\pi(G)| \leqslant 4$. In [34] wurden die Gruppen mit $|\pi(G)| \leqslant 4$ klassifiziert und gezeigt, dass jede einfache Gruppe S mit $\pi(S) = \{2,3,13\}$ isomorph zu $PSL(3,3)$ ist. Da Gruppen mit nur zwei Primteilern nach Burnside auflösbar sind (siehe z.B. [32, V, 7.3 Hauptsatz]), folgt $\pi(H_0) = \{2,3,13\}$ und somit $H_0 \cong G$. Wegen Satz 2.1 folgt dann $H \cong H_0 \cong G$ und H ist kein kleinster Verbrecher.

3.3.3 $G = PSL(2,p^f)$: Vorbereitung für die verbleibenden Fälle

Der Fall $p = f = 2$ also $G = PSL(2,4) \cong A_5$ ist trivial, da es in diesem Fall keine nichtauflösbare Gruppe mit kleinerer Ordnung als der von G gibt. Im Folgenden gilt also stets $(p,f) \neq (2,2)$.

Ist r eine von p verschiedene, ungerade Primzahl, dann besitzt G nach Dickson (Abschnitt 3.2.4) zyklische r-Sylowgruppen. Insbesondere enthält G, und damit $V(\mathbb{Z}G)$ keine Untergruppen der Form $C_r \times C_r$. Nach [32, III, Satz 7.6] sind also auch die r-Sylowgruppen von H zyklisch, insbesondere also abelsch.

Die Struktur von Gruppen mit abelschen Sylowgruppen ist bekannt. Für Gruppen mit abelschen 2-Sylowgruppen wurde die Struktur von J. Walter [58, Theorem 1] bestimmt (kurze Zeit später gab H. Bender [3] einen stark verkürzten Beweis). Der Fall für ungerades p geht auf W. Kimmerle und R. Sandling [41, Theorem 2.1] zurück und benutzt die Klassifikation der endlichen einfachen Gruppen.

Satz 3.14. *Eine endliche Gruppe G besitzt genau dann abelsche p-Sylowgruppen, wenn $O^{p'}(G/O_{p'}(G))$ das direkte Produkt einer abelschen p-Gruppe mit einfachen Gruppen ist, deren p-Sylowgruppen jeweils nicht-trivial sind.*

Ist $p = 2$, dann ist jeder nicht-abelsche Faktor von $O^{p'}(G/O_{p'}(G))$ isomorph zu einer der folgenden Gruppen:

(a) $PSL(2,2^f)$.

(b) $PSL(2,q)$ *mit* $q \equiv 3,5$ *mod* 8.

(c) Die Janko-Gruppe J_1.

(d) Eine Ree-Gruppe ${}^2G_2(q)$.

In der hier vorliegenden Situation bedeutet dies, dass wenn r (von p verschiedene ungerade Primzahl) die Ordnung von H_0 teilt, dann ist der auflösbare Normalteiler $A \trianglelefteq H$ aus Lemma 3.13, mit $H/A \cong H_0$, eine r'-Gruppe.

Nach Satz 3.9 sind Elemente der Ordnung r aus $V(\mathbb{Z}G)$ rational zu Gruppenelementen konjugiert. Mit den Lemmata 3.7 und 3.8 und man erhält das folgende allgemein gültige Lemma, das auch später in Kapitel 4 Verwendung findet:

Lemma 3.15. *Sei* $G = \mathsf{PSL}(2, p^f)$ *und* r *eine von* p *verschiedene, ungerade Primzahl. Weiter sei* $H \leqslant \mathsf{V}(\mathbb{Z}G)$ *eine endliche Untergruppe, deren Ordnung von* r *geteilt wird, und* N *ein* r'*-Normalteiler von* H*. Dann besitzt* H/N *mindestens soviele Konjugiertenklassen mit Elementen der Ordnung* r*, wie es solche Klassen in* G *gibt.*

3.3.4 $G = \mathsf{PSL}(2, 3^l)$

Die Ordnung von G ist $|G| = \frac{1}{2} \cdot 3^l \cdot (3^l - 1)(3^l + 1)$ mit $l \neq 2$ prim. Zunächst wird gezeigt, dass die Ordnung von G nicht von 5 geteilt wird, und dass 4 der maximale 2-Potenzteiler der Ordnung von G ist.

Behauptung 1: Es gilt $5 \nmid |G|$.

Beweis. Es ist

$$(3^l - 1)(3^l + 1) = 3^{2l} - 1 = 9^l - 1 \equiv -1 - 1 \equiv -2 \bmod 5$$

□

Behauptung 2: Es gilt $4 \,||\, |G|$.

Beweis. Es ist $l = 2n + 1$ für ein $n \in \mathbb{N}$. Dann ist

$$(3^l - 1)(3^l + 1) = 3^{4n+2} - 1 = 9 \cdot 81^n - 1 \equiv 9 - 1 \equiv 8 \bmod 16\,.$$

□

Ist H_0 eine Suzukigruppe oder $H_0 \cong \mathsf{PSL}(2, 4)$, dann wird die Ordnung von H_0 von 5 geteilt. Ist $H_0 \cong \mathsf{PSL}(3, 3)$ oder $H_0 \cong \mathsf{PSL}(2, 2^p)$, dann wird die Ordnung von H_0 von 8 geteilt. Beides steht nach Satz 2.1 im Widerspruch zu Behauptung 1, bzw. zu Behauptung 2.

Ist $H_0 \cong \mathsf{PSL}(2, 3^s)$ für eine Primzahl $s \neq 2$, dann folgt mit

$$\frac{1}{2} \cdot 3^s \cdot (3^{2s} - 1) = |H_0| \,\big|\, |G| = \frac{1}{2} \cdot 3^l (3^{2l} - 1)$$

aus Lemma 3.4, dass $2s \,\big|\, 2l$ gelten muss. Da s und l aber prim sind, folgt daraus $s = l$. Also ist $H_0 \cong G$ und H kein kleinster Verbrecher.

Es ist also $H_0 \cong \mathsf{PSL}(2, p)$ für eine ungerade Primzahl $p > 5$ mit $p^2 + 1 \equiv 0 \bmod 5$. Dann besitzt H_0 und damit H aber nur zwei Konjugiertenklassen mit Elementen der Ordnung p. In G gibt es aber $\frac{p-1}{2}$ solcher Konjugiertenklassen. Nach Lemma 3.15 ist das aber unmöglich.

3.3.5 $G = PSL(2, 2^p)$

Es gilt $|G| = 2^p \cdot (2^p - 1) \cdot (2^p + 1)$. Ist $p = 2$, dann ist $G \cong A_5$ und es gibt keinen kleinsten Verbrecher H. Ist $p > 2$, dann ist wegen

$$2^{2p} - 1 \equiv 4^p - 1 \equiv (-1)^p - 1 \equiv -2 \bmod 5$$

die Zahl 5 kein Teiler der Ordnung von G. In diesem Fall kann also H_0 keine Suzukigruppe sein. Auch $H_0 \cong PSL(3, 3)$ bzw. $PSL(2, 3^f)$ ist nach Satz 3.6 unmöglich, da $PSL(3, 3)$ bzw. $PSL(2, 3^f)$ im Gegensatz zu $PSL(2, 2^p)$ Gruppen der Form C_3^2 besitzen. Nach Lemma 3.4 scheidet auch $H_0 \cong PSL(2, 2^t)$ für eine Primzahl $t < p$ aus. Es verbleibt also der Fall $H_0 \cong PSL(2, r)$, mit r prim. Da G genau $\frac{r-1}{2}$ Konjugiertenklassen mit Elementen der Ordnung r besitzt, widerspricht dieser Fall Lemma 3.15.

3.3.6 $G = PSL(2, p)$

Der Beweis für $H_0 \ncong PSL(2, 2^{\overline{p}})$ verläuft analog zu den obigen Fällen. Wegen $p^2 \equiv -1 \bmod 5$ ist 5 kein Teiler von $|G|$, und damit ist $H_0 \ncong Sz(2^s)$ und $H_0 \ncong PSL(2, 4)$. Auch enthält G keine Untergruppe der Form C_3^2, weshalb $H_0 \ncong PSL(3, 3)$, bzw. $H_0 \ncong PSL(2, 3^r)$ ist. Ebenso scheidet $H_0 \cong PSL(2, \overline{p})$ nach Lemma 3.15 aus, da G mehr als zwei Konjugiertenklassen mit Elementen der Ordnung $\overline{p}$ enthält.

Es ist also $H_0 \cong PSL(2, 2^{\overline{p}})$ mit $\overline{p} \geqslant 3$. Sei S eine 2-Sylowgruppe von H, dann folgt nach Korollar 3.12, dass S, und damit auch jedes Bild von S, von zwei Elementen erzeugt wird. Die 2-Sylowgruppen von H_0 sind aber elementar-abelsch von Ordnung $\geqslant 8$ und damit von mindestens 3 Elementen erzeugt. Die Gruppe $PSL(2, 2^{\overline{p}})$ kann also nicht als Faktor von H auftreten.

□

In der Abbildung auf der nächsten Seite ist zusammenfassend schematisch dargestellt, mit welcher Methode ein jeweiliges H_0 im Beweis von Satz 3.3 als Sektion in $V(\mathbb{Z}G)$ ausgeschlossen wurde.

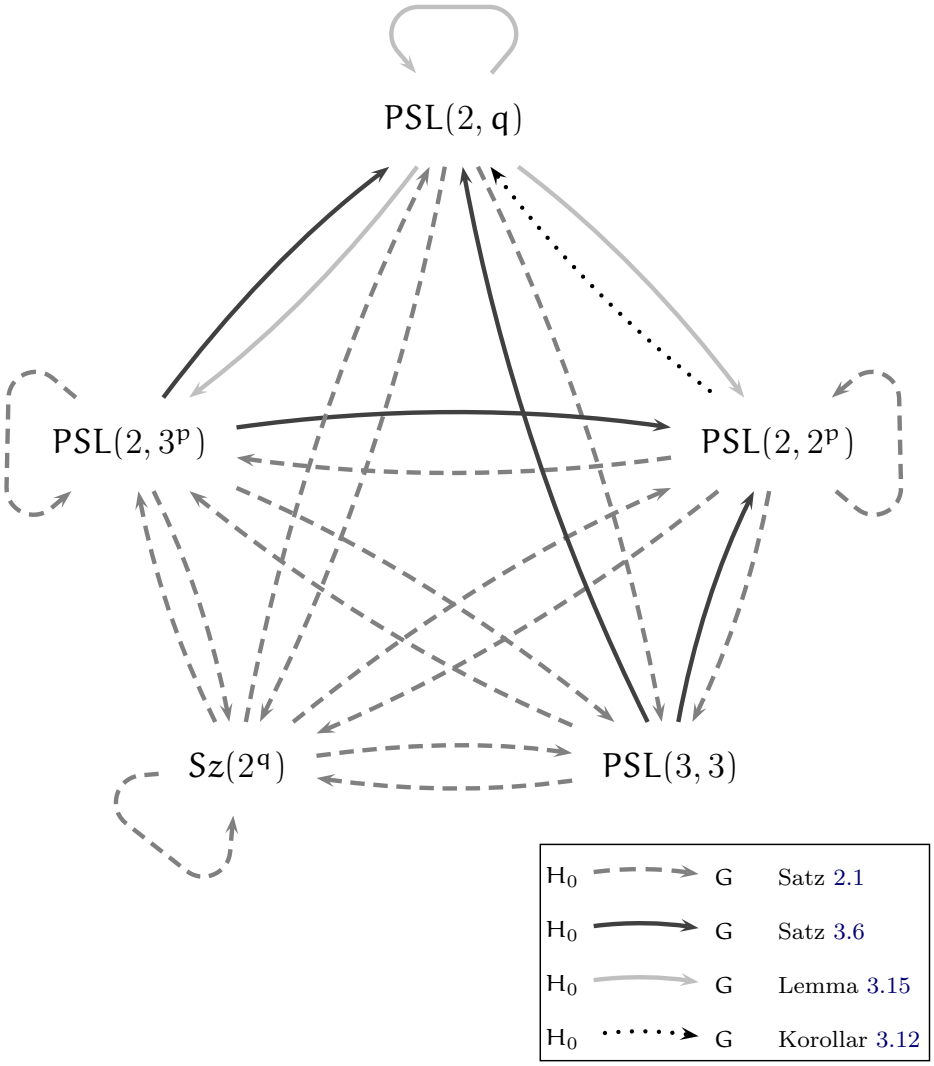


Abbildung 3.1: Übersicht zum Beweis von Satz 3.3

KAPITEL 4

Endliche Untergruppen in $\mathsf{V}(\mathbb{Z}\mathsf{PSL}(2,\mathsf{p}^\mathsf{f}))$

In diesem abschließenden Kapitel sollen die endlichen Untergruppen in den Einheiten des ganzzahligen Gruppenrings von $\mathsf{G} = \mathsf{PSL}(2,\mathsf{p}^\mathsf{f})$ näher untersucht werden. In Kapitel 3 wurde bereits gezeigt, dass jede endliche abelsche 2-Untergruppe von $\mathsf{V}(\mathbb{Z}\mathsf{G})$ isomorph zu einer Untergruppe von G ist (Proposition 3.11). Zunächst wird dieses Resultat auf beliebige endliche 2-Untergruppen verallgemeinert.

Sind die 2-Sylowgruppen von G elementar-abelsch und ist H eine endliche, nicht-auflösbare Untergruppe von $\mathsf{V}(\mathbb{Z}\mathsf{G})$, dann zeigt sich, dass H einen eindeutig bestimmten nicht-abelschen Kompositionsfaktor besitzt, der isomorph zu einer Untergruppe von G ist.

Letztlich wird für den Fall, dass G eine der Gruppen $\mathsf{PSL}(2,7), \mathsf{PSL}(2,11)$ oder $\mathsf{PSL}(2,13)$ ist, bewiesen, dass jede endliche Untergruppe in den Einheiten von $\mathbb{Z}\mathsf{G}$ isomorph zu einer Untergruppe von G ist. Im Fall $\mathsf{G} = \mathsf{PSL}(2,7)$ sind sogar sämtliche endlichen Untergruppen in $\mathsf{V}(\mathbb{Z}\mathsf{G})$ rational zu Untergruppen von G konjugiert, d.h. für $\mathsf{G} = \mathsf{PSL}(2,7)$ ist (ZC·3) wahr[1].

Bei den Beweisen geht das bekannte Wissen über Torsionseinheiten in $\mathsf{V}(\mathbb{Z}\mathsf{PSL}(2,\mathsf{p}^\mathsf{f}))$ (siehe Satz 3.9) wesentlich ein. Besonders bei der Betrachtung der drei „kleinen“ Gruppen ist entscheidend, dass die erste Zassenhausvermutung (ZC·1) wahr ist [27].

4.1 Der allgemeine Fall

Erstes Ziel ist die Verallgemeinerung von Proposition 3.11 auf beliebige endliche 2-Gruppen in $\mathsf{V}(\mathbb{Z}\mathsf{G})$. Dazu ist noch die Quaternionengruppe Q_8 der Ordnung 8 als Untergruppe von $\mathsf{V}(\mathbb{Z}\mathsf{G})$ auszuschließen. Die Idee dazu ist die aus [22, Example 7.], es müssen jedoch die reellen

[1] Die Ideen zu den Abschnitten 4.2 und 4.3 entsprangen Diskussionen mit Wolfgang Kimmerle.

Darstellungen von Q_8 betrachtet werden[2].

Proposition 4.1. *Ist* $G = PSL(2,p^f)$*, dann enthält* $V(\mathbb{Z}G)$ *keine Untergruppe isomorph zur Quaternionengruppe* Q_8 *der Ordnung 8.*

Beweis. Es ist

$$\mathbb{C}Q_8 = \mathbb{C}\oplus\mathbb{C}\oplus\mathbb{C}\oplus\mathbb{C}\oplus\mathbb{C}^{2\times 2} \quad\text{und}\quad \mathbb{R}Q_8 = \mathbb{R}\oplus\mathbb{R}\oplus\mathbb{R}\oplus\mathbb{R}\oplus\mathbb{H}\,.$$

Fasst man die vierdimensionale reelle Darstellung komplex auf, dann zerfällt sie in zwei irreduzible zweidimensionale Darstellungen. Insbesondere tritt also die zweidimensionale irreduzible gewöhnliche Darstellung in komplex aufgefassten reellen Darstellungen von Q_8 immer paarweise auf. Es sei $\psi \in \mathrm{Irr}(Q_8)$ der Charakter der irreduziblen gewöhnlichen zweidimensionalen Darstellung.

Angenommen, in $V(\mathbb{Z}G)$ gibt es eine zu Q_8 isomorphe Untergruppe H. Die irreduziblen Charaktere von G kann man als Charaktere von H auffassen. Wie in Kapitel 3 wähle man (mit den Bezeichnungen aus den Tabellen A.1 und A.2) $\chi = \delta_2$ im Fall $p^f \equiv 1 \bmod 4$ und $\chi = \theta_2$ im Fall $p^f \equiv -1 \bmod 4$. In Kapitel 3 wurde dann bereits gezeigt, dass für eine Involution ι gilt $\chi(\iota) = 2\alpha$ mit $\alpha = -1$ für $p^f \equiv 1 \bmod 4$ und $\alpha = 1$ für $p^f \equiv -1 \bmod 4$. Es ist dann

$$\begin{aligned}\langle \chi|_H, \psi\rangle &= \tfrac{1}{8}\left(\chi|_H(1)\psi(1) + \chi|_H(\iota)\psi(\iota)\right) = \tfrac{1}{8}\left((p^f-\alpha)\cdot 2 + 2\alpha\cdot(-2)\right)\\ &= \tfrac{1}{8}\left(2p^f - 6\alpha\right) = \tfrac{1}{4}\left(p^f - 3\alpha\right) = \tfrac{1}{4}\left(p^f+\alpha\right) - \alpha\,.\end{aligned}$$

Nach Voraussetzung gilt $8 \,\big|\, (p^f+\alpha)$. Insbesondere ist also der linke Teil der letzten Summe gerade und der Wert $\langle \chi|_H, \psi\rangle$ somit stets ungerade.

Es genügt also zu zeigen, dass die zu χ, und damit auch die zu $\chi|_H$, gehörende Darstellung reell realisierbar ist. Dies ist genau dann der Fall, wenn der Frobenius-Schur-Indikator von χ gleich 1 ist (s. z.B. [33, XI, Theorem 8.3]). Der Frobenius-Schur-Indikator von χ ist

$$c := \frac{1}{|G|}\sum_{x\in G}\chi(x^2)\,.$$

Es müssen also die Charakterwerte $\chi(x^2)$ bestimmt werden.

Für Involutionen und Elemente der Ordnung p ist dies trivial. Es ist ebenfalls trivial für ein Element $x \neq 1$, dessen Ordnung $\frac{p^f-\alpha}{2}$ teilt: Für x verschwindet der Wert $\chi(x)$ und damit ist auch $\chi(x^2) = 0$, da $\frac{p^f-\alpha}{2}$ ungerade ist.

Es sei nun also x ein Element der Ordnung $\frac{p^f+\alpha}{2n}$ mit $1 \leqslant n \leqslant \frac{p^f+\alpha}{4} - 1$. Dann ist $\chi(x) = -\alpha\rho^{2n} - \alpha\rho^{-2n}$ und damit $\chi(x^2) = -\alpha\rho^{4n} - \alpha\rho^{-4n}$. Setzt man $\lambda := \rho^4$, dann ist λ eine primitive $\frac{p^f+\alpha}{4}$-te Einheitswurzel. Der Zentralisator von x ist zyklisch von Ordnung

[2] Die entscheidende Idee zum Beweis - die Verwendung reeller Darstellungen - erhielt ich von Martin Hertweck. Ich möchte ihm dafür herzlich danken.

$\frac{p^f+\alpha}{2}$, unabhängig von n. Damit ist auch die Länge der Konjugiertenklasse von x unabhängig von n.

Der Anteil, den all solche Elemente zum Frobenius-Schur-Indikator liefern, ist also

$$\frac{|G|}{|C_G(x)|}\sum_{n=1}^{\frac{p^f+\alpha}{4}-1}(-\alpha\lambda^n-\alpha\lambda^{-n}) = -\alpha p^f(p^f-\alpha)\Big(\underbrace{\sum_{n=1}^{\frac{p^f+\alpha}{4}-1}\lambda^n}_{=-1}+\underbrace{\sum_{n=1}^{\frac{p^f+\alpha}{4}-1}\lambda^{-n}}_{=-1}\Big) = 2\alpha p^f(p^f-\alpha)\,.$$

Insgesamt ergibt sich daher für den Frobenius-Schur-Indikator von χ:

$$\begin{aligned}
c &= \tfrac{1}{|G|}\sum_{x\in G}\chi(x^2)\\
&= \tfrac{1}{|G|}\left(\sum_{o(x)=1}\chi(x^2)+\sum_{o(x)=2}\chi(x^2)+\sum_{o(x)=p}\chi(x^2)+\sum_{o(x)\,\mid\,\frac{p^f+\alpha}{4}}\chi(x^2)\right)\\
&= \tfrac{1}{|G|}\Big((p^f-\alpha)+\tfrac{\frac{1}{2}p^f(p^f+1)(p^f-1)}{p^f+\alpha}(p^f-\alpha)+2\cdot\tfrac{\frac{1}{2}p^f(p^f+1)(p^f-1)}{p^f}\cdot(-\alpha)+2\alpha p^f(p^f-\alpha)\Big)\\
&= \tfrac{1}{|G|}\left((p^f-\alpha)+\tfrac{1}{2}p^f(p^f-\alpha)(p^f-\alpha)-\alpha(p^f+1)(p^f-1)+2\alpha p^f(p^f-\alpha)\right)\\
&= \tfrac{2}{p^f(p^f+\alpha)}\left(1+\tfrac{1}{2}p^f(p^f-\alpha)-\alpha(p^f+\alpha)+2\alpha p^f\right)\\
&= \tfrac{2}{p^f(p^f+\alpha)}\left(1+\tfrac{1}{2}p^{2f}-\tfrac{1}{2}\alpha p^f-\alpha p^f-\alpha^2+2\alpha p^f\right)\\
&= \tfrac{2}{p^f(p^f+\alpha)}\left(\tfrac{1}{2}p^{2f}+\tfrac{1}{2}\alpha p^f)\right)\\
&= 1\,.
\end{aligned}$$

□

Damit kann die folgende Proposition bewiesen werden.

Proposition 4.2. *Ist* $G = PSL(2,p^f)$*, dann ist jede endliche 2-Gruppe* $H \leqslant V(\mathbb{Z}G)$ *isomorph zu einer Untergruppe von* G*.*

Beweis. Für $p = 2$ ist die Behauptung nach Satz 2.2 trivial. Für abelsche Untergruppen wurde die Behauptung bereits in Proposition 3.11 gezeigt. Nach dem Satz von Dickson (s. Abschnitt 3.2.4) bleibt also zu zeigen, dass jede nicht-abelsche 2-Untergruppe H von $V(\mathbb{Z}G)$ eine Diedergruppe ist. Für $|H| = 8$ folgt die Behauptung unmittelbar aus Proposition 3.11 und Proposition 4.1. Es kann also $|H| = 2^{n+1}$ mit $n \geqslant 3$ angenommen werden. Nach Korollar 3.12 enthält H einen zyklischen Normalteiler vom Index 2. Nach [32, I, 14.9 b)] ist H dann isomorph zu einer der folgenden Gruppen:

(1) Diedergruppe D_{2^n}

(2) Verallgemeinerte Quaternionengruppe $Q_{2^{n+1}}$

$$Q_{2^{n+1}} = \langle a, b \mid a^{2^n} = 1, b^2 = a^{2^{n-1}}, a^b = a^{-1} \rangle$$

(3) $S = \langle a, b \rangle$ mit

$$S = \langle a, b \mid a^{2^n} = b^2 = 1, a^b = a^{1+2^{n-1}} \rangle$$

(4) Quasidiedergruppe $\overline{D}_{2^n}$

$$\overline{D}_{2^n} = \langle a, b \mid a^{2^n} = b^2 = 1, a^b = a^{-1+2^{n-1}} \rangle .$$

Für $n = 2$ liefert (2) die Quaternionengruppe

$$Q = Q_8 = \langle q, r \mid q^4 = 1, r^2 = q^2, q^r = q^{-1} \rangle$$

der Ordnung 8, und via

$$\iota_2 : Q \longrightarrow Q_{2^{n+1}} ; \begin{cases} q & \mapsto & a^{2^{n-2}} \\ r & \mapsto & b \end{cases}$$

ist Q eine Untergruppe von $Q_{2^{n+1}}$. Es gelten nämlich die Relationen

$$q^4 = a^{4 \cdot 2^{n-2}} = a^{2^n} = 1 ,$$
$$q^r = \left(a^{2^{n-2}}\right)^r = \left(a^{2^{n-2}}\right)^b = \left(a^b\right)^{2^{n-2}} = (a^{-1})^{2^{n-2}} = \left(a^{2^{n-2}}\right)^{-1} = q^{-1} \quad \text{und}$$
$$r^2 = b^2 = a^{2^{n-1}} = a^{2 \cdot 2^{n-2}} = q^2 .$$

Auch die Gruppen in (4) enthalten via

$$\iota_4 : Q \longrightarrow \overline{D}_{2^{n+1}} ; \begin{cases} q & \mapsto & a^{2^{n-2}} \\ r & \mapsto & ab \end{cases}$$

eine zu Q isomorphe Untergruppe, denn es gilt

$$q^4 = a^{4 \cdot 2^{n-2}} = a^{2^n} = 1 ,$$
$$q^r = \left(a^{2^{n-2}}\right)^{ab} = \left(a^{2^{n-2}}\right)^b = a^{2^{n-2}(-1+2^{n-1})} = a^{-2^{n-2}} \underbrace{a^{2^{2n-3}}}_{=1 \ ;(n \geqslant 3)} = q^{-1} \quad \text{und}$$
$$r^2 = (ab)^2 = a \cdot a^b = a \cdot a^{-1+2^{n-1}} = a^{2^{n-1}} = a^{2 \cdot 2^{n-2}} = q^2 .$$

Da es in $V(\mathbb{Z}G)$ nach Proposition 4.1 keine Quaternionengruppe gibt, können die Gruppen aus (2) und (4) nicht als Untergruppen von $V(\mathbb{Z}G)$ auftauchen. Auch die Gruppen in (3) sind

keine Untergruppen von $V(\mathbb{Z}G)$, denn jede dieser Gruppen enthält eine Untergruppe isomorph zu $C_4 \times C_2$: Ist nämlich $C_4 \times C_2 = \langle s \rangle \times \langle t \rangle$, dann ist

$$\iota_3 : C_4 \times C_2 \longrightarrow S ; \begin{cases} s & \mapsto & a^{2^{n-2}} \\ t & \mapsto & b \end{cases}$$

ein injektiver Gruppenhomomorphismus, denn es gilt (für $n \geqslant 3$)

$$\begin{gathered} s^4 = a^{4 \cdot 2^{n-2}} = a^{2^n} = 1 , \\ s^t = (a^{2^{n-2}})^b = a^{2^{n-2}(1+2^{n-1})} = a^{2^{n-2}} \underbrace{a^{2^{2n-3}}}_{=1} = s \quad \text{und} \\ r^2 = b^2 = 1 . \end{gathered}$$

Damit können die Gruppen in (3) nach Proposition 3.11 ebenfalls nicht als Untergruppen von $V(\mathbb{Z}G)$ vorkommen und es folgt die Behauptung. □

Proposition 4.3. *Ist* $G = PSL(2, p^f)$ *mit* $p = 2$ *oder* $p^f \equiv 3, 5$ *mod* 8 *und ist* $H \leqslant V(\mathbb{Z}G)$ *eine endliche nicht-auflösbare Gruppe, dann besitzt* H *einen eindeutig bestimmten nicht-abelschen Kompositionsfaktor* X *mit Multiplizität 1, und* X *ist zu einer Untergruppe von* G *isomorph.*

Beweis. Für jedes $r \in \pi(H)$ sei $N_r = O_{r'}(H)$ gesetzt, und es sei $N_r \leqslant M_r \leqslant H$ mit $O^{r'}(H/N_r) = M_r/N_r$.

Die 2-Sylowgruppen von G, und nach Proposition 4.2 damit auch die von H, sind elementar-abelsch: Für $p = 2$ ist dies trivial. Auch für $p^f \equiv 3, 5 \bmod 8$ folgt das unmittelbar, da die Ordnung von G in diesem Fall nicht von 8 geteilt wird. Nach Satz 3.14 ist dann $M_2/N_2 = A_2 \times X_1 \times \ldots \times X_k$, wobei A_2 eine elementar-abelsche 2-Gruppe sein muss, und die Gruppen X_i nicht-abelsche einfache Gruppen sind. Jedes der X_i ist isomorph zu einer der folgenden Gruppen:

(a) $PSL(2, 2^{\bar{f}})$.

(b) $PSL(2, \bar{q})$ mit $\bar{q} \equiv 3, 5 \bmod 8$.

(c) J_1.

(d) Eine Ree-Gruppe ${}^2G_2(\bar{q})$.

- Sei zunächst $p = 2$.

  Die Ordnung von jedem X_i wird von 3 geteilt. Insbesondere besitzt H/N_2 also eine zu C_3^k isomorphe Untergruppe. Da die 3-Sylowgruppen von G zyklisch sind, muss dies auch für die 3-Sylowgruppen von H gelten. Es folgt also $k = 1$, d.h. H besitzt einen eindeutig bestimmten nicht-abelschen Kompositionsfaktor $X = X_1$ mit Multiplizität 1.

  Sei nun $r \in \pi(X) \setminus \{2\}$. Die r-Sylowgruppen von G und H sind zyklisch und nach Satz 3.14 ist $M_r/N_r = X$. Insbesondere folgt für alle $r \in \pi(X) \setminus \{2\}$, dass $r \nmid \frac{|H|}{|X|}$ gilt. Die Gruppe

N_2 ist also eine $(\pi(H) \setminus \pi(X))$-Gruppe und nach dem Satz von Schur-Zassenhaus gilt $M_2 = N_2 \rtimes (A_2 \times X)$. Insbesondere gibt es in H, und damit in $V(\mathbb{Z}G)$ eine zu X isomorphe Untergruppe.

Ist $X = PSL(2, 2^{\bar{f}})$, dann muss

$$2^{\bar{f}}(2^{2\bar{f}} - 1) = |X| \;\Big|\; |G| = 2^f(2^{2f} - 1) \implies 2\bar{f} \,\big|\, 2f \implies \bar{f} \,\big|\, f$$

gelten. Nach dem Satz von Dickson besitzt G dann eine zu X isomorphe Untergruppe.

Ist $X = PSL(2, \bar{q})$ mit ungeradem $\bar{q} = \bar{p}^{\bar{f}}$, dann gibt es in X nur zwei Konjugiertenklassen mit Elementen der Ordnung $\bar{p}$. Jedes Element der Ordnung $\bar{p}$ aus $V(\mathbb{Z}G)$ ist aber nach Satz 3.9 rational zu einem Element aus G konjugiert. Da es in G jedoch $\frac{\bar{p}-1}{2}$ solcher Konjugiertenklassen gibt, folgt aus Lemma 3.15, dass $\bar{p} \in \{3, 5\}$ sein muss. Ist $\bar{p} = 3$, dann ist $\bar{f} \geqslant 2$, und X besitzt, im Widerspruch zu Satz 3.6 eine Untergruppe C_3^2. Es ist also $\bar{p} = 5$. Wiederum nach Satz 3.6 muss $\bar{f} = 1$ gelten. Es ist also $X = PSL(2, 5) \cong A_5$ isomorph zu einer Untergruppe von G.

Ist $X = J_1$, dann sind in X alle Elemente der Ordnung 7 konjugiert. Dies widerspricht aber Lemma 3.15.

Ist $X = {}^2G_2(\bar{q})$ mit $\bar{q} = 3^{2n+1}$ eine Ree-Gruppe, dann gibt es in X, im Widerspruch zu Satz 3.6, Gruppen isomorph zu C_3^2.

- Sei nun $p \neq 2$.

  Dann sind die 2-Sylowgruppen von H isomorph zu Untergruppen der Kleinschen Vierergruppe V_4. Die Sylowgruppen eines jeden möglichen X_i besitzen mindestens 4 Elemente. Aus Ordnungsgründen folgt also unmittelbar $k = 1$, sowie $A = 1$. Die 2-Sylowgruppen von J_1, bzw. der Ree-Gruppen haben sogar mindestens 8 Elemente. Diese Gruppen scheiden also als $X = X_1$ aus. Ebenso sind die Gruppen $X = PSL(2, 2^{\bar{f}})$ mit $f \geqslant 3$ unmöglich. Es verbleiben für X die Möglichkeiten $X = PSL(2, 2^2)$ und $X = PSL(2, \bar{p}^{\bar{f}})$ mit $\bar{p}^{\bar{f}} \equiv 3, 5 \bmod 8$.

  Ist $X = PSL(2, 2^2)$, dann wird die Ordnung von G von 5 geteilt und G besitzt eine zu X isomorphe Untergruppe. O.B.d.A sei also $X = PSL(2, \bar{p}^{\bar{f}})$ mit $\bar{p} \neq 2$.

  Ist $\bar{p} = p$, dann folgt wie im Fall $p = 2$, dass f von $\bar{f}$ geteilt wird. G besitzt also eine zu X isomorphe Untergruppe. Ist $\bar{p} \neq p$, dann sind die $\bar{p}$-Sylowgruppen von H zyklisch. Da die $\bar{p}$-Sylowgruppen von $X = PSL(2, \bar{p}^{\bar{f}})$ elementar-abelsch sind ist $\bar{f} = 1$ und $M_{\bar{p}}/N_{\bar{p}}$ ist isomorph zu $X = PSL(2, \bar{p})$. Da in $V(\mathbb{Z}G)$ Elemente der Ordnung $\bar{p}$ rational zu Elementen von G konjugiert sind, erfüllen $M_{\bar{p}}$ und $N_{\bar{p}}$ die Voraussetzungen von Lemma 3.15 und X muss mindestens soviele Konjugiertenklassen mit Elementen der Ordnung $\bar{p}$ besitzen wie G. In G gibt es $\frac{\bar{p}-1}{2}$, in X genau zwei solcher Klassen. Es folgt $\bar{p} = 3$ oder $\bar{p} = 5$. Ist $\bar{p} = 3$, dann ist X auflösbar. Der Fall $\bar{p} = 5$ entspricht obigem Fall $X = PSL(2, 2)$.

□

Falls $G = PSL(2,p)$ kann auch für eine andere Klasse von Untergruppen von $V(\mathbb{Z}G)$ die Isomorphie zu Untergruppen von G gezeigt werden:

Proposition 4.4. *Sei* $G = PSL(2,p)$ *und* $H \leqslant V(\mathbb{Z}G)$ *eine endliche Gruppe. Teilt* p *die Ordnung von* H*, dann ist* H *isomorph zu einer Untergruppe von* G*.*

Beweis. Ist $p = 2$ bzw. $p = 3$, dann ist $G = PSL(2,2) \cong S_3$, bzw. $G = PSL(2,3) \cong A_4$. In beiden Fällen kennt man die Struktur von $V(\mathbb{Z}G)$ ([31], [2]) und weiß insbesondere, dass (ZC-3) für G wahr ist. Die Gruppe H ist also sogar rational zu einer Untergruppe von G konjugiert.

Sei also $p \geqslant 5$. Wegen $|G| = \frac{1}{2}p(p^2-1)$ ist $p \,\|\, |H|$. Für G gilt nach Satz 3.9 $\Gamma(G) = \Gamma(V(\mathbb{Z}G))$, die Ecke p ist also in $\Gamma(V(\mathbb{Z}G))$ isoliert.

Falls H einen zu C_p isomorphen minimalen Normalteiler N besitzt, hat H die Form $H \cong C_p \rtimes X$. Ist $X = 1$, dann ist H trivialerweise zu einer Untergruppe von G isomorph. Ist $X \neq 1$, dann muss die Operation treu sein, da sonst p in $\Gamma(V(\mathbb{Z}G))$ nicht isoliert ist. Es existiert also ein injektiver Gruppenhomomorphismus $\varphi : X \longrightarrow \mathrm{Aut}(C_p) \cong C_{p-1}$ und H ist isomorph zu einer Untergruppe von $C_p \rtimes C_{p-1}$.

Ist H isomorph zu einer Untergruppe von $C_p \rtimes C_{\frac{p-1}{2}}$, dann ist H nach Dickson (Abschnitt 3.2.4) isomorph zu einer Untergruppe von G. Die Gruppe $X \leqslant C_{p-1}$ sei also nicht zu einer Untergruppe von $C_{\frac{p-1}{2}}$ isomorph, d.h. $|X| \nmid \frac{p-1}{2}$. Weiter sei $2^a \,\|\, \exp(G)$ und $2^b \,\|\, \exp(X)$. Gilt $2^a \mid \frac{p-1}{2}$, dann folgt $b = a+1$. Dies widerspricht aber Satz 2.2. Gilt $2^a \mid \frac{p+1}{2}$, dann ist $\frac{p-1}{2}$ ungerade. Ist $|X| \neq 2$, dann gibt es in $\pi(X)$ eine ungerade Primzahl r, die in $\Gamma(X)$ mit der Ecke 2 verbunden ist. Das ist aber unmöglich. Also ist $|X| = 2$ und H ist eine Diedergruppe. Insbesondere ist H zu einer Untergruppe von G isomorph.

Gibt es in H keinen zu C_p isomorphen minimalen Normalteiler, dann gibt es in H ein Element x der Ordnung p und einen minimalen Normalteiler N, der isomorph zu C_r mit r prim oder isomorph zu $C_2 \times C_2$ oder nicht-auflösbar ist. Ist N nicht-auflösbar, dann sind die 2-Sylowgruppen von N nach Proposition 4.2 elementar-abelsch oder Diedergruppen. Nach [20] und [58] ist N dann einfach und isomorph zu $PSL(2,2^f)$, $PSL(2,\bar{p}^{\bar{f}})$, J_1, ${}^2G_2(\bar{q})$ oder A_7 . Da es in G keine elementar-abelsche Gruppe der Ordnung 8 gibt, scheiden die Fälle J_1, ${}^2G_2(\bar{q})$, sowie $PSL(2,2^f)$ mit $f \geqslant 3$ aus. Für $f = 1$ ist $PSL(2,2^f)$ auflösbar. Es verbleibt also der Fall $f = 2$, d.h. $N \cong PSL(2,2^2) \cong A_5$.

Ist $N \cong PSL(2,\bar{p}^{\bar{f}})$ dann folgt aus Satz 3.6 $\bar{f} = 1$. Aus Lemma 3.15 folgt analog zum Beweis von Proposition 4.3, dass $\bar{p} = 5$ sein muss. Auch hier ist also $N \cong A_5$.

Ist $N \cong A_7$, dann gibt es in N zwei Konjugiertenklassen mit Elementen der Ordnung 7. Aus Lemma 3.15 folgt dann $G = PSL(2,7)$. Dann ist aber $|N| > |G|$, was nach Satz 2.1 unmöglich ist.

Insgesamt müssen also für N die folgenden Fälle untersucht werden:

- Ist $N \cong C_r$ mit einer Primzahl r, dann gibt es in H eine Untergruppe der Form $N \rtimes \langle x \rangle$. Da p in $\Gamma(V(\mathbb{Z}G))$ isoliert ist, muss es einen injektiven Gruppenhomomorphismus

$\varphi : \langle x\rangle \longrightarrow \mathrm{Aut}(C_r) \cong C_{r-1}$ geben. Es ist also $r-1 \geqslant p \geqslant 5$, und damit $r \geqslant 7$. Die nicht-triviale Operation von x auf C_r liefert in $C_r \rtimes \langle x\rangle$ genau $\frac{r-1}{p}$ Konjugiertenklassen mit Elementen der Ordnung r. In G gibt es aber $\frac{r-1}{2}$ solcher Klassen, im Widerspruch zu Lemma 3.15.

- Ist $N \cong C_2 \times C_2$, dann muss es mit denselben Argumenten wie oben einen injektiven Homomorphismus von C_p nach $\mathrm{Aut}(C_2 \times C_2) \cong S_3$ geben. Wegen $p \geqslant 5$ ist das aber unmöglich.
- Sei also $N \cong A_5$. Es ist $\mathrm{Aut}(A_5) \cong S_5$. Ein injektiver Gruppenhomomorphismus von C_p nach S_5 erfordert $p \in \{2,3,5\}$. Wie bereits oben erwähnt, ist für die Gruppen $\mathsf{PSL}(2,2) \cong S_3$ und $\mathsf{PSL}(2,3) \cong A_4$ die dritte Zassenhausvermutung wahr. Auch für die Gruppe $\mathsf{PSL}(2,5) \cong A_5$ ist das der Fall [15, Theorem 3.2]. In jedem Fall ist also H isomorph zu einer Untergruppe von G.

□

4.2 Endliche Untergruppen in $\mathsf{V}(\mathbb{Z}\mathsf{PSL}(2,7))$

In diesem Abschnitt sei $G = \mathsf{PSL}(2,7)$. Nach [26] gilt für G die erste Zassenhausvermutung. Die Charaktertafel von G ist durch

χ	1a	2a	3a	4a	7a	7b
χ^2	1a	2a	3a	4a	7a	7b
χ^3	1a	2a	3a	4a	7b	7a
1	1	1	1	1	1	1
ζ_1	3	-1	$\cdot$	1	$\frac{-1+\sqrt{-7}}{2}$	$\frac{-1-\sqrt{-7}}{2}$
ζ_2	3	-1	$\cdot$	1	$\frac{-1-\sqrt{-7}}{2}$	$\frac{-1+\sqrt{-7}}{2}$
θ	6	2	$\cdot$	$\cdot$	-1	-1
ψ	7	-1	1	-1	$\cdot$	$\cdot$
χ	8	$\cdot$	-1	$\cdot$	1	1

gegeben. Da (ZC-1) für G wahr ist, sind die Primgraphen von G und $\mathsf{V}(\mathbb{Z}G)$ identisch und haben die Gestalt

Ziel dieses Abschnitts ist der Beweis des folgenden Satzes:

Satz 4.5. *Ist* $G = \mathsf{PSL}(2,7)$*, dann ist jede endliche Untergruppe* $H \leqslant \mathsf{V}(\mathbb{Z}G)$ *rational zu einer Untergruppe von* G *konjugiert.*

Zunächst wird gezeigt:

Lemma 4.6. *Ist* $G = PSL(2,7)$ *und* $H \leqslant V(\mathbb{Z}G)$ *eine endliche Untergruppe, dann ist* H *isomorph zu einer Untergruppe* U *von* G.

Beweis. O.B.d.A. ist $|H| < |G|$. Da G minimal-einfach ist, ist H nach Proposition 3.3 auflösbar. Sei N ein minimaler Normalteiler von H. Der Beweis wird durch Unterscheidung der möglichen Fälle von $\pi(N)$ geführt. Da N ein minimaler Normalteiler ist, gilt sicherlich $|\pi(N)| = 1$.

- $\pi(N) = \{7\}$:

  Wegen $7 \,\|\, |G|$ ist N zyklisch von Ordnung 7. Es sei $N = \langle x \rangle$. Gilt $H = N$, dann ist die Aussage trivialerweise richtig. Es sei also $N < H$. Angenommen H enthalte ein Element ι der Ordnung 2. Da die Ecke 7 in $\Gamma(G)$ isoliert ist, G und damit auch H also keine Elemente der Ordnung 14 besitzt, muss $x^\iota = x^{-1}$ sein. Da für G die erste Zassenhausvermutung gilt, existiert ein $u \in V(\mathbb{Z}G)$ mit $x^u = g \in G$. In G ist das Element g der Ordnung 7 nicht zu seinem Inversen g^{-1} konjugiert. Es gibt also mindestens einen Charakter $\varphi \in \mathrm{Irr}(G)$ mit $\varphi(g) \neq \varphi(g^{-1})$. Damit erhält man aber den Widerspruch

  $$\varphi(x^{-1}) = \varphi(x^\iota) = \varphi(x) = \varphi(g) \neq \varphi(g^{-1}) = \varphi(x^{-1})\,.$$

  Die Gruppe H enthält demnach keine Involutionen und die Ordnung von H ist 21. Da 7 in $\Gamma(G)$ eine isolierte Ecke ist, muss $H \cong C_7 \rtimes C_3$ isomorph zur Frobeniusgruppe der Ordnung 21 sein. Diese kommt aber auch in G als Untergruppe vor.

- $\pi(N) = \{3\}$:

  Wegen $3 \,\|\, |G|$ ist N zyklisch von Ordnung 3. Da es in G keine Elemente der Ordnung $3r$ für $r > 1$ gibt, ist H entweder isomorph zu C_3 oder zu $C_3 \rtimes X$, wobei es einen injektiven Gruppenhomomorphismus von X nach $\mathrm{Aut}(C_3) \cong C_2$ geben muss. Es ist dann also $X \cong C_2$ und H in diesem Fall isomorph zu S_3. In G gibt es Untergruppen isomorph zu C_3 und S_3.

- $\pi(N) = \{2\}$:

  Wegen $8 \,\|\, |G|$ ist $N = C_2^i$ mit $i = 1, 2, 3$. Der Fall $i = 3$ scheidet nach Proposition 4.2 aus, da es in G keine elementar-abelsche Gruppe der Ordnung 8 gibt.

  Sei $N = C_2$. Angenommen in H gibt es ein Element x von ungerader Ordnung r. Es ist dann $N \rtimes \langle x \rangle \leqslant H$. Da jeder Automorphismus von N trivial ist, ist das Produkt direkt, und in H gibt es Elemente der Ordnung $2r$. Das ist aber nicht möglich, da die Ecke 2 in $\Gamma(G) = \Gamma(V(\mathbb{Z}G))$ isoliert ist. H ist also eine 2-Gruppe, und wiederum nach Proposition 4.2 isomorph zu einer Untergruppe von G.

  Sei $N = C_2^2$. Da N minimaler Normalteiler von H ist, also insbesondere $N \neq H$ ist, kann H keine 2-Gruppe sein. Es ist also $|H| \geqslant 12$. Wegen $\mathrm{Aut}(N) \cong S_3$ folgt $H \leqslant S_4$ und damit $H = A_4$ oder $H = S_4$. Beide Gruppen kommen in G als Untergruppen vor.

□

Der Beweis von Satz 4.5 beruht nun auf folgendem Lemma:

Lemma 4.7 ([54, Lemma 37.2]). *Sei* G *eine endliche Gruppe und* H *eine endliche Untergruppe von* $V(\mathbb{Z}G)$ *die via* φ *isomorph zu einer Untergruppe* U *von* G *ist. Ist* $\chi(h) = \chi(\varphi(h))$ *für alle* $h \in H$ *und alle* $\chi \in \mathrm{Irr}(G)$*, dann ist* $H \underset{\mathbb{Q}G}{\sim} U$.

Beweis von Satz 4.5. Da für G die zweite Zassenhausvermutung gilt ([8], [9, Theorem 1]), kann o.B.d.A. $|H| < |G|$ angenommen werden. Ist H nicht zur Frobeniusgruppe F_{21} der Ordnung 21 isomorph, dann sind die Voraussetzungen von Lemma 4.7 sicherlich erfüllt, und H ist damit rational zu einer Untergruppe von G konjugiert.

Es sei also $V(\mathbb{Z}G) \geqslant H \cong F_{21} \cong U \leqslant G$ oder $H \cong G$. Via φ sei ein Isomorphismus zwischen H und U gegeben. Ist $h \in H$ ein Element mit $o(h) \neq 7$, dann gilt $\chi(h) = \chi(\varphi(h))$ für alle $\chi \in \mathrm{Irr}(G)$, da es in G nur eine Konjugiertenklasse mit Elementen der Ordnung $o(h)$ gibt, und da h zu einem Element von G konjugiert ist. Es seien x_1 und x_2 Repräsentanten der beiden Konjugiertenklassen mit Elementen der Ordnung 7 von H, g_1 und g_2 seien Repräsentanten der beiden Klassen mit Elementen der Ordnung 7 in G. Da (ZC·1) für G wahr ist, gilt sicherlich o.B.d.A. $\chi(x_1) = \chi(g_1)$ und $\chi(x_2) = \chi(g_2)$ für alle $\chi \in \mathrm{Irr}(G)$. Ist $\chi(\varphi(x_1)) = \chi(x_1)$, dann greift Lemma 4.7. Ist $\chi(\varphi(x_1)) \neq \chi(x_1)$, dann muss $\chi(\varphi(x_1)) = \chi(x_2)$ gelten. In diesem Fall kann man aber den Isomorphismus φ durch $\varphi \circ \alpha$ ersetzen, wobei $\alpha \in \mathrm{Aut}(H)$ mit $\alpha(x_1) = x_2$ gewählt wird. Es gilt dann $\chi((\varphi \circ \alpha)(x_i)) = \chi(x_i)$ für $i = 1, 2$ und damit $\chi((\varphi \circ \alpha)(h)) = \chi(h)$ für alle $h \in H$. Lemma 4.7 schließt dann den Beweis ab. □

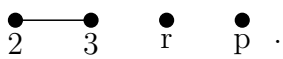
4.3 Endliche Untergruppen in $V(\mathbb{Z}PSL(2,11))$ und $V(\mathbb{Z}PSL(2,13))$

In diesem abschließenden Abschnitt wird gezeigt:

Proposition 4.8. *Ist* $G = PSL(2,11)$ *oder* $G = PSL(2,13)$*, dann ist jede endliche Untergruppe in* $V(\mathbb{Z}G)$ *isomorph zu einer Untergruppe von* G.

Beweis.

Für die Ordnung von G gilt $|G| = 2^2 \cdot 3 \cdot p \cdot r$, mit $(p,r) = (11,5)$ oder $(p,r) = (13,7)$. Aus Satz 3.9 (s. [27]) folgt, dass (ZC·1) für G wahr ist. Damit stimmen die Primgraphen von G und $V(\mathbb{Z}G)$ überein, haben also die Gestalt



Im Folgenden sei H eine Untergruppe von $V(\mathbb{Z}G)$ mit $|H| < |G|$. Für $p = 13$ ist G minimal-einfach und H daher nach Satz 3.3 auflösbar. Ist $p = 11$, dann folgt aus Proposition 4.3 für nicht-auflösbares H, dass H einen Kompositionsfaktor isomorph zu A_5 besitzt. Da $\frac{|G|}{|A_5|} = 11$ gilt, muss $H \cong A_5$ sein. Damit ist H isomorph zu einer Untergruppe von G.

O.B.d.A. sei also H auflösbar und M ein minimaler Normalteiler von H. Nach Proposition 4.4 kann angenommen werden, dass p die Ordnung von H nicht teilt.

- Sei $M \cong C_r$. Es gilt $r \,\|\, |G|$ und damit muss nach dem Satz von Schur-Zassenhaus $H \cong M \rtimes X$ sein, wobei X eine $\{2,3\}$-Gruppe ist. Da die Ecke r in $\Gamma(V(\mathbb{Z}G))$ isoliert ist, muss es einen injektiven Gruppenhomomorphismus φ von X nach $\mathrm{Aut}(C_r) \cong C_{r-1}$ geben.

  Für $p = 13$ ist $r - 1 = 6$ und damit $H \leqslant C_7 \rtimes C_6$. Teilt 3 die Ordnung von H, dann gibt es in $C_7 \rtimes C_3 \leqslant H$ nur zwei Konjugiertenklassen mit Elementen der Ordnung 7. Das steht im Widerspruch zu Lemma 3.15, da es drei solcher Klassen in G gibt. Es ist also $X \cong C_2$ oder $X = 1$. In beiden Fällen gibt es in G eine zu H isomorphe Untergruppe.

  Für $p = 11$ ist $r - 1 = 4$ und X damit trivial oder isomorph zu C_2. Auch hier gibt es dann stets eine zu H isomorphe Untergruppe in G.

- Sei $M \cong C_3$. Teilt r die Ordnung von H, dann muss es in H eine zu $C_3 \rtimes C_r$ isomorphe Untergruppe geben. Da r in $\Gamma(V(\mathbb{Z}G))$ isoliert ist, muss auch hier die Operation nichttrivial sein. Wegen $\mathrm{Aut}(C_3) \cong C_2$ ist das aber unmöglich.

  Also gilt $H \cong C_3 \rtimes X$ mit $X = 1$, $X \cong C_2$ oder $X \cong C_2 \times C_2$. In den ersten beiden Fällen besitzt G offensichtlich eine zu H isomorphe Untergruppe. Ist $X \cong C_2 \times C_2$, dann ist H isomorph zur abelschen Gruppe $C_3 \times C_2 \times C_2$ oder zur Diedergruppe $(C_3 \times C_2) \rtimes C_2$. Die Diedergruppe kommt auch als Untergruppe von G vor. Es bleibt also der Fall

  $$H = \langle a \rangle \times \langle b \rangle \times \langle c \rangle \cong C_3 \times C_2 \times C_2$$

  zu untersuchen.

  Es sei $\psi \in \mathrm{Irr}(H)$ der Charakter mit $\psi(a) = \zeta$, $\psi(b) = 1$ und $\psi(c) = -1$, wobei ζ eine primitive dritte Einheitswurzel ist. Weiter sei $\chi \in \mathrm{Irr}(G)$ ein Charakter vom Grad $\frac{p+\varepsilon}{2}$, mit $\varepsilon = -1$ für $p = 11$ und $\varepsilon = 1$ für $p = 13$. Da $(ZC{\cdot}1)$ für G wahr ist, gilt für $x \in H$

  $$\chi\big|_H(x) = \begin{cases} -\varepsilon & \text{, für } o(x) = 2 \\ \varepsilon & \text{, für } o(x) = 3 \\ -\varepsilon & \text{, für } o(x) = 6 \end{cases} .$$

  Fasst man χ als Charakter von H auf, so muss $\langle \chi\big|_H, \psi \rangle$ eine ganze Zahl $\geqslant 0$ sein. Es ist aber

  $$\begin{aligned} \langle \chi\big|_H, \psi \rangle &= \tfrac{1}{|H|} \left(\sum_{h \in H} \chi\big|_H(h) \cdot \psi(h^{-1}) \right) \\ &= \tfrac{1}{12} \left(\tfrac{p+\varepsilon}{2} - \varepsilon \sum_{o(h)=2} \psi(h) + \varepsilon \sum_{o(h)=3} \psi(h) - \varepsilon \sum_{o(h)=6} \psi(h) \right) \\ &= \tfrac{1}{12} \left(\tfrac{p+\varepsilon}{2} - \varepsilon(1-1-1) + \varepsilon(\zeta + \zeta^2) - \varepsilon(\zeta + \zeta^2 - \zeta - \zeta^2 - \zeta - \zeta^2) \right) \\ &= \tfrac{1}{12} \left(\tfrac{p+\varepsilon}{2} + \varepsilon - \varepsilon - \varepsilon \right) = \tfrac{p-\varepsilon}{24} = \tfrac{1}{2} . \end{aligned}$$

In $\mathsf{V}(\mathbb{Z}\mathsf{G})$ gibt es also keine zu $\mathsf{C}_3 \times \mathsf{C}_2 \times \mathsf{C}_2$ isomorphe Untergruppe.

- Ist $\mathsf{M} \cong \mathsf{C}_2$, dann muss H auch hier, mit den gleichen Argumenten wie oben, in jedem Fall eine $\{2,3\}$-Gruppe sein. Ist $|\mathsf{H}| \leqslant 6$, dann gibt es in G eine zu H isomorphe Untergruppe. Es kann also $|\mathsf{H}| = 12$ angenommen werden. Es gibt 5 verschiedene Isomporphieklassen von Gruppen der Ordnung 12. Davon besitzen nur die Diedergruppe D_6 und die Gruppe $\mathsf{C}_2 \times \mathsf{C}_2 \times \mathsf{C}_3$ einen minimalen Normalteiler isomorph zu C_2 und den Exponenten 6. Die Diedergruppe kommt als Untergruppe von G vor, die Gruppe $\mathsf{C}_2 \times \mathsf{C}_2 \times \mathsf{C}_3$ scheidet nach dem Vorherigen aus.
- Ist $\mathsf{M} \cong \mathsf{C}_2 \times \mathsf{C}_2$, dann ist H auch hier, wegen $\mathrm{Aut}(\mathsf{M}) \cong \mathsf{S}_3$, eine $\{2,3\}$-Gruppe. Insbesondere ist also $|\mathsf{H}| \leqslant 12$. O.B.d.A. ist $\mathsf{H} \neq \mathsf{M}$. Dann ist $|\mathsf{H}| = 12$ und H ist isomorph zu $\mathsf{M} \times \mathsf{C}_3$ oder $\mathsf{M} \rtimes \mathsf{C}_3 \cong \mathsf{A}_4$. Der Fall $\mathsf{H} \cong \mathsf{M} \times \mathsf{C}_3$ scheidet nach Obigem aus. H ist also isomorph zur alternierenden Gruppe A_4 und damit isomorph zu einer Untergruppe von G.

□

ANHANG A

Tabellen

Generische Charaktertafeln

Für die generischen Charaktertafeln der Gruppen $G = \mathsf{PSL}(2, p^f)$ im Fall $p^f \equiv 1 \bmod 4$ und $p^f \equiv 3 \bmod 4$ siehe z.B. [16, § 38]. Sie finden sich aber auch bereits in [51] und wurden implizit schon in [17] berechnet.

Im Folgenden sind $a, b \in \mathsf{PSL}(2, p^f)$ Elemente der Ordnung $o(a) = \frac{p^f-1}{2}$ und $o(b) = \frac{p^f+1}{2}$, abhängig von p^f mod 4. Die Involutionen in G werden demnach von $a^{\frac{p^f-1}{4}}$ bzw. $b^{\frac{p^f+1}{4}}$ repräsentiert. Die Charakterwerte dieser Klassen sind explizit angegeben.

In den Tafeln ist ρ eine $(p^f - 1)$-te primitive Einheitswurzel und σ eine primitive $(p^f + 1)$-te Einheitswurzel.

χ	1	p_1	p_2	a^l	a^d	b^m
1	1	1	1	1	1	1
ζ_1	$\frac{p^f+1}{2}$	$\frac{1+\sqrt{p^f}}{2}$	$\frac{1-\sqrt{p^f}}{2}$	$(-1)^l$	$(-1)^d$	0
ζ_2	$\frac{p^f+1}{2}$	$\frac{1-\sqrt{p^f}}{2}$	$\frac{1+\sqrt{p^f}}{2}$	$(-1)^l$	$(-1)^d$	0
θ_j	p^f-1	-1	-1	0	0	$-\sigma^{jm}-\sigma^{-jm}$
ψ	p^f	0	0	1	1	-1
δ_i	p^f+1	1	1	$\rho^{il}+\rho^{-il}$	$\rho^{id}+\rho^{-id}$	0

$$d = \tfrac{p^f-1}{4} \quad ; \quad o(a^d) = 2$$
$$i = 2,4,6,\ldots,\tfrac{p^f-5}{2} \quad ; \quad j = 2,4,6,\ldots,\tfrac{p^f-1}{2}$$
$$1 \leqslant l \leqslant \tfrac{p^f-5}{4} \quad ; \quad 1 \leqslant m \leqslant \tfrac{p^f-1}{4}$$

Tabelle A.1: Charaktertafel für $\mathsf{PSL}(2,p^f)$ mit $p^f \equiv 1 \bmod 4$

	1	p_1	p_2	a^l	b^m	b^e
1	1	1	1	1	1	1
ζ_1	$\frac{p^f-1}{2}$	$\frac{-1+\sqrt{-p^f}}{2}$	$\frac{-1-\sqrt{-p^f}}{2}$	0	$(-1)^{m+1}$	$(-1)^{e+1}$
ζ_2	$\frac{p^f-1}{2}$	$\frac{-1-\sqrt{-p^f}}{2}$	$\frac{-1+\sqrt{-p^f}}{2}$	0	$(-1)^{m+1}$	$(-1)^{e+1}$
θ_j	p^f-1	-1	-1	0	$-\sigma^{jm}-\sigma^{-jm}$	$-\sigma^{je}-\sigma^{-je}$
ψ	p^f	0	0	1	-1	-1
δ_i	p^f+1	1	1	$\rho^{il}+\rho^{-il}$	0	0

$$e = \tfrac{p^f+1}{4} \quad ; \quad o(b^e) = 2$$
$$i = 2,4,6,\ldots,\tfrac{p^f-3}{2} \quad ; \quad j = 2,4,6,\ldots,\tfrac{p^f-3}{2}$$
$$1 \leqslant l \leqslant \tfrac{p^f-3}{4} \quad ; \quad 1 \leqslant m \leqslant \tfrac{p^f-3}{4}$$

Tabelle A.2: Charaktertafel für $\mathsf{PSL}(2,p^f)$ mit $p^f \equiv -1 \bmod 4$

Primgraphkomponenten

G	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	|Out(G)|
J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3$	23	29	31	37	43	1
M_{22}	$2^7 \cdot 3^2$	5	7	11			2
J_1	$2^3 \cdot 3 \cdot 5$	7	11	19			1
O'N	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3$	11	19	31			2
Fi'_{24}	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13$	17	23	29			2
Ly	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11$	31	37	67			1
M	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 47$	41	59	71			1
M_{11}	$2^4 \cdot 3^2$	5	11				1
HS	$2^9 \cdot 3^2 \cdot 5^3$	7	11				2
Suz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7$	11	13				2
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7$	11	23				1
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7$	11	23				1
Co_2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7$	11	23				1
J_3	$2^7 \cdot 3^5 \cdot 5$	17	19				2
Fi_{23}	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	17	23				1
Th	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13$	19	31				1
B	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	31	47				1
J_2	$2^7 \cdot 3^3 \cdot 5^2$	7					2
M_{12}	$2^6 \cdot 3^3 \cdot 5$	11					2
McL	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7$	11					2
Fi_{22}	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11$	13					2
He	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3$	17					2
HN	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11$	19					2
Co_3	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11$	23					1
Co_1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13$	23					1
Ru	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13$	29					1

Tabelle A.3: Die Primgraphkomponenten der sporadisch-einfachen Gruppen
(erstellt aus Tabellen in [60] und [13])

G	Bedingungen	γ_1	γ_2	γ_3
$E_7(2)$		$2^{63} \cdot 3^{11} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17$ $\cdot 19 \cdot 31 \cdot 43$	73	127
$E_7(3)$		$2^{24} \cdot 3^{63} \cdot 5^2 \cdot 7^3 \cdot 11^2 \cdot 13^3 \cdot 19$ $\cdot 37 \cdot 41 \cdot 61 \cdot 73 \cdot 547$	757	1093
A_5		2^2	3	5
A_6		2^3	5	3^2
$A_2(2)$		2^3	3	7
${}^2A_5(2)$		$2^{15} \cdot 3^7 \cdot 5$	7	11
A_p	$p, q = p-2$ prim	$p!/(2pq)$	$q = p-2$	p
$A_1(q)$	$q \equiv 1 \bmod 4$	$(q-1)$	$(q+1)/2$	q
	$q \equiv -1 \bmod 4$	$(q+1)$	$(q-1)/2$	q
	$q \equiv 0 \bmod 2$	q	$q-1$	$q+1$
$G_2(q)$	$q = 3^m; m \geqslant 1$	$q^6(q-1)^2(q+1)^2$	q^2-q+1	q^2+q+1
${}^2G_2(q^2)$	$q^2 = 3^{2m+1}; m \geqslant 1$	$q^6(q^4-1)$	$q^2-\sqrt{3q^2}+1$	$q^2+\sqrt{3q^2}+1$
${}^2D_p(3)$	$p = 2^m+1$ prim; $m \geqslant 2$	$2 \cdot 3^{p(p-1)}(3^{p+1}-1)\prod_{i=1}^{p-2}(3^{2i}-1)$	$(3^{p-1}+1)/2$	$(3^p+1)/4$
${}^2D_{p+1}(2)$	$p = 2^m-1$ prim; $m \geqslant 2$	$2^{p(p+1)}(2^p-1)\prod_{i=1}^{p-1}(2^{2i}-1)$	2^p+1	$2^{p+1}+1$
$F_4(q)$	$q = 2^f; f \geqslant 2$	$q^{24}(q^6-1)^2(q^4-1)^2$	q^4-q^2+1	q^4+1
${}^2F_4(q)$	$q = 2^{2m+1}; m \geqslant 1$	$q^{12}(q^4-1)(q^3+1)(q^2+1)(q-1)$	$q^2-\sqrt{2q^3}+q-\sqrt{2q}+1$	$q^2+\sqrt{2q^3}+q+\sqrt{2q}+1$

Tabelle A.4: Die Primgraphkomponenten einfacher, nicht-sporadischer Gruppen G mit $|\Gamma(G)| = 3$
(erstellt aus Tabellen in [60], [43], [35] und [13])

G	Bedingungen	γ_1	γ_2	γ_3	γ_4
$A_2(4)$		2^6	5	7	3^2
${}^2E_6(2)$		$2^{36} \cdot 3^{10} \cdot 5^2 \cdot 7^2 \cdot 11$	13	17	19
${}^2B_2(q)$	$q = 2^{2m+1}; m \geqslant 1$	q^2	$q - \sqrt{2q} + 1$	$q - 1$	$q + \sqrt{2q} + 1$
$E_8(q)$	$q \equiv 2, 3 \bmod 5$	s.u.	$q^8 - q^7 + q^5 - q^4 + q^3 - q + 1$	$q^8 - q^4 + 1$	$q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$
		$\gamma_1 = q^{120}(q^8-1)(q^{10}-1)(q^{12}-1)(q^{14}-1)(q^{18}-1)(q^{20}-1)(q^{24}-1)(q^{30}-1)/(\gamma_2\gamma_3\gamma_4)$			
$E_8(q)$	$q \equiv 0, 1, 4 \bmod 5$	s.u.	$q^8 - q^7 + q^5 - q^4 + q^3 - q + 1$	$q^8 - q^6 + q^4 - q^2 + 1$	$q^8 - q^4 + 1$
		$\gamma_5 = q^8 + q^7 - q^5 - q^4 - q^3 + q + 1$			
		$\gamma_1 = q^{120}(q^8-1)(q^{10}-1)(q^{12}-1)(q^{14}-1)(q^{18}-1)(q^{20}-1)(q^{24}-1)(q^{30}-1)/(\gamma_2\gamma_3\gamma_4\gamma_5)$			

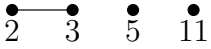
Tabelle A.5: Die Primgraphkomponenten einfacher, nicht-sporadischer Gruppen G mit $|\Gamma(G)| > 3$
(erstellt aus Tabellen in [60], [43], [35] und [13])

ANHANG B

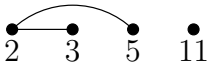
Primgraphen der sporadisch-einfachen Gruppen und ihrer Automorphismengruppe

Die Bezeichnungen der folgenden sporadisch-einfachen Gruppen sind nach dem „Atlas of Finite Group Representation“ [13] gewählt. Bei sporadisch-einfachen Gruppen G mit nicht-trivialer äußerer Automorphismengruppe bezeichnet $\mathsf{G}.2$ die volle Automorphismengruppe. In diesem Fall ist stets $|\mathrm{Out}(\mathsf{G})| = 2$.

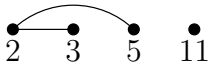
$\Gamma(\mathsf{M}_{11})$



$\Gamma(\mathsf{M}_{12})$

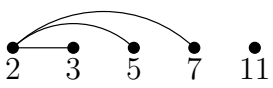


$\Gamma(\mathsf{M}_{12}.2)$

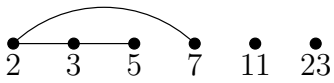


$\Gamma(\mathsf{M}_{22})$

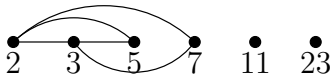
$\Gamma(\mathsf{M}_{22}.2)$



$\Gamma(M_{23})$

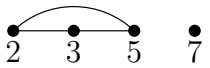


$\Gamma(M_{24})$

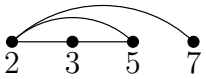


$\Gamma(J_1)$

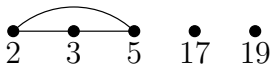
$\Gamma(J_2)$



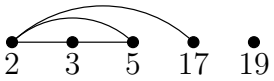
$\Gamma(J_2.2)$



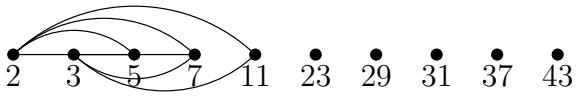
$\Gamma(J_3)$



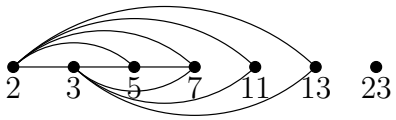
$\Gamma(J_3.2)$



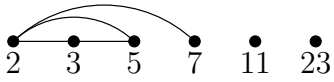
$\Gamma(J_4)$



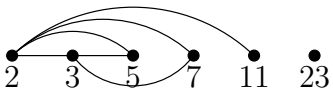
$\Gamma(Co_1)$



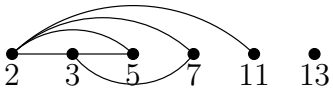
$\Gamma(Co_2)$



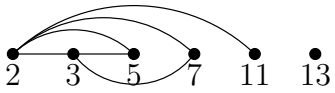
$\Gamma(\mathsf{Co}_3)$



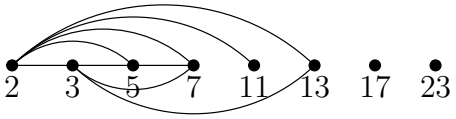
$\Gamma(\mathsf{Fi}_{22})$



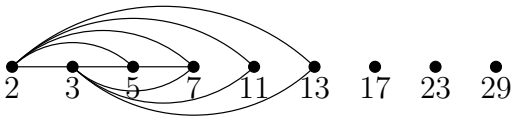
$\Gamma(\mathsf{Fi}_{22}.2)$



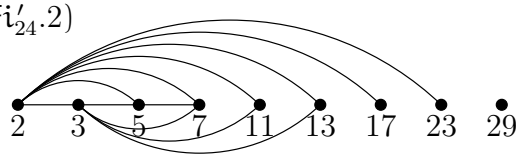
$\Gamma(\mathsf{Fi}_{23})$



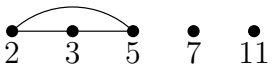
$\Gamma(\mathsf{Fi}'_{24})$



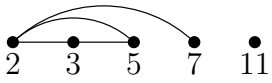
$\Gamma(\mathsf{Fi}'_{24}.2)$



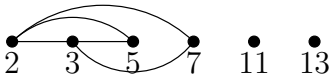
$\Gamma(\mathsf{HS})$



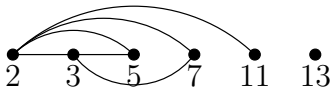
$\Gamma(\mathsf{HS}.2)$



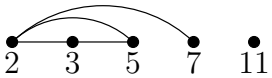
$\Gamma(\mathsf{Suz})$



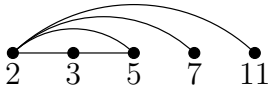
$\Gamma(\mathsf{Suz}.2)$



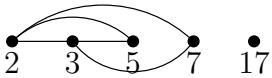
$\Gamma(\mathsf{McL})$



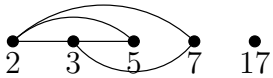
$\Gamma(\mathsf{McL}.2)$



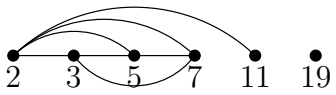
$\Gamma(\mathsf{He})$



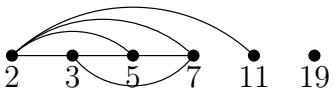
$\Gamma(\mathsf{He}.2)$



$\Gamma(HN)$

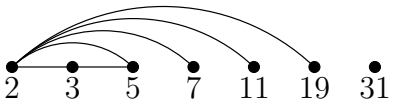


$\Gamma(HN.2)$

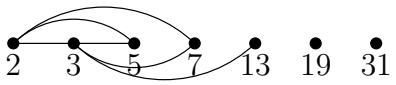


$\Gamma(O'N)$

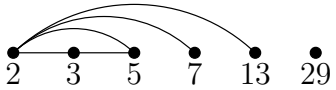
$\Gamma(O'N.2)$



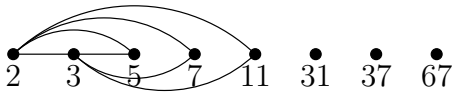
$\Gamma(Th)$



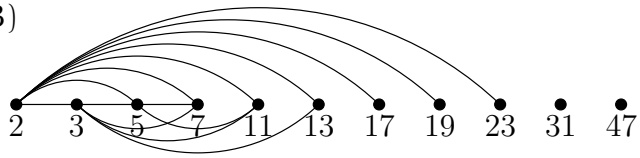
$\Gamma(Ru)$



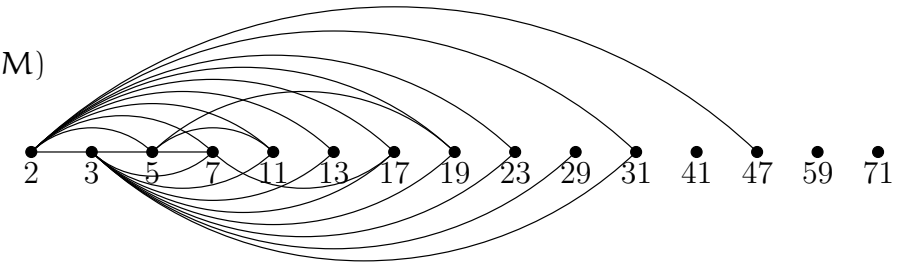
$\Gamma(Ly)$



$\Gamma(B)$



$\Gamma(M)$



Symbolverzeichnis

$\mathbb{N}$, $\mathbb{Z}$	die natürlichen und ganzen Zahlen
$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$	die komplexen, reellen und rationalen Zahlen
$\mathbb{H}$	der Quaternionenschiefkörper
C_n	die zyklische Gruppe der Ordnung n
D_n	die Diedergruppe der Ordnung $2n$
V_4	die Kleinsche Vierergruppe
E_n	die elementar-abelsche Gruppe der Ordnung n
Q_8	die Quaternionengruppe Gruppe der Ordnung 8
A_n	die alternierende Gruppe vom Grad n
S_n	die symmetrische Gruppe vom Grad n

G	eine (in der Regel) endliche Gruppe
$Z(G)$	das Zentrum von G
$C_G(X)$	der Zentralisator von X in G
$N_G(X)$	der Normalisator von X in G
$O_{p'}(G)$	der größte p'- Normalteiler von G
$O^{p'}(G)$	der kleinste Normalteiler von G, so dass $G/O^{p'}(G)$ eine p'-Gruppe ist
$\mathrm{Aut}(G)$	die Gruppe der Automorphismen von G
$\mathrm{Out}(G)$	die Gruppe der äußeren Automorphismen von G
$o(x)$	die Ordnung des Gruppenelementes x
$[x]$	die Konjugiertenklasse von x
x^g	die Konjugation $g^{-1}xg$
$ccl_G(n)$	die Menge der Konjugiertenklassen von G, die Elemente der Ordnung n enthalten
$\pi(n)$	die Menge aller Primteiler von n
$\pi(G)$	die Menge aller Primteiler von Elementordnungen in G
$\pi_e(G)$	das Spektrum von G
$\exp(G)$	der Exponent von G
$\Gamma(G)$	der Primgraph von G
$\lvert\Gamma(G)\rvert$	die Anzahl der Zusammenhangskomponenten von $\Gamma(G)$
$\Gamma_i(G)$	die i-te Zusammenhangskomponente von $\Gamma(G)$
$\Gamma_1(G)$	die Zusammenhangskomponente von $\Gamma(G)$, die 2 als Ecke enthält
$\pi_i(G)$	die Eckenmenge von $\Gamma_i(G)$
$\pi_i'(G)$	$\pi(G) \setminus \pi_i(G)$
$\pi'(G)$	$\{p \text{ prim } ;\ p \notin \pi(G)\}$

$n \mid m$	n teilt m
$n \parallel m$	n teilt m, und $\frac{m}{n}$ und n sind teilerfremd
$\gamma_i(G)$	das Produkt aller maximalen p-Potenzteiler von $\lvert G\rvert$ mit $p \in \pi_i(G)$
$\gamma_i'(G)$	$\frac{\lvert G\rvert}{\gamma_1(G)}$
$\gamma_o(G)$	das Maximum aller $\gamma_i(G)$ mit $i \geqslant 2$
$\gamma_u(G)$	das Minimum aller $\gamma_i(G)$ mit $i \geqslant 2$
$B(G)$	der Burnsidering von G
$MT(G)$	die Markentafel von G
X^K	die Fixpunkte der G-Menge X unter $K \leqslant G$
KG	der Gruppenring von G über dem Körper K
$\mathbb{Z}G$	der ganzzahlige Gruppenring von G
$V(\mathbb{Z}G)$	die Gruppe der normierten Einheiten von $\mathbb{Z}G$
$[\mathbb{Z}G, \mathbb{Z}G]$	der additive Kommutator von $\mathbb{Z}G$
$(ZC{\cdot}i)$	die i-te Zassenhausvermutung
$x \underset{\mathbb{Q}G}{\sim} y$	x ist via einer Einheit aus $\mathbb{Q}G$ zu y konjugiert
$\varepsilon_{[x]}(u)$	die partielle Augmentation von u bezüglich $[x]$
$\sigma_n(u)$	die Summe aller partiellen Augmentation von u bezüglich Konjugiertenklassen mit Elementen der Ordnung n
$\mathrm{Irr}(G)$	die gewöhnlichen irreduziblen Charaktere von G
$\chi\big\vert_H$	die Einschränkung des Charakters χ auf die Gruppe H
$\langle \cdot, \cdot \rangle$	das Standardskalarprodukt für gewöhnliche Charaktere

Literaturverzeichnis

[1] Akasaki, T. Idempotent ideals in integral group rings. *J. Algebra 23* (1972), 343–346.

[2] Allen, P. J. und Hobby, C. A characterization of units in $\mathbb{Z}\mathsf{A}_4$. *J. Algebra 66* (1980), 534–543.

[3] Bender, H. On groups with abelian Sylow 2-subgroups. *Math. Z. 117* (1970), 164–176.

[4] Berman, S. D. On the equation $\mathsf{X}^{\mathrm{m}} = 1$ in an integral group ring. *Ukr. Math Z. 7* (1955), 253–261.

[5] Blanchard, P. F. Exceptional group ring automorphisms for some metabelian groups. *Commun. Algebra 25*, 9 (1997), 2727–2733.

[6] Blanchard, P. F. Exceptional group ring automorphisms for some metabelian groups. II. *Commun. Algebra 25*, 9 (1997), 2735–2742.

[7] Blanchard, P. F. Exceptional group ring automorphisms for groups of order 96. *Commun. Algebra 29*, 11 (2001), 4823–4830.

[8] Bleher, F. Zassenhaus-Vermutung und einfache Gruppen. *Diplomarbeit, Universität Stuttgart* (1993).

[9] Bleher, F. M., Hiss, G. und Kimmerle, W. Autoequivalences of blocks and a conjecture of Zassenhaus. *J. Pure Appl. Algebra 103*, 1 (1995), 23–43.

[10] Bovdi, V., Höfert, C. und Kimmerle, W. On the first Zassenhaus conjecture for integral group rings. *Publ. Math. 65*, 3-4 (2004), 291–303.

[11] Chigira, N., Iiyori, N. und Yamaki, H. Nonabelian Sylow subgroups of finite groups of even order. *Electron. Res. Announc. Amer. Math. Soc. 4* (1998), 88–90 (electronic).

[12] Cohn, J. A. und Livingstone, D. On the structure of group algebras I. *Canad. J. Math. 17* (1965), 583–593.

[13] Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A. und Wilson, R. A. *Atlas of finite groups.* Oxford University Press, Eynsham, 1985.

[14] Dokuchaev, M. A. und Juriaans, S. O. Finite subgroups in integral group rings. *Can. J. Math. 48* (1996), 1170–1179.

[15] Dokuchaev, M. A., Juriaans, S. O. und Milies, C. P. Integral group rings of Frobenius groups and the conjecture of Zassenhaus. *Commun. Algebra 25* (1997), 2311–2325.

[16] Dornhoff, L. *Group representation theory (in 2 parts). Part A: Ordinary representation theory.* Pure and Applied Mathematics. 7. New York: Marcel Dekker, Inc. VII, 254 p., 1971.

[17] Frobenius, G. *Über Gruppencharaktere.* Berl. Ber., 985-1021, 1896.

[18] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.10*, 2007.

[19] Geck, M., Hiss, G., Lübeck, F., Malle, G. und Pfeiffer, G. CHEVIE – A system for computing and processing generic character tables for finite groups of Lie type, Weyl groups and Hecke algebras. *Appl. Algebra Engrg. Comm. Comput. 7* (1996), 175–210.

[20] Gorenstein, D. und Walter, J. The characterization of finite groups with dihedral Sylow 2-subgroups. I, II. *J. Algebra*, 2 (1965), 85–151, 218–270.

[21] Hertweck, M. The orders of torsion units in integral group rings of finite solvable groups. *Commun. Algebra , to appear*.

[22] Hertweck, M. Unit groups of integral finite group rings with no noncyclic abelian finite p-subgroups. *Commun. Algebra , to appear*.

[23] Hertweck, M. Another counterexample to a conjecture of Zassenhaus. *Beiträge Algebra Geom. 43*, 2 (2002), 513–520.

[24] Hertweck, M. Integral group ring automorphisms without Zassenhaus factorization. *Illinois J. Math. 46*, 1 (2002), 233–245.

[25] Hertweck, M. Contributions to the integral representation theory of groups. *Habilitationsschrift, Universität Stuttgart* (2004), 191.

[26] Hertweck, M. On the torsion units of some integral group rings. *Algebra Colloq. 13*, 2 (2006), 329–348.

[27] Hertweck, M. Partial Augmentations and Brauer Character Values of Torsion Units in Group Rings. *Manuskript* (2007), 1–16.

[28] Höfert, C. Die erste Vermutung von Zassenhaus für Gruppen kleiner Ordnung. *Diplomarbeit, Universität Stuttgart* (2004).

[29] Higman, G. Units in group rings. *Ph.D. thesis, University of Oxford* (1940).

[30] Huerta-Aparicio, L. M., Molina-Rueda, A., Raggi-Cárdenas, A. G. und Valero-Elizondo, L. On some invariants preserved by isomorphisms of tables of marks. *Preprint*.

[31] Hughes, I. und Pearson, K. R. The group of units of the integral group ring $\mathbb{Z}S_3$. *Canad. Bull. 15(4)* (1972), 529–534.

[32] Huppert, B. *Endliche Gruppen I.* Springer, Berlin-Heidelberg, 1967.

[33] Huppert, B. und Blackburn, N. *Finite groups. III*, vol. 243 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 1982.

[34] Huppert, B. und Lempken, W. Simple groups of order divisible by at most four primes. *Preprintreihe des IEM 5* (2000).

[35] Iiyori, N. und Yamaki, H. Prime graph components of the simple groups of Lie type over the field of even characteristic. *J. Algebra 155*, 2 (1993), 335–343.

[36] Kimmerle, W. Torsion units in integral group rings of finite insoluble groups. *Arithmetik von Gruppenringen, Mathematisches Forschungsinstitut Oberwolfach, Report No. 55/2007*, 21–22.

[37] Kimmerle, W. Beiträge zur ganzzahligen Darstellungstheorie endlicher Gruppen. *Bayreuth. Math. Schr.*, 36 (1991), 139.

[38] Kimmerle, W. On the prime graph of the unit group of integral group rings of finite groups. Chin, William (ed.) et al., Groups, rings and algebras. A conference in honor of Donald S. Passman, Madison, WI, USA, June 10–12, 2005. Providence, RI: American Mathematical Society (AMS). Contemporary Mathematics 420, 215-228, 2006.

[39] Kimmerle, W., Luca, F. und Raggi-Cárdenas, A. G. Irreducible Components and Isomorphisms of the Burnside Ring. *J. Group Theory, to appear*.

[40] Kimmerle, W., Lyons, R., Sandling, R. und Teague, D. N. Composition factors from the group ring and Artin's theorem on orders of simple groups. *Proc. Lond. Math. Soc., III. Ser. 60*, 1 (1990), 89–122.

[41] Kimmerle, W. und Sandling, R. Group theoretic and group ring theoretic determination of certain Sylow and Hall subgroups and the resolution of a question of R. Brauer. *J. Algebra 171*, 2 (1995), 329–346.

[42] Klingler, L. Construction of a counterexample to a conjecture of Zassenhaus. *Commun. Algebra 19* (1993), 2303–2330.

[43] Kondrat'ev, A. S. Prime graph components of finite simple groups. *Math. USSR, Sb. 67*, 1 (1990), 235–247.

[44] Lüneburg, H. Ein einfacher Beweis für den Satz von Zsigmondy über primitive Primteiler von $\mathsf{A}^{\mathsf{N}} - 1$. In *Geometries and groups (Berlin, 1981)*, vol. 893 of *Lecture Notes in Math.* Springer, Berlin, 1981, pp. 219–222.

[45] Luthar, I. S. und Passi, I. B. S. Zassenhaus conjecture for A_5. *Indian Acad. Sci. 99(1)* (1989), 1–5.

[46] Marciniak, Z., Ritter, J., Sehgal, S. und Weiss, A. Torsion units in integral group rings of some metabelian groups. II. *J. Number Theory 25* (1987), 340–352.

[47] Raggi-Cárdenas, A. G. und Valero-Elizondo, L. Groups with isomorphic Burnside rings. *Arch. Math. 84*, 3 (2005), 193–197.

[48] Roggenkamp, K. W. Integral group rings of solvable finite groups have no idempotent ideals. *Arch. Math. 25* (1974), 125–128.

[49] Roggenkamp, K. W. Observations to a conjecture of H. Zassenhaus. *Groups, St.Andrews 1989, Conf. Proc., Lond. Math. Soc. Lect. Note ser. 160, Nr.2* (1991), 427–444.

[50] Rottlaender, A. Nachweis der Existenz nicht-isomorpher Gruppen von gleicher Situation der Untergruppen. *Math. Z. 28*, 1 (1928), 641–653.

[51] Schur, I. Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. *J. reine angew. Math. 132* (1907), 85–137.

[52] Scott, L. L. On a conjecture of Zassenhaus, and beyond. *Algebra, Proc. Int. Conf. Memory A.I. Mal'cev, Novosibirsk 1989, Contemp. Math. 131(1)* (1992), 325–343.

[53] Sehgal, S. K. *Topics in group rings.* Dekker, New York, 1978.

[54] Sehgal, S. K. *Units in integral group rings.* Pitman Monographs and Surveys in Pure and Applied Mathematics. Vol. 69. Harlow: Longman Scientific & Technical, 1993.

[55] Thévenaz, J. Isomorphic Burnside rings. *Commun. Algebra 16*, 9 (1988), 1945–1947.

[56] Thompson, J. G. Nonsolvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc. 74* (1968), 383–437.

[57] Wagner, R. Zassenhausvermutung für die Gruppen $\mathsf{PSL}(2, \mathfrak{p})$. Diplomarbeit an der Universität Stuttgart, 1995.

[58] Walter, J. H. The characterization of finite groups with abelian Sylow 2-subgroups. *Ann. of Math. (2) 89* (1969), 405–514.

[59] Weiss, A. Torsion units in integral group rings. *J. reine angew. Math. 415* (1991), 175–187.

[60] Williams, J. S. Prime graph components of finite groups. *J. Algebra 69*, 2 (1981), 487–513.

[61] Zsigmondy, K. Zur Theorie der Potenzreste. *Monatsh. Math. Phys. 3*, 1 (1892), 265–284.