Der Darstellungstyp des Charakterrings einer endlichen Gruppe

Dissertation

zur Erlangung des akademischen Grades
doctor rerum naturalium (Dr. rer. nat.)

vorgelegt dem Rat der Fakultät für Mathematik und Informatik
der Friedrich-Schiller-Universität Jena

von Dipl.-Math. Tim Fritzsche
geboren am 29. 08. 1985 in Leipzig

Gutachter

1. Prof. Dr. Burkhard Külshammer, Jena

2. Prof. Dr. Wolfgang Kimmerle, Stuttgart

3. PD Dr. Klaus Haberland, Jena

Tag der öffentlichen Verteidigung: 18. 06. 2014

Inhaltsverzeichnis

Einleitung

Die Darstellungstheorie spielt beim Studium der Eigenschaften endlicher Gruppen oft eine wesentliche Rolle. Gewöhnlich betrachtet man zu einer endlichen Gruppe G die Gruppenalgebra $\mathbb{K}G$ für einen Körper $\mathbb{K}$ und untersucht die Isomorphieklassen von $\mathbb{K}G$-Moduln. Äquivalent dazu ist es, die Isomorphieklassen von $\mathbb{K}$-Darstellungen von G zu untersuchen. Eine mögliche Herangehensweise an diese Aufgabe ist, über die durch die direkte Summe und das Tensorprodukt definierte Halbring-Struktur dieser Darstellungen, den Grothendieckring $R_{\mathbb{K}}(G)$ zu definieren. Dieser wird auch als Darstellungsring oder Greenring bezeichnet. Im Fall $\mathbb{K} = \mathbb{C}$ verzichtet man meist auf die Bezeichnung, um welchen Körper es sich handelt, und schreibt nur $R(G)$.

Ebenso gibt es zum Halbring der gewöhnlichen Charaktere von G einen Grothendieckring, den Charakterring von G. Dieser ist isomorph zu $R(G)$, weswegen man auch den Charakterring mit $R(G)$ bezeichnet. Der Charakterring ist als $\mathbb{Z}$-Modul frei und endlich erzeugt, eine Basis bilden z. B. die irreduziblen Charaktere von G. Das impliziert, dass $R(G)$ eine $\mathbb{Z}$-Ordnung in der $\mathbb{Q}$-Algebra $\mathbb{Q} \otimes_{\mathbb{Z}} R(G)$ ist.

Welche Eigenschaften Ordnungen im Allgemeinen haben, wird in der Ganzen Darstellungstheorie untersucht. Für einen kommutativen Ring R mit 1 und eine R-Ordnung Λ in einer Algebra A schaut man sich dabei, wenn möglich, meist eine maximale R-Ordnung Λ' in A an, die Λ enthält, und versucht, über deren Eigenschaften auf die Eigenschaften von Λ zu schließen. Dieses Verfahren wird z. B. häufig bei der Untersuchung des mit dem Charakterring verwandten Burnsiderings $A(G)$ von G verwendet. So gelangt man beispielsweise zum Darstellungstyp [40, 41], zur Brauergruppe [50] und in vielen Fällen zur Einheitengruppe (siehe Bemerkungen in [50]) von $A(G)$. Auch die Brauergruppe von $R(G)$ lässt sich auf diesem Weg berechnen [22], was suggeriert, dass man weitere Eigenschaften von $R(G)$ über diesen Zugang bestimmen können sollte.

In dieser Dissertation wollen wir den Darstellungstyp des Charakterrings $R(G)$ einer endlichen Gruppe G allein über Angaben zur Gruppenstruktur von G bestimmen. Für den Gruppenring $\mathbb{Z}G$ weiß man, dass dessen Darstellungstyp genau dann endlich ist, wenn G ausschließlich zyklische Sylowgruppen enthält und die Ordnung von G kubikfrei ist [25, 26, 34, 3]. Da der Charakterring einer endlichen abelschen Gruppe zu deren Gruppenring isomorph ist, kennt man im Fall abelscher Gruppen also bereits das Ergebnis.

Für eine nichtabelsche Gruppe hat der Darstellungstyp des Gruppenrings nichts mehr mit dem des Charakterrings zu tun, da der Charakterring dann immer noch ein kommutativer Ring ist. Dafür gibt es für kommutative Ordnungen starke Kriterien, wann deren Darstellungstyp endlich ist (siehe [14]). Ein wesentliches Resultat stammt von Jones, wonach man ein Lokal-Global-Prinzip für den Darstellungstyp einer R-Ordnung Λ hat: Man betrachtet für gewisse Primideale $\mathfrak{p}$ von R die $\widehat{R}_{\mathfrak{p}}$-Ordnung $\widehat{R}_{\mathfrak{p}} \otimes_R \Lambda$, wobei $\widehat{R}_{\mathfrak{p}}$ für die Komplettierung des von $\mathfrak{p}$ induzierten diskreten

Bewertungsrings steht. Ein weiteres haben Jacobinski beziehungsweise Drozd und Roĭter gezeigt: Eine kommutative Ordnung Λ hat genau dann endlichen Darstellungstyp, wenn der Λ-Modul Λ'/Λ ein aus höchstens zwei Elementen bestehendes Erzeugendensystem hat und das Radikal dieses Moduls zyklisch ist. Beide Resultate stellen noch einige technische Bedingungen an Λ, die im Falle $\Lambda = R(G)$ aber alle erfüllt sind, wie wir sehen werden. Wir müssen nicht einmal auf die im Satz von Jones erwähnten Komplettierungen zurückgreifen, sondern können Lokalisierungen verwenden.

Im Laufe der Arbeit werden wir verschiedene Ergebnisse aus der Darstellungstheorie, der Theorie endlicher Gruppen sowie der algebraischen Zahlentheorie benötigen. Diese fassen wir im ersten Kapitel zusammen. Dort werden auch fast alle später verwendeten Bezeichnungen eingeführt.

Im zweiten Kapitel zeigen wir zunächst einige Eigenschaften des Charakterrings, ohne die die Anwendung des Satzes von Jacobinski/Drozd-Roĭter nicht zulässig wäre. Zudem bestimmen wir die maximale Ordnung $R(G)'$ von $R(G)$ in $\mathbb{Q} \otimes_{\mathbb{Z}} R(G)$ (Folgerung 2.6). Wir werden feststellen, dass diese maximale Ordnung isomorph zu einer direkten Summe von Ganzheitsringen algebraischer Zahlkörper, genauer gewissen Teilkörpern von Kreisteilungskörpern, ist. Daraus lässt sich mithilfe des Dirichletschen Einheitensatzes schnell auf den Rang der Einheitengruppe von $R(G)$ schließen. Des Weiteren sind die Torsionseinheiten nach Saksonov genau die linearen Charaktere von G und deren (additive) Inverse (siehe [43] oder [36]). Damit können wir den Isomorphietyp der Einheitengruppe von $R(G)$ exakt bestimmen (Satz 2.8). Dieser war bisher nur für wenige Gruppen G bekannt, beispielsweise hat sich Yamauchi mit der Einheitengruppe von $R(A_n)$ für alternierende Gruppen A_n vom Grad $n \geq 5$ befasst [57, 58] sowie mit der Frage, für welche Gruppen G es Einheiten unendlicher Ordnung in $R(G)$ gibt [59]. Dieses Ergebnis mag vielleicht vor allem deshalb überraschen, weil man den Isomorphietyp der maximalen Ordnung $R(G)'$ im Allgemeinen nicht kennt. Deren Torsionseinheiten zu bestimmen wäre nämlich äquivalent dazu, die Torsionseinheiten der Ganzheitsringe von Teilkörpern gewisser Kreisteilungskörper zu ermitteln. Es ist jedoch bis auf wenige Ausnahmen nicht einmal der Isomorphietyp der Einheitengruppen der Ganzheitsringe von Kreisteilungskörpern bekannt (siehe z. B. [53]).

Nach diesem kurzen Einschub zur Einheitengruppe von $R(G)$ schauen wir uns einige konkrete Funktionen aus $R(G)$ sowie aus $R(G)' \setminus R(G)$ an. Mithilfe dieser werden wir in Folgerung 2.14 zeigen, dass $R(G)$ unendlichen Darstellungstyp hat, sobald es in einer rationalen p'-Sektion von G mindestens vier $\mathbb{Q}$-Klassen gibt. Die Definition der $\mathbb{Q}$-Klassen endlicher Gruppen geht zurück auf Berman [1, 2], die $\mathbb{Q}$-Klassen von G stehen kanonisch in Bijektion zu den Konjugationsklassen zyklischer Untergruppen von G. Insbesondere folgt also, dass der Exponent von G nicht von der dritten Potenz irgendeiner Primzahl geteilt werden kann, wenn $R(G)$ endlichen Darstellungstyp hat.

Abgesehen davon, dass für eine Primzahl p der Exponent einer p-Sylowgruppe P von G höchstens p^2 sein kann, lässt sich noch viel mehr über die Struktur von P

aussagen, wenn der Darstellungstyp von $R(G)$ endlich ist. Das dritte Kapitel widmet sich diesem Thema. Am Ende dieses Kapitels werden wir schließen können, dass, sollte p ungerade sein, P entweder zyklisch der Ordnung $\leq p^2$ oder aber elementar-abelsch ist. Außerdem kommen neben elementar-abelschen 2-Gruppen und zyklischen Gruppen der Ordnung ≤ 4 auch noch Quaternionen- und Diedergruppen der Ordnung 8 sowie Suzuki 2-Gruppen, die als 2-Sylowgruppen der projektiven speziellen unitären Gruppen $\mathrm{PSU}(3, 2^n)$ für gewisse n auftreten, und eine weitere Suzuki 2-Gruppe der Ordnung 2^9 als 2-Sylowgruppen von G infrage.

Viele Ideen sowie das prinzipielle Vorgehen im dritten Kapitel orientieren sich an [11], wo Costantini und Jabara Gruppen untersuchen, in denen je zwei Untergruppen derselben Ordnung konjugiert sind. Strukturell ist das Kapitel wie folgt aufgebaut: Wir werden zunächst zeigen, dass G nur einen nichtabelschen Kompositionsfaktor haben kann, wenn $R(G)$ endlichen Darstellungstyp hat, und dann in Satz 3.6 die möglichen Isomorphietypen dieses Kompositionsfaktors ermitteln. Zur Bestimmung dieser möglichen Isomorphietypen nutzen wir die Tatsache, dass G nur eine Konjugationsklasse von Involutionen besitzen kann. Die (fast-)einfachen Gruppen mit nur einer Klasse von Involutionen sind durch Yamaki in [56] klassifiziert worden. Die Gruppen aus der Liste dieser Klassifikation betrachten wir separat. Wir werden feststellen, dass jede dieser Gruppen, deren Charakterring endlichen Darstellungstyp hat, nur zyklische und elementar-abelsche Sylowgruppen besitzt.

Anschließend bestimmen wir in Satz 3.12 die mögliche Gestalt der 2-Sylowgruppen und in Satz 3.15 die der p-Sylowgruppen ungerader Ordnung für eine Gruppe G, deren Charakterring endlichen Darstellungstyp hat. Die Beweise nutzen aus, dass man annehmen kann, dass in G eine Komponente, die eine p-Sylowgruppe von G enthält, liegt oder dass die p-Sylowgruppe von G der verallgemeinerten Fittinggruppe von G entspricht. Im Fall der 2-Sylowgruppen hilft dann die Klassifikation aller 2-Gruppen, in denen je zwei zyklische Untergruppen derselben Ordnung in deren Automorphismengruppe konjugiert sind, von Wilkens weiter [54]. Für die ungeraden p-Sylowgruppen werden wir auf die Klassifikation der transitiven linearen Gruppen durch Huppert und Hering zurückgreifen [31, 27]. Die Klassifikation der endlichen einfachen Gruppen geht damit an vielen Stellen in die Beweise im dritten Kapitel ein.

Schließlich versuchen wir im vierten Kapitel, auch hinreichende Kriterien dafür zu finden, dass $R(G)$ endlichen Darstellungstyp hat. Wir unterscheiden dabei nach der Gestalt der Sylowgruppen von G. Besitzt G zyklische p-Sylowgruppen der Ordnung $\leq p^2$, so können wir zeigen, dass die Ordnung $R(G)_p := \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} R(G)$ endlichen Darstellungstyp hat (Abschnitt 4.1). Damit folgt insbesondere, dass der Darstellungstyp von G endlich ist, wenn $|G|$ kubikfrei ist und G ausschließlich zyklische p-Sylowgruppen hat.

Im Fall, dass G elementar-abelsche p-Sylowgruppen enthält, wird es uns jedoch nicht in jedem Fall gelingen, von der Struktur von G auf den Darstellungstyp von $R(G)_p$ zu schließen. Wir untersuchen als erstes den Fall, dass alle zyklischen Gruppen der

Ordnung p konjugiert sind. Für eine p-Sylowgruppe P wissen wir in diesem Fall aufgrund der Klassifikation der transitiven linearen Gruppen, wie $N_G(P)/C_G(P)$ auf P operiert. Dies erlaubt unter Anwendung eines Satzes von Stickelberger (Satz 1.20) den Schluss, dass alle Elemente der Ordnung p in G konjugiert sein müssen, damit der Darstellungstyp von $R(G)_p$ endlich sein kann. Wir werden in einem Beispiel sehen, dass selbst das noch nicht garantiert, dass $R(G)_p$ endlichen Darstellungstyp hat.

Der Fall, dass G genau zwei Konjugationsklassen zyklischer Untergruppen der Ordnung p besitzt, ist in Ermangelung eines ähnlichen Resultats wie die Klassifikation der transitiven linearen Gruppen, deutlich komplizierter. Wir werden in einigen Fällen zwar ausschließen, dass $R(G)$ endlichen Darstellungstyp haben kann, jedoch auch ein Beispiel einer Gruppe G angeben, deren Charakterring endlichen Darstellungstyp hat, obwohl G eine elementar-abelsche 5-Sylowgruppe der Ordnung 25 besitzt und nicht alle Elemente der Ordnung 5 in G konjugiert sind.

Zu guter Letzt werden wir sehen, dass es bei der Bestimmung des Darstellungstyps von $R(G)_2$, wenn G nichtzyklische 2-Sylowgruppen besitzt, ähnliche Probleme gibt, wie bei der Bestimmung des Darstellungstyps von $R(G)_p$, wenn G eine elementar-abelsche p-Sylowgruppe und nur eine Konjugationsklasse von Elementen der Ordnung p hat. Diese Beobachtung sowie eine Zusammenfassung der vorherigen Strukturaussagen wird die Dissertation abschließen.

Für die interessante Aufgabenstellung und die Unterstützung meiner Arbeit möchte ich mich bei meinem Betreuer Prof. Dr. Burkhard Külshammer bedanken. Ein weiterer Dank gilt PD Dr. Haberland für den Beweis zu Lemma 4.8, ohne das deutlich mehr Fragen zu Gruppen mit elementar-abelschen Sylowgruppen offen geblieben wären.

1 Grundlagen

In diesem Kapitel wollen wir bekannte Fakten aus der Zahlentheorie, Gruppentheorie und Darstellungstheorie zusammentragen, die wir später verwenden werden. Die Beweise der einzelnen Resultate lassen sich, sofern keine weiteren Angaben erfolgen, in der Standardliteratur finden. Für die Zahlentheorie sind damit zum Beispiel [4] und [39] gemeint, für die Aussagen zur Theorie ganzer Darstellungen beispielsweise [14]. Weiter stehen die Resultate zur Charaktertheorie unter anderem in [32] oder [44] und die über endliche Gruppen in [29, 30, 31]. Zudem setzen wir einige Begriffe aus der Algebra als bekannt voraus und gehen nicht weiter auf diese ein.

Sämtliche in dieser Arbeit auftretende Moduln sind als Linksmoduln anzusehen. Die im Verlauf der Arbeit verwendeten Charaktertafeln sind entweder in den jeweils angegebenen Quellen oder im Anhang zu finden.

1.1 Dedekindringe

Ein wesentliches Prinzip in dieser Arbeit wird es sein, Fragen über gewisse kommutative Ringe auf Fragen über zu diesen assoziierte Dedekindringe zurückzuführen. In diesem Abschnitt wollen wir deshalb auf einige Aussagen sowohl zu Dedekindringen im Allgemeinen als auch zu speziellen Klassen von Dedekindringen eingehen.

Definition 1.1. Sei R ein nullteilerfreier, kommutativer Ring mit Einselement. Ist R noethersch sowie ganzabgeschlossen in seinem Quotientenkörper und ist außerdem jedes von (0) verschiedene Primideal von R ein maximales Ideal, so bezeichnet man R als Dedekindring.

Eine wichtige Eigenschaft von Dedekindringen ist, dass es in ihnen eine Primfaktorzerlegung gibt. Genauer lässt sich jedes nichttriviale echte Ideal eines Dedekindrings in (bis auf Reihenfolge) eindeutiger Weise als Produkt von endlich vielen Primidealen schreiben. Oft wird der Begriff Dedekindring auch als Integritätsbereich, in dem eine solche Primfaktorzerlegung existiert, definiert. Es lässt sich zeigen, dass diese Definition äquivalent zur obigen ist.

Aus der eindeutigen Primfaktorzerlegung in Dedekindringen folgt sofort, dass jeder Hauptidealring ein Dedekindring ist. Umgekehrt ist natürlich nicht jeder Dedekindring auch ein Hauptidealring, es gilt aber zumindest Folgendes:

Lemma 1.2. *Sei R ein Dedekindring mit nur endlich vielen Primidealen. Dann ist R ein Hauptidealring.*

Weitere Dedekindringe, die für uns von Interesse sein werden (und zum Teil ebenfalls Hauptidealringe sind), sind unter anderem Ganzheitsringe von algebraischen Zahlkörpern. Unter einem algebraischen Zahlkörper verstehen wir dabei eine endliche Körpererweiterung der rationalen Zahlen $\mathbb{Q}$, und der Ganzheitsring eines solchen ist der ganze Abschluss von $\mathbb{Z}$ in diesem Erweiterungskörper. Im Folgenden bezeichnen wir den Ganzheitsring eines algebraischen Zahlkörpers $\mathbb{K}$ mit $\mathcal{O}_{\mathbb{K}}$.

1.1.1 Primideale in Erweiterungen

In diesem Abschnitt sei R ein Dedekindring mit Quotientenkörper $\mathbb{K}$, $\mathbb{L}/\mathbb{K}$ eine endliche separable Körpererweiterung und S der ganze Abschluss von R in $\mathbb{L}$. Unter diesen Voraussetzungen ist auch S ein Dedekindring, insbesondere ist jedes von (0) verschiedene Primideal von S maximal. Unser Interesse gilt den Zusammenhängen zwischen den Primidealen von R und S. Um nicht jedes Mal das Nullideal extra ausschließen zu müssen, formulieren wir die folgenden Aussagen für maximale Ideale statt Primideale.

Für ein maximales Ideal $\mathfrak{p}$ aus R lässt sich das Ideal $\mathfrak{p}S$ von S also als Produkt $\mathfrak{p}S = \mathfrak{P}_1 \cdots \mathfrak{P}_n$ endlich vieler maximaler Ideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ aus S schreiben. Ist $\mathfrak{P}$ eines dieser Ideale, so gilt $\mathfrak{P} \cap R = \mathfrak{p}$. Man sagt in diesem Fall, dass $\mathfrak{P}$ über $\mathfrak{p}$ liegt. Offenbar liegt kein maximales Ideal von S, das nicht mit einem der Ideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ übereinstimmt, über $\mathfrak{p}$. Die Aussagen dieses Absatzes lassen sich also wie folgt zusammenfassen:

Satz 1.3. *Zu jedem maximalen Ideal $\mathfrak{p}$ von R existiert ein maximales Ideal $\mathfrak{P}$ in S, das über $\mathfrak{p}$ liegt. Zudem liegen in S nur endlich viele maximale Ideale über $\mathfrak{p}$.*

Über die Anzahl der über einem maximalen Ideal $\mathfrak{p}$ von R liegenden maximalen Ideale aus S lassen sich genauere Aussagen treffen. Bevor wir diese formulieren können, benötigen wir aber noch einige Begriffe.

Definition 1.4. Sei $\mathfrak{p}$ ein maximales Ideal von R und habe $\mathfrak{p}S$ die Primfaktorzerlegung $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_n^{e_n}$ in S mit paarweise verschiedenen Primidealen $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$.

(i) Der Exponent $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ heißt Verzweigungsindex von $\mathfrak{P}_i$ (über $\mathfrak{p}$), $i \in \{1, \ldots, n\}$.

(ii) Der Grad $f_i = f(\mathfrak{P}_i/\mathfrak{p})$ der Körpererweiterung $(S/\mathfrak{P}_i)/(R/\mathfrak{p})$ ist der Trägheitsgrad von $\mathfrak{P}_i$ (über $\mathfrak{p}$), $i \in \{1, \ldots, n\}$.

Des Weiteren nennen wir ein maximales Ideal $\mathfrak{p}$ von R unverzweigt, wenn für jedes $\mathfrak{P}$ aus S, welches über $\mathfrak{p}$ liegt, der Verzweigungsindex von $\mathfrak{P}$ gleich 1 ist. Andernfalls heißt $\mathfrak{p}$ verzweigt und wenn der Trägheitsgrad von $\mathfrak{P}$ den Wert 1 hat, total verzweigt.

Für die Anzahl der in S über einem maximalen Ideal von R liegenden maximalen Ideale erhält man nun die folgende Formel.

Satz 1.5. *Für ein maximales Ideal* $\mathfrak{p}$ *von* R *mit* $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_n^{e_n}$, $\mathfrak{P}_i \neq \mathfrak{P}_j$ *für* $i \neq j$, *gilt*

$$[\mathbb{L} : \mathbb{K}] = \sum_{i=1}^{n} e_i f_i \,.$$

Diese Formel legt nahe, dass es, wie für den Grad endlicher separabler Körpererweiterungen, auch für den Verzweigungsindex und den Trägheitsgrad Turmsätze gibt. Das ist tatsächlich der Fall. Sei also zusätzlich zu den obigen Voraussetzungen noch $\mathbb{M}/\mathbb{L}$ eine endliche separable Erweiterung und T der ganze Abschluss von S in $\mathbb{M}$.

Satz 1.6. *Sind* $\mathfrak{p}$, $\mathcal{P}$ *und* $\mathfrak{P}$ *maximale Ideale von* R, S *bzw.* T, *sodass* $\mathcal{P}$ *über* $\mathfrak{p}$ *und* $\mathfrak{P}$ *über* $\mathcal{P}$ *liegt, so gilt*

$$\begin{aligned} e(\mathfrak{P}/\mathfrak{p}) &= e(\mathfrak{P}/\mathcal{P}) \cdot e(\mathcal{P}/\mathfrak{p}) \qquad \textit{sowie} \\ f(\mathfrak{P}/\mathfrak{p}) &= f(\mathfrak{P}/\mathcal{P}) \cdot f(\mathcal{P}/\mathfrak{p}) \,. \end{aligned}$$

Um herauszubekommen, welche Primideale von R in S verzweigt sind, kann man die Diskriminante von $\mathbb{L}/\mathbb{K}$ zurate ziehen. Bevor wir diese einführen, wollen wir noch an die Begriffe Spur und Norm für endliche Körpererweiterungen erinnern.

Definition 1.7. Für $x \in \mathbb{L}$ sei A_x die Abbildungsmatrix der $\mathbb{K}$-linearen Abbildung $f : \mathbb{L} \to \mathbb{L}$, $y \mapsto xy$. Die Spur $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ und die Norm $\mathrm{N}_{\mathbb{L}/\mathbb{K}}$ der Körpererweiterung $\mathbb{L}/\mathbb{K}$ sind die durch

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}} : \mathbb{L} \to \mathbb{K} \,, \quad x \mapsto \mathrm{Spur}(A_x) \qquad \text{sowie} \qquad \mathrm{N}_{\mathbb{L}/\mathbb{K}} : \mathbb{L}^\times \to \mathbb{K}^\times \,, \quad x \mapsto \det(A_x)$$

definierten Abbildungen.

Wenn klar ist, bezüglich welcher Erweiterung wir die Spur oder die Norm betrachten, schreiben wir auch einfach Tr statt $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ bzw. N statt $\mathrm{N}_{\mathbb{L}/\mathbb{K}}$. Für konkrete Berechnungen empfehlen sich oft die folgenden Darstellungen von Spur und Norm.

Proposition 1.8. *Sei* $\overline{\mathbb{K}}$ *der algebraische Abschluss von* $\mathbb{K}$. *Für* $x \in \mathbb{L}$ *gilt dann*

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) = \sum_{\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})} \sigma(x) \qquad \textit{und} \qquad \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) = \prod_{\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})} \sigma(x) \,.$$

Ist $\mathbb{L}/\mathbb{K}$ *eine Galois-Erweiterung, so laufen die Summe und das Produkt also jeweils über die Galois-Automorphismen von* $\mathbb{L}/\mathbb{K}$.

Manchmal kann man mithilfe der Norm schnell herausfinden, ob ein Element aus S ein Primideal von S erzeugt. Ist beispielsweise $R = \mathbb{Z}$ und $\mathfrak{p}$ ein Primideal aus S, das über einem Primideal (p) von $\mathbb{Z}$ total verzweigt und zudem ein Hauptideal ist, so erzeugt $x \in \mathfrak{p}$ das Ideal $\mathfrak{p}$ genau dann, wenn $|\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)| = p$ gilt. Natürlich hat die Norm noch wichtigere Anwendungen, insbesondere wenn man sie auf eine Norm für Ideale verallgemeinert. Davon werden wir aber keinen Gebrauch machen.

Mithilfe der Spur lässt sich eine nichtausgeartete Bilinearform $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$, die Spurform, definieren. Diese ist gegeben durch $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}} : \mathbb{L} \times \mathbb{L} \to \mathbb{K}$, $(x, y) \mapsto \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(xy)$. Über sie gelangen wir zur Diskriminante.

Definition 1.9. Sei $\{x_1, \ldots, x_n\}$ eine $\mathbb{K}$-Basis von $\mathbb{L}$ und A die $n \times n$-Matrix, die an der Stelle (i, j) den Eintrag $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x_i x_j)$ hat. Dann heißt $d(x_1, \ldots, x_n) := \det(A)$ Diskriminante von $x_1, \ldots, x_n$.

Auch hier gibt es wieder eine Darstellung über die $\mathbb{K}$-Einbettungen von $\mathbb{L}$ in $\overline{\mathbb{K}}$. Bezeichnen wir diese mit $\sigma_1, \ldots, \sigma_n$ und setzen B als die Matrix, deren Eintrag an der Stelle (i, j) gerade $\sigma_i(x_j)$ für eine $\mathbb{K}$-Basis $\{x_1, \ldots, x_n\}$ von $\mathbb{L}$ ist, so gilt $d(x_1, \ldots, x_n) = (\det(B))^2$. Ist $\{y_1, \ldots, y_n\}$ eine weitere $\mathbb{K}$-Basis von $\mathbb{L}$ und $C = (c_{ij})$ die $n \times n$-Matrix über $\mathbb{K}$, die $y_i = \sum_{j=1}^{n} c_{ij} x_j$ erfüllt, so erhält man mithilfe dieser Darstellung leicht $d(y_1, \ldots, y_n) = d(x_1, \ldots, x_n)(\det(C))^2$.

Wenn die Elemente der $\mathbb{K}$-Basis $\{x_1, \ldots, x_n\}$ von $\mathbb{L}$ allesamt in R liegen, dann ist offenbar auch $d(x_1, \ldots, x_n) \in R$. Die Diskriminanten unterschiedlicher R-Basen von S unterscheiden sich aufgrund der eben genannten Formel für den Basiswechsel höchstens um eine Einheit aus R. Das durch $d(x_1, \ldots, x_n)$ in R erzeugte Hauptideal $\mathfrak{d}$ ist also unabhängig von der Wahl der Basis $\{x_1, \ldots, x_n\}$. Dieses Ideal enthält alle Informationen darüber, welche Primideale aus R in S verzweigt sind.

Satz 1.10. *Ein Primideal $\mathfrak{p}$ von R ist genau dann in S verzweigt, wenn $\mathfrak{p}$ das Ideal $\mathfrak{d}$ teilt.*

Wir interessieren uns vor allem für den Spezialfall $\mathbb{K} = \mathbb{Q}$. Für zwei $\mathbb{Z}$-Basen $\{x_1, \ldots, x_n\}$ und $\{y_1, \ldots, y_n\}$ von S und die entsprechende Basiswechselmatrix C ist $d(y_1, \ldots, y_n) = d(x_1, \ldots, x_n)(\det(C))^2$. Nun ist $\det(C)$ aber eine Einheit in $\mathbb{Z}$ und folglich $(\det(C))^2 = 1$. Die Diskriminante $d_{\mathbb{L}}$ von $\mathbb{L}$ ist deshalb als $d(x_1, \ldots, x_n)$ für irgendeine Basis $\{x_1, \ldots, x_n\}$ definiert. Mit dem vorigen Satz erhalten wir sofort:

Folgerung 1.11. *Eine Primzahl $p \in \mathbb{Z}$ ist genau dann in S verzweigt, wenn p ein Teiler von $d_{\mathbb{L}}$ ist.*

Mit Satz 1.6 folgt dann, dass jede in S verzweigte Primzahl auch in T verzweigt ist.

Die Diskriminante ist nicht nur im Zusammenhang mit der Verzweigung von Primidealen interessant. Auch über die Struktur gewisser Ganzheitsringe lassen sich dank ihr mitunter Aussagen treffen.

Lemma 1.12. *Seien $\mathbb{E}, \mathbb{F}$ algebraische Zahlkörper mit $\mathbb{E} \cap \mathbb{F} = \mathbb{Q}$ und $\mathrm{ggT}(d_{\mathbb{E}}, d_{\mathbb{F}}) = 1$. Dann gilt $\mathcal{O}_{\mathbb{E}\mathbb{F}} = \mathcal{O}_{\mathbb{E}}\mathcal{O}_{\mathbb{F}}$.*

1.1.2 Ganzheitsringe von Kreisteilungskörpern

Sei n eine natürliche Zahl > 2 und ζ_n eine primitive n-te Einheitswurzel. Die Körpererweiterung $\mathbb{Q}(\zeta_n)$ von $\mathbb{Q}$ wird dann n-ter Kreisteilungskörper genannt. Hierbei handelt es sich um eine Galois-Erweiterung vom Grad $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, wobei φ die

Eulersche φ-Funktion bezeichnet. Die Galois-Automorphismen werden durch die Abbildungen $\zeta_n \mapsto \zeta_n^a$ mit $1 \leq a < n$ und $\mathrm{ggT}(a,n) = 1$ induziert.

Im Allgemeinen ist es schwierig, den Ganzheitsring eines algebraischen Zahlkörpers explizit anzugeben. Dagegen lassen sich die Ganzheitsringe der Kreisteilungskörper einfach beschreiben.

Satz 1.13. *Der Ganzheitsring von $\mathbb{Q}(\zeta_n)$ ist $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.*

Zudem kennt man nicht nur die Gestalt der Ganzheitsringe, sondern auch ihre Diskriminanten. Wir geben diese hier nicht exakt an, sondern beschränken uns auf ihre Primteiler.

Proposition 1.14. *Seien m, n positive ganze Zahlen mit $\mathrm{ggT}(m,n) = 1$. Dann gilt $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ und $\mathrm{ggT}(d_{\mathbb{Q}(\zeta_m)}, d_{\mathbb{Q}(\zeta_n)}) = 1$.*

Mithilfe von Lemma 1.12 gelangen wir also zu folgendem Resultat:

Folgerung 1.15. *Seien m, n positive ganze Zahlen mit $\mathrm{ggT}(m,n) = 1$ und $\mathbb{K}, \mathbb{L}$ algebraische Zahlkörper mit $\mathbb{K} \subseteq \mathbb{Q}(\zeta_m)$ und $\mathbb{L} \subseteq \mathbb{Q}(\zeta_n)$. Dann gilt $\mathcal{O}_{\mathbb{KL}} = \mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$.*

Neben der Gestalt der Ganzheitsringe von Kreisteilungskörpern ist für uns auch das Zerlegungsverhalten der gewöhnlichen Primzahlen (also der nichttrivialen Primideale von $\mathbb{Z}$) in ihnen von Interesse. Die Menge dieser Primzahlen werden wir im Folgenden mit $\mathbb{P}$ bezeichnen.

Satz 1.16. *Seien $p \in \mathbb{P}$ und $k \in \mathbb{N}$, sodass $p^k > 2$ gilt. Ist p kein Teiler von n, so ist p in $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ unverzweigt. Außerdem ist p die einzige verzweigte Primzahl in $\mathcal{O}_{\mathbb{Q}(\zeta_{p^k})}$ und dort total verzweigt.*

Für den Fall, dass n eine Potenz der Primzahl p ist, gibt es also nur ein einziges Primideal in $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$, das p enthält. Auch dessen Gestalt lässt sich allgemein angeben.

Lemma 1.17. *Seien $p \in \mathbb{P}$ und $k \in \mathbb{N}$, sodass $p^k > 2$ gilt. Das p enthaltende Primideal von $\mathcal{O}_{\mathbb{Q}(\zeta_{p^k})}$ ist $(1 - \zeta_{p^k})$.*

1.1.3 Lokalisierungen und Komplettierungen

Sei wieder R ein Dedekindring mit Quotientenkörper $\mathbb{K}$. Eine Teilmenge $S \subset R$ heißt multiplikativ, wenn mit $x, y \in S$ auch xy in S liegt und außerdem 1_R, nicht jedoch 0_R in S enthalten ist. Die Lokalisierung $S^{-1}R$ von R in S ist dann die Menge $\left\{\frac{r}{s} \in \mathbb{K} : r \in R,\, s \in S\right\}$.

Proposition 1.18. *Ist $S \subset R$ multiplikativ, so ist $S^{-1}R$ ein Dedekindring. Die Primideale von $S^{-1}R$ stehen dabei in Bijektion zu den Primidealen von R, die kein Element mit S gemeinsam haben.*

Der Ring $S^{-1}R$ enthält also im Allgemeinen viel weniger Primideale als R und hat dadurch eine leichter zu verstehende Struktur. Wählt man insbesondere $S = R \setminus \mathfrak{p}$ für ein maximales Ideal $\mathfrak{p}$ von R, so besitzt $S^{-1}R$ nur noch ein maximales Ideal. Statt Eigenschaften von $\mathfrak{p}$ in R zu untersuchen, versucht man diese über die Eigenschaften des maximalen Ideals in $S^{-1}R$ herzuleiten.

Für $S = R \setminus \mathfrak{p}$ schreiben wir auch $R_\mathfrak{p}$ statt $S^{-1}R$ und nennen $R_\mathfrak{p}$ die Lokalisierung von R nach $\mathfrak{p}$. Nach Lemma 1.2 ist $R_\mathfrak{p}$ ein Hauptidealring. Ein Integritätsbereich, der nur ein maximales Ideal besitzt und außerdem ein Hauptidealring ist, heißt diskreter Bewertungsring, $R_\mathfrak{p}$ ist also ein solcher.

Ist π ein Erzeuger des maximalen Ideals von $R_\mathfrak{p}$, so lässt sich jedes Element $x \in \mathbb{K}^\times$ in eindeutiger Weise als $x = u\pi^k$ für eine Einheit $u \in R_\mathfrak{p}^\times$ und ein $k \in \mathbb{Z}$ schreiben. Dies motiviert die Definition eines Homomorphismus $\nu_\mathfrak{p} : \mathbb{K}^\times \to \mathbb{Z}$, $x = u\pi^k \mapsto k$. Zusätzlich setzen wir noch $\nu_\mathfrak{p}(0) := \infty$. Für diesen Homomorphismus gilt offenbar $\nu_\mathfrak{p}(x + y) \geq \min\{\nu_\mathfrak{p}(x), \nu_\mathfrak{p}(y)\}$, falls $x, y \in \mathbb{K}$. Die Lokalisierung $R_\mathfrak{p}$ können wir dann auch als $R_\mathfrak{p} = \{x \in \mathbb{K} : \nu_\mathfrak{p}(x) \geq 0\}$ und das maximale Ideal (π) von $R_\mathfrak{p}$ als $(\pi) = \{x \in \mathbb{K} : \nu_\mathfrak{p}(x) > 0\}$ schreiben. Diese Konstruktion lässt sich wie folgt auf beliebige Körper der Charakteristik 0 verallgemeinern.

Definition 1.19. Sei $\mathbb{L}$ ein Körper der Charakteristik 0. Eine Abbildung $\nu : \mathbb{L} \to \mathbb{R} \cup \{\infty\}$ heißt Exponentialbewertung, falls für $x, y \in \mathbb{L}$ gilt:

(i) $\nu(x) = \infty \Leftrightarrow x = 0$,

(ii) $\nu(xy) = \nu(x) + \nu(y)$,

(iii) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$.

Ist zusätzlich $\nu(\mathbb{L}^\times)$ zyklisch, so nennt man ν diskrete Exponentialbewertung.

Sei im Folgenden $\mathbb{L}$ ein Körper der Charakteristik 0 und ν eine Exponentialbewertung von $\mathbb{L}$. Ist ν diskret, so ist $\mathcal{O}_\nu := \{x \in \mathbb{L} : \nu(x) \geq 0\}$ tatsächlich ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m}_\nu = \{x \in \mathbb{L} : \nu(x) > 0\}$. Der Körper $\mathcal{O}_\nu/\mathfrak{m}_\nu$ heißt Restklassenkörper von $\mathbb{L}$.

Für eine beliebige reelle Zahl $0 < \gamma < 1$ liefert die Abbildung $d_\nu : \mathbb{L} \times \mathbb{L} \to \mathbb{R}$, $(x, y) \mapsto \gamma^{\nu(x-y)}$ eine Metrik auf $\mathbb{L}$, wenn man noch $\gamma^{\nu(0)} = \gamma^\infty := 0$ setzt. Auf diese Weise lassen sich analytische Begriffe wie Grenzwert, Konvergenz, Cauchyfolge usw. auf $\mathbb{L}$ definieren. Metriken, die durch dieselbe Exponentialbewertung induziert werden, sind dabei äquivalent. Der Körper $\mathbb{L}$ heißt vollständig bezüglich ν, wenn in $\mathbb{L}$ jede Cauchyfolge bezüglich d_ν konvergiert. Falls $\mathbb{L}$ nicht vollständig bezüglich ν ist, so lässt sich $\mathbb{L}$ zumindest in einen im Wesentlichen eindeutig bestimmten Körper $\widehat{\mathbb{L}}$ einbetten, in dem $\mathbb{L}$ dicht liegt und der eine Exponentialbewertung $\hat{\nu}$ trägt, die ν fortsetzt und bezüglich der $\widehat{\mathbb{L}}$ vollständig ist. Diesen Körper $\widehat{\mathbb{L}}$ nennt man die Komplettierung von $\mathbb{L}$ (bezüglich ν). Ist ν diskret, so ist dabei auch $\hat{\nu}$ diskret.

Ist $\mathbb{K}$ ein algebraischer Zahlkörper und $\mathfrak{p}$ ein maximales Ideal von R, so ist das oben definierte $\nu_\mathfrak{p}$ also eine diskrete Exponentialbewertung von $\mathbb{K}$. Die Komplettierung

von $\mathbb{K}$ bezüglich $\nu_{\mathfrak{p}}$ wird mit $\mathbb{K}_{\mathfrak{p}}$ bezeichnet. Ein wichtiger Spezialfall ergibt sich für $R = \mathbb{Z}$. Für $p \in \mathbb{P}$ bezeichnet $\mathbb{Q}_p$ die Komplettierung von $\mathbb{Q}$ bezüglich $\nu_{(p)}$. Diese Komplettierung nennt man den Körper der p-adischen Zahlen und den durch $\{x \in \mathbb{Q}_p : \nu_{(p)}(x) \geq 0\}$ definierten diskreten Bewertungsring $\mathbb{Z}_p$ den Ring der ganzen p-adischen Zahlen. Jedes Element x aus $\mathbb{Z}_p$ besitzt damit eine eindeutige Darstellung

$$x = \sum_{i=0}^{\infty} x_i p^i \quad \text{mit } x_i \in \{0, 1, \ldots, p-1\}\,.$$

Das maximale Ideal von $\mathbb{Z}_p$ ist dann $p\mathbb{Z}_p$. Der Körper $\mathbb{Q}_p$ ist zwar nicht algebraisch abgeschlossen und sein algebraischer Abschluss $\overline{\mathbb{Q}}_p$ nicht vollständig, dessen Komplettierung $\mathbb{C}_p$ ist aber schließlich algebraisch abgeschlossen.

Man kann zeigen, dass sich jede endliche Erweiterung von $\mathbb{Q}_p$ in der Form $\mathbb{K}_{\mathfrak{p}} = \mathbb{K}\mathbb{Q}_p$ für einen algebraischen Zahlkörper $\mathbb{K}$ und ein über (p) liegendes Primideal $\mathfrak{p}$ von $\mathcal{O}_{\mathbb{K}}$ schreiben lässt. Man setzt dann $e(\mathbb{K}_{\mathfrak{p}}/\mathbb{Q}_p) = e(\mathfrak{p}/(p))$ und nennt die Erweiterung unverzweigt, wenn $e(\mathbb{K}_{\mathfrak{p}}/\mathbb{Q}_p) = 1$ gilt. Für jede positive ganze Zahl n gibt es dann genau eine unverzweigte Erweiterung von $\mathbb{Q}_p$ vom Grad n. Der Restklassenkörper dieses Erweiterungskörpers besteht dabei aus p^n Elementen.

Wir bezeichnen die Lokalisierung von $\mathbb{Z}$ nach dem Primideal (p) im Folgenden immer mit $\mathbb{Z}_{(p)}$, um sie von den ganzen p-adischen Zahlen $\mathbb{Z}_p$ zu unterscheiden.

1.1.4 Gaußsche Summen

Sei $\mathbb{L} = \mathbb{Q}(\zeta_p)$ für ein $p \in \mathbb{P}$. Im Allgemeinen ist es schwierig zu entscheiden, ob gewisse Summen oder gar $\mathcal{O}_{\mathbb{L}}$-Linearkombinationen von Potenzen von ζ_p Einheiten in $\mathcal{O}_{\mathbb{L}}$ sind bzw. in welcher Potenz des p enthaltenden maximalen Ideals von $\mathcal{O}_{\mathbb{L}}$ sie womöglich liegen. In einigen Fällen kennt man jedoch die Antwort, z. B. wenn Gaußsche Summen vorliegen.

Sei $q = p^k$ für eine positive ganze Zahl k. Den endlichen Körper mit q Elementen bezeichnen wir mit $\mathbb{F}_q$. Sind $\psi \in \mathrm{Hom}(\mathbb{F}_q, \mathbb{C}^\times)$ ein additiver und $\chi \in \mathrm{Hom}(\mathbb{F}_q^\times, \mathbb{C}^\times)$ ein multiplikativer Homomorphismus, so definieren wir die Gaußsche Summe $\Gamma(\chi)$ durch

$$\Gamma(\chi) := \Gamma(\chi, \psi) := \sum_{\alpha \in \mathbb{F}_q^\times} \chi(\alpha)\psi(\alpha)\,.$$

Meist bezeichnet man Gaußsche Summen mit G. Bei uns wird G jedoch in der Regel für eine Gruppe stehen, deshalb weichen wir davon ab. Da Gaußsche Summen für endliche Körper das sind, was die Gammafunktion für die reellen bzw. komplexen Zahlen ist, wählen wir Γ als Bezeichnung.

Sei $\mathbb{K}$ die unverzweigte Erweiterung von $\mathbb{Q}_p$ mit Restklassenkörper $\mathbb{F}_q$. Mit μ_n bezeichnen wir für eine positive ganze Zahl n die Gruppe der n-ten Einheitswurzeln

in $\mathbb{C}_p$. Dann gibt es einen Isomorphismus zwischen der Gruppe $\mu_{q-1} \subset \mathbb{K}$ und $\mathbb{F}_q^\times$. Da die Spurform $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}_p}$ nicht ausgeartet ist, lässt sich $\Gamma(\chi, \psi)$ auch in der Form

$$\Gamma_\ell = \sum_{\alpha \in \mu_{q-1}} \alpha^{-\ell} \zeta^{\mathrm{Tr}(\alpha)}$$

für gewisse $\ell \in \mathbb{Z}$ und $\zeta \in \mu_p$ schreiben. Für diese Summe kann man die folgende Kongruenz zeigen.

Satz 1.20 (Stickelberger)**.** *Sei ℓ eine natürliche Zahl mit $0 < \ell < q-1$. Die p-adische Darstellung von ℓ habe die Form $\ell = \sum_{j=0}^{n-1} \ell_j p^j$, $0 \leq \ell_j < p$, und es sei*

$$\Gamma_\ell := \sum_{\alpha \in \mu_{q-1}} \alpha^{-\ell} \zeta^{\mathrm{Tr}(\alpha)}$$

für ein $\zeta \in \mu_p$. Dann gilt

$$\Gamma_\ell \equiv -\frac{(1-\zeta)^{\ell_0 + \ldots + \ell_{n-1}}}{\ell_0! \cdot \ldots \cdot \ell_{n-1}!} \quad \left(\mathrm{mod}\ (1-\zeta)^{\ell_0 + \ldots + \ell_{n-1}+1}\right).$$

Ein klassischer Beweis dieses Satzes lässt sich z. B. in [6] finden, ein modernerer Beweis in [8]. Ein analoges Resultat erhält man auch, wenn man Lokalisierungen statt Komplettierungen zugrunde legt (siehe z. B. [7]).

1.2 Gewöhnliche Charaktere

Im gesamten Abschnitt sei G eine endliche Gruppe. Für $g \in G$ und eine Teilmenge $X \subseteq G$ bezeichnen $C_G(g)$ den Zentralisator von g in G, $N_G(X)$ den Normalisator von X in G und $C_G(X)$ den Zentralisator von X in G, d. h. die Menge aller Elemente von G, die mit jedem Element aus X kommutieren. Außerdem stehe $Z(G)$ für das Zentrum von G. Das neutrale Element von G nennen wir 1 oder auch 1_G, auch die triviale Untergruppe $\{1\}$ von G wird im weiteren Verlauf mit 1 bezeichnet. Weiter schreiben wir $g \sim h$ bzw. $g \sim_G h$, wenn $g, h \in G$ in G konjugiert sind, und $\mathrm{cl}_G(g)$ für die Konjugationsklasse von g in G. Schließlich seien $\mathrm{Syl}_p(G)$ die Menge aller p-Sylowgruppen von G für $p \in \mathbb{P}$ und $\exp(G)$ der Exponent von G, d. h. die kleinste positive ganze Zahl n, sodass $g^n = 1$ für jedes $g \in G$ gilt.

1.2.1 Die Algebra der Klassenfunktionen

Eine gewöhnliche Darstellung von G ist ein Homomorphismus $\varrho : G \to \mathrm{GL}(n, \mathbb{C})$ für eine positive ganze Zahl n. Man sagt dann, dass die Darstellung ϱ den Grad n hat. Der zugehörige gewöhnliche Charakter wird durch $\chi_\varrho : G \to \mathbb{C}$, $g \mapsto \mathrm{Spur}(\varrho(g))$ definiert. Offenbar gilt $\chi_\varrho(1) = n$ und man nennt χ_ϱ einen Charakter vom Grad n.

Es sei an dieser Stelle angemerkt, dass es eine Korrespondenz zwischen den gewöhnlichen Darstellungen von G und den $\mathbb{C}G$-Moduln gibt, wobei $\mathbb{C}G$ für die Gruppenalgebra $\{\sum_{g\in G} a_g g : a_g \in \mathbb{C}\}$ steht. Für $v \in \mathbb{C}^n$, $g \in G$ und eine gewöhnliche Darstellung ϱ von G setzt man $g \cdot v := \varrho(g)v$, womit $\mathbb{C}^n$ zu einem $\mathbb{C}G$-Modul wird. Hat man andererseits einen $\mathbb{C}G$-Modul M, so kann man eine Basis von M wählen und $\varrho(g)$ für $g \in G$ als die Matrix der durch g auf M induzierten Abbildung definieren. Diese Korrespondenz hat man allgemein auch, wenn man $\mathbb{C}$ durch einen beliebigen anderen Körper $\mathbb{K}$ ersetzt (und als Darstellungen demzufolge Homomorphismen nach $\mathrm{GL}(n, \mathbb{K})$ betrachtet). Deshalb versteht man unter Darstellungstheorie im Allgemeinen die Untersuchung von Moduln über Algebren.

Wenn wir von Darstellungen oder Charakteren einer Gruppe schreiben, meinen wir ab jetzt immer gewöhnliche Darstellungen bzw. gewöhnliche Charaktere. Für verschiedene Darstellungen ϱ_1, ϱ_2 können χ_{ϱ_1} und χ_{ϱ_2} durchaus identisch sein. Das passiert aber nur dann, wenn es eine Matrix $M \in \mathrm{GL}(n, \mathbb{C})$ gibt, sodass $M\varrho_1(g)M^{-1} = \varrho_2(g)$ für jedes $g \in G$ gilt. Umgekehrt folgt aus $\mathrm{Spur}(AB) = \mathrm{Spur}(BA)$ für beliebige $n\times n$-Matrizen A, B, dass $\chi_{\varrho_1} = \chi_{\varrho_2}$ ist, wenn solch eine Matrix M existiert. Die Darstellungen ϱ_1 und ϱ_2 heißen dann ähnlich. Bis auf Ähnlichkeit kann man jedem Charakter also in eindeutiger Weise eine Darstellung zuordnen.

Aus $\mathrm{Spur}(AB) = \mathrm{Spur}(BA)$ für $n\times n$-Matrizen A, B folgt außerdem, dass für Elemente $g, h \in G$, die in derselben Konjugationsklasse von G liegen, $\chi_\varrho(g) = \chi_\varrho(h)$ gilt. Die gewöhnlichen Charaktere von G sind also konstant auf den Konjugationsklassen von G und gehören dementsprechend zu den Klassenfunktionen von G.

Man kann schnell nachweisen, dass es für eine Darstellung ϱ vom Grad n und ein Element $g \in G$ der Ordnung a eine zu ϱ ähnliche Darstellung $\tilde{\varrho}$ gibt, sodass $\tilde{\varrho}(g)$ eine Diagonalmatrix mit a-ten Einheitswurzeln als Diagonaleinträgen ist. Demzufolge lässt sich die Zahl $\chi_\varrho(g)$ als Summe von genau n a-ten Einheitswurzeln schreiben. Ist ϱ irreduzibel, so folgt daraus und mit der unten aufgeführten zweiten Orthogonalitätsrelation für ein Element $z \in Z(G)$ die Gleichung $\chi_\varrho(z) = \zeta\chi_\varrho(1)$, wobei ζ eine $|\langle z\rangle|$-te Einheitswurzel ist. Des Weiteren gilt immer $\chi_\varrho(g^{-1}) = \overline{\chi_\varrho(g)}$ bzw. allgemeiner $\chi_\varrho(g^k) = \sigma(\chi_\varrho(g))$, wenn σ der Automorphismus aus $\mathrm{Gal}(\mathbb{Q}(\zeta_{|\langle g\rangle|})/\mathbb{Q})$ ist, für den $\sigma(\zeta_{|\langle g\rangle|}) = \zeta^k_{|\langle g\rangle|}$ gilt.

Wie für algebraische Strukturen üblich, versucht man auch Darstellungen als Summe ihrer unzerlegbaren Bestandteile zu schreiben. Zu einer Darstellung ϱ von G existiert stets ein $m \in \mathbb{N}$ und eine invertierbare komplexe $n\times n$-Matrix M, sodass die Matrix $M\varrho(g)M^{-1}$ die Blockdiagonalgestalt

$$\begin{pmatrix} \varrho_1(g) & & & \\ & \varrho_2(g) & & \\ & & \ddots & \\ & & & \varrho_m(g) \end{pmatrix}$$

für $g \in G$ hat. Dabei ist die Größe der einzelnen Blöcke unabhängig von g. Ist dies sogar für ein $m \geq 2$ der Fall, so repräsentieren $\varrho_1, \ldots, \varrho_m$ Darstellungen von G, und

ϱ lässt sich im Wesentlichen als direkte Summe von $\varrho_1, \ldots, \varrho_m$ auffassen. In solch einem Fall nennt man ϱ reduzibel, andernfalls heißt ϱ irreduzibel. Ist ϱ irreduzibel, so heißt auch χ_ϱ irreduzibel. Die Menge aller irreduziblen Charaktere von G bezeichnen wir mit $\mathrm{Irr}(G)$.

Jede Darstellung lässt sich folglich in eine direkte Summe irreduzibler Darstellungen zerlegen. Des Weiteren kann man zeigen, dass jede irreduzible Darstellung ein direkter Summand der regulären Darstellung $\varrho_{\mathrm{reg}} : G \to \mathrm{GL}(|G|, \mathbb{C})$, $g \mapsto A_g$, ist, wobei A_g für die Matrix der Abbildung $\mathbb{C}G \to \mathbb{C}G$, $x \mapsto gx$ steht. Daher besitzt G nur endlich viele irreduzible Darstellungen. Es lässt sich sogar zeigen, dass eine irreduzible Darstellung vom Grad n genau n-mal als direkter Summand von ϱ_{reg} auftaucht. Daraus schließt man auf die Gleichung

$$|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 \,.$$

Wenn sich eine Darstellung ϱ als Summe von Darstellungen $\varrho_1, \ldots, \varrho_m$ schreiben lässt, so gilt für die entsprechenden Charaktere offenbar $\chi_\varrho = \chi_{\varrho_1} + \ldots + \chi_{\varrho_m}$. Jeder Charakter lässt sich also als Summe irreduzibler Charaktere schreiben. Einen Summanden eines Charakters χ nennen wir auch Konstituente von χ.

Für Klassenfunktionen φ, η von G hat man neben der Addition $(\varphi + \eta)(g) := \varphi(g) + \eta(g)$ für $g \in G$ auch noch eine durch $(\varphi\eta)(g) := \varphi(g)\eta(g)$ gegebene Multiplikation. Sind ϱ_1, ϱ_2 Darstellungen von G, so stimmt der Charakter $\chi_{\varrho_1 \otimes \varrho_2}$ mit dem Produkt der Charaktere χ_{ϱ_1} und χ_{ϱ_2} überein. Das Produkt zweier Charaktere ist also unabhängig davon, ob man es in der Algebra der Klassenfunktionen oder über die Darstellungen der Charaktere berechnet.

Das Produkt zweier Charaktere vom Grad 1, auch lineare Charaktere genannt, ist also wieder ein Charakter vom Grad 1. Zudem besitzt jede Gruppe eine triviale Darstellung $\varrho_{\mathrm{triv}} : G \to G$, $g \mapsto 1$. Den zugehörigen trivialen Charakter bezeichnen wir mit $\mathbb{1}$. Für eine Klassenfunktion φ von G gilt offensichtlich $\varphi\mathbb{1} = \varphi$. Der triviale Charakter ist also das Einselement der $\mathbb{C}$-Algebra der Klassenfunktionen und insbesondere folgt daraus auch, dass die linearen Charaktere eine Gruppe bezüglich der Multiplikation bilden.

Schließlich lässt sich zeigen, dass $|\mathrm{Irr}(G)|$ mit der Anzahl der Konjugationsklassen von G übereinstimmt. Zudem sind die irreduziblen Charaktere von G linear unabhängig über $\mathbb{C}$ und folglich ist $\mathrm{Irr}(G)$ eine Basis der $\mathbb{C}$-Algebra der komplexen Klassenfunktionen von G. Diese Algebra ist mit einem Skalarprodukt $\langle \cdot, \cdot \rangle$ ausgestattet, bezüglich dem die irreduziblen Charaktere eine Orthonormalbasis bilden. Für zwei Klassenfunktionen φ, η wird dieses durch

$$\langle \varphi, \eta \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\overline{\eta(g)}$$

definiert. Insbesondere gilt also

$$\varphi = \sum_{\chi \in \mathrm{Irr}(G)} \langle \varphi, \chi \rangle \chi \,.$$

Zusätzlich dazu gibt es für irreduzible Charaktere χ, ψ auch noch die verallgemeinerte (erste) Orthogonalitätsrelation

$$\frac{1}{|G|}\sum_{g\in G}\chi(gh)\overline{\psi(g)} = \begin{cases}\frac{\chi(h)}{\chi(1)}\,, & \chi = \psi\\ 0\,, & \chi \neq \psi\end{cases}$$

sowie die daraus für Elemente $g, h \in G$ abgeleitete zweite Orthogonalitätsrelation

$$\sum_{\chi\in\mathrm{Irr}(G)}\chi(g)\overline{\chi(h)} = \begin{cases}|C_G(g)|\,, & g \sim h\\ 0\,, & g \nsim h\end{cases}.$$

Auf den komplexwertigen Funktionen von G lässt sich außerdem eine Fourier-Transformation definieren (siehe z. B. [51]). Wir interessieren uns hier nur für den Fall, dass G abelsch ist. In diesem entsprechen die komplexwertigen Funktionen von G den komplexen Klassenfunktionen und die irreduziblen Charaktere von G stehen in Bijektion zu den Elementen von G. Dann wird die Fourier-Transformierte $\hat{f}$ von f durch

$$\hat{f}(\chi) = \sum_{x\in G} f(x)\overline{\chi(x)}$$

für $\chi \in \mathrm{Irr}(G)$ definiert und die inverse Fourier-Transformierte erhält man durch

$$f(x) = \frac{1}{|G|}\sum_{\chi\in\mathrm{Irr}(G)}\hat{f}(\chi)\chi(x)$$

für $x \in G$.

1.2.2 Restriktion, Induktion und Erweiterung von Charakteren

Eine grundlegende Aufgabe in der Charaktertheorie ist es, aus den irreduziblen Charakteren von G die irreduziblen Charaktere von Unter- und Faktorgruppen von G zu gewinnen, bzw. umgekehrt aus der Kenntnis der irreduziblen Charaktere einiger Unter- und Faktorgruppen von G auf die Gestalt der irreduziblen Charaktere von G zu schließen. Sei H eine Untergruppe von G. Für einen irreduziblen Charakter χ von G ist dann natürlich die Restriktion bzw. Einschränkung χ_H von χ auf H ebenfalls ein Charakter, der aber nicht irreduzibel sein muss.

Ist H sogar ein Normalteiler von G, so kann man zumindest noch einiges über die Zerlegung von χ_H in irreduzible Charaktere aussagen. Für eine Klassenfunktion φ von H und ein $g \in G$ sei φ^g die Klassenfunktion mit $\varphi^g(h) := \varphi(ghg^{-1})$ für $h \in H$. Wir sagen, dass φ^g G-konjugiert zu φ ist. Es lässt sich leicht einsehen, dass φ^g genau dann ein Charakter von H ist, wenn dies auch auf φ zutrifft, und ebenso $\varphi^g \in \mathrm{Irr}(H)$ genau dann gilt, wenn auch $\varphi \in \mathrm{Irr}(H)$ ist.

Satz 1.21 (Clifford)**.** *Seien H ein Normalteiler von G, $\chi \in \mathrm{Irr}(G)$ und ψ eine irreduzible Konstituente von χ_H. Die zu ψ in G konjugierten Charaktere seien $\psi = \psi_1, \ldots, \psi_t$. Dann gilt $\chi_H = e \sum_{i=1}^{t} \psi_i$, wobei e mit $\langle \chi_H, \psi \rangle$ übereinstimmt.*

Im noch spezielleren Fall, dass sich G als direktes Produkt $H \times K$ zweier Untergruppen $H, K \leq G$ schreiben lässt, sind die Einschränkungen irreduzibler Charaktere von G auf H bzw. K Vielfache irreduzibler Charaktere von H bzw. K und zu $\psi \in \mathrm{Irr}(H)$ bzw. $\varphi \in \mathrm{Irr}(K)$ existiert ein $\chi \in \mathrm{Irr}(G)$, sodass $\chi_H = \psi$ bzw. $\chi_K = \varphi$ gilt. Umgekehrt gewinnt man die irreduziblen Charaktere von G auch aus denen von H und K. Sind nämlich ψ und φ Klassenfunktionen von H bzw. K, so ist $\chi := \psi \times \varphi$ mit $\chi(hk) = \psi(h)\varphi(k)$, $h \in H$, $k \in K$, eine Klassenfunktion von G. Es lässt sich leicht einsehen, dass χ ein Charakter von G ist, wenn ψ, φ Charaktere von H bzw. K sind.

Proposition 1.22. *Seien H, K endliche Gruppen und $G = H \times K$. Dann sind die Charaktere $\psi \times \varphi$ mit $\psi \in \mathrm{Irr}(H)$ und $\varphi \in \mathrm{Irr}(K)$ genau die irreduziblen Charaktere von G.*

Ein weiterer Fall, in dem alles bekannt ist, ist der des Übergangs von den irreduziblen Charakteren von G zu denen der Faktorgruppe G/N für einen Normalteiler $N \trianglelefteq G$. Für jedes $\chi \in \mathrm{Irr}(G)$ mit $N \subseteq \mathrm{Kern}(\chi) = \{g \in G : \chi(g) = \chi(1)\}$ liegt der durch $\hat{\chi}(gN) := \chi(g)$ definierte Charakter $\hat{\chi}$ in $\mathrm{Irr}(G/N)$. Auf diese Weise lässt sich jeder irreduzible Charakter von G/N gewinnen. Umgekehrt erhält man für $\hat{\chi} \in \mathrm{Irr}(G/N)$ durch die Definition $\chi(g) := \hat{\chi}(gN)$ stets einen irreduziblen Charakter von G. Wählt man speziell $N = G'$, so ergibt sich aus dieser Korrespondenz leicht die folgende Aussage:

Proposition 1.23. *Für die Kommutatorgruppe G' von G gilt*

$$G' = \bigcap_{\lambda \in \mathrm{Irr}(G)} \{\mathrm{Kern}(\lambda) : \lambda(1_G) = 1\} \quad \textit{und}$$
$$|G : G'| = |\{\lambda \in \mathrm{Irr}(G) : \lambda(1_G) = 1\}| .$$

Eine Art Gegenstück zur Einschränkung eines Charakters von G auf eine Untergruppe H ist die Induktion eines Charakters von H nach G.

Definition 1.24. Seien $H \leq G$ und φ eine Klassenfunktion von H. Die nach G induzierte Klassenfunktion φ^G ist definiert durch

$$\varphi^G(g) = \frac{1}{|H|} \sum_{x \in G} \varphi^\circ(xgx^{-1}) ,$$

wobei $\varphi^\circ(h) := \varphi(h)$ für $h \in H$ und $\varphi^\circ(x) := 0$ für $x \notin H$ ist.

Es lässt sich schnell nachrechnen, dass für Klassenfunktionen φ von H und η von G die sogenannte Frobenius-Reziprozität $\langle \varphi^G, \eta \rangle = \langle \varphi, \eta_H \rangle$ gilt. Damit folgt sofort, dass die induzierte Klassenfunktion ψ^G eines Charakters ψ von H ein Charakter von G ist. Natürlich kann man dagegen nicht erwarten, dass für $\psi \in \mathrm{Irr}(H)$ auch $\psi^G \in \mathrm{Irr}(G)$ liegt.

Auch über induzierte Charaktere lässt sich wieder deutlich mehr sagen, wenn man einen Normalteiler $N \trianglelefteq G$ statt einer beliebigen Untergruppe betrachtet. Natürlich kann man aus den irreduziblen Charakteren von N nicht alle irreduziblen Charaktere von G gewinnen, da sich über die Werte auf den in $G \setminus N$ enthaltenden Konjugationsklassen kaum Aussagen treffen lassen. Zumindest eine Teilmenge von $\mathrm{Irr}(G)$ kann man aber über einen kleinen Umweg dennoch bestimmen.

Sei $\vartheta \in \mathrm{Irr}(N)$, dann nennen wir $I_G(\vartheta) := \{g \in G : \vartheta^g = \vartheta\}$ die Trägheitsgruppe von ϑ in G. Offenbar gilt $N \leq I_G(\vartheta)$. Im Fall $I_G(\vartheta) = G$ bezeichnen wir ϑ auch als G-invariant bzw. invariant in G. Die irreduziblen Charaktere von $I_G(\vartheta)$ sind nun diejenigen, durch deren Induktion man Charaktere aus $\mathrm{Irr}(G)$ erhält.

Satz 1.25. *Seien $N \trianglelefteq G$ und $\vartheta \in \mathrm{Irr}(N)$. Wir setzen*

$$\mathcal{I} := \{\psi \in \mathrm{Irr}(I_G(\vartheta)) : \langle \psi_N, \vartheta \rangle \neq 0\} \quad \textit{und} \quad \mathcal{G} := \{\chi \in \mathrm{Irr}(G) : \langle \chi_N, \vartheta \rangle \neq 0\}.$$

Dann ist die Abbildung $\mathcal{I} \to \mathcal{G}$, $\psi \mapsto \psi^G$, eine Bijektion. Außerdem ist ψ die einzige irreduzible Konstituente von ψ^G in $\mathcal{I}$.

Eine Klasse von Gruppen, für die die beschriebenen Verfahren zur Gewinnung der irreduziblen Charaktere bereits ausreichen, ist die der Frobeniusgruppen. Die Gruppe G wird als Frobeniusgruppe bezeichnet, wenn sie eine echte nichttriviale Untergruppe H enthält, sodass $H \cap gHg^{-1} = \{1\}$ für jedes $g \in G \setminus H$ gilt. Dann lässt sich zeigen, dass ein Normalteiler $N \trianglelefteq G$ mit $NH = G$ und $N \cap H = \{1\}$ existiert. Die Untergruppe H wird als Frobeniuskomplement bzw. Komplement von G und der Normalteiler N als Frobeniuskern bzw. Kern von G bezeichnet.

Die irreduziblen Charaktere von G kommen dann auf zwei Weisen zustande. Zum einen erhält man zu jedem irreduziblen Charakter $\hat{\chi}$ von $H \cong G/N$ einen irreduziblen Charakter χ wie oben beschrieben. Zum anderen kann man für jeden nichttrivialen irreduziblen Charakter $\psi \in \mathrm{Irr}(N)$ zeigen, dass $I_G(\psi) = N$ gilt, ψ^G also ein irreduzibler Charakter von G ist. Jeden irreduziblen Charakter von G erhält man durch eine dieser beiden Konstruktionen.

Sei G jetzt wieder eine beliebige endliche Gruppe. Für $N \trianglelefteq G$ und $\vartheta \in \mathrm{Irr}(N)$ hilft Satz 1.25 im Fall $I_G(\vartheta) = G$ nicht weiter, wenn man irreduzible Charaktere von G mittels ϑ konstruieren möchte. Dafür kann man jedoch Glück haben und einen irreduziblen Charakter χ von G erhalten, wenn man $\chi_N = \vartheta$ definiert und für $\chi(g)$, $g \in G \setminus N$, geeignete Werte findet. In so einem Fall nennt man ϑ erweiterbar.

Es gibt eine Reihe von Aussagen dazu, unter welchen Bedingungen sich ein Charakter erweitern lässt. Wir werden später nur die folgende verwenden und beschränken uns deshalb auf diese.

Proposition 1.26. *Sei N ein Normalteiler von G, sodass G/N zyklisch ist. Dann lässt sich jeder G-invariante Charakter $\vartheta \in \mathrm{Irr}(N)$ zu einem irreduziblen Charakter von G erweitern.*

Schließlich stellt sich des Öfteren die Frage, ob eine gegebene Klassenfunktion φ ein Charakter ist oder, falls dies nicht der Fall ist, ob sie zumindest im Ring $R[\mathrm{Irr}(G)]$ für einen gewissen Ring R, der $\mathbb{Z}$ enthält, liegt. Im Fall $R = \mathbb{Z}$ entspricht dieser Ring, wie wir später sehen werden, gerade dem Charakterring von G, auch Ring der virtuellen Charaktere von G genannt. Wir werden uns außerdem für den Fall $R = \mathbb{Z}_{(p)}$, $p \in \mathbb{P}$, interessieren.

Um herauszufinden, ob φ in $R[\mathrm{Irr}(G)]$ liegt, ist es manchmal einfacher zu untersuchen, ob sich φ_H für gewisse Untergruppen $H < G$ in $R[\mathrm{Irr}(H)]$ befindet. Wählt man eine geeignete Familie von Untergruppen von G, so kann man daraus schließen, ob φ in $R[\mathrm{Irr}(G)]$ enthalten ist. Solch eine geeignete Familie sind z. B. die elementaren Untergruppen von G. Vor deren Definition erinnern wir daran, dass eine Gruppe p-Gruppe heißt, wenn ihre Ordnung eine p-Potenz für ein $p \in \mathbb{P}$ ist.

Definition 1.27. Sei $\ell \in \mathbb{P}$. Eine Gruppe E heißt ℓ-elementar, wenn E das direkte Produkt einer zyklischen Gruppe und einer ℓ-Gruppe ist. Weiter heißt E elementar, wenn E eine p-elementare Gruppe für irgendeine Primzahl p ist.

Satz 1.28 (Brauer)**.** *Sei R ein Ring mit $\mathbb{Z} \subseteq R \subseteq \mathbb{C}$. Eine Klassenfunktion φ von G liegt genau dann in $R[\mathrm{Irr}(G)]$, wenn für jede elementare Untergruppe $E \leq G$ die Einschränkung φ_E in $R[\mathrm{Irr}(E)]$ enthalten ist.*

1.2.3 Sektionen und $\mathbb{Q}$-Klassen

Sei $p \in \mathbb{P}$. Dann bezeichnen wir $g \in G$ als p-Element, wenn die Ordnung von g eine p-Potenz ist. Weiter sagen wir, dass g ein p'-Element ist, wenn die Ordnung von g teilerfremd zu p ist. Analog nennen wir g ein π-Element, wenn für $\pi \subseteq \mathbb{P}$ alle Primteiler von $|\langle g \rangle|$ in π liegen bzw. π'-Element, wenn keine Zahl aus π ein Teiler der Ordnung von g ist.

Ein Element $g \in G$ können wir in eindeutiger Weise als Produkt $g = g_p g_{p'}$ schreiben, sodass $g_p g_{p'} = g_{p'} g_p$ gilt, g_p ein p-Element und $g_{p'}$ ein p'-Element aus G ist. Das Element g_p heißt dann p-Anteil und das Element $g_{p'}$ p'-Anteil von g. Analoge Aussagen gelten allgemeiner für den π- und den π'-Anteil von g.

Auf der Gruppe G kann man über den p-Anteil ihrer Elemente eine Äquivalenzrelation definieren. Man sagt, dass $g, h \in G$ genau dann in Relation stehen, wenn ihre p-Anteile in G konjugiert sind. Die Äquivalenzklassen heißen dann p-Sektionen von G. Eine analoge Definition erhält man, wenn man statt dem p- den p'-Anteil der Elemente aus G betrachtet. In diesem Fall nennt man die Äquivalenzklassen dementsprechend p'-Sektionen. Auch diese Definitionen lassen sich auf π- bzw. π'-Sektionen ausdehnen.

Diese Einteilung wird uns später bei der Anwendung lokaler Methoden helfen. Dabei werden wir unter anderem die beiden folgenden Aussagen benötigen.

Lemma 1.29. *Seien* $|G| = mn$ *mit* $\mathrm{ggT}(m,n) = 1$, $\pi := \{p \in \mathbb{P} : p \mid m\}$ *und* $R := \mathbb{Z}[\zeta_n]$. *Für* $g \in G$ *mit* $g = g_{\pi'}$ *werde die Klassenfunktion* ϑ *von* G *durch*

$$\vartheta(x) = \begin{cases} n, & x_{\pi'} \sim g \\ 0, & x_{\pi'} \nsim g \end{cases}$$

definiert. Dann liegt ϑ *in* $R[\mathrm{Irr}(G)]$.

Lemma 1.30. *Seien* $p \in \mathbb{P}$ *und* $\mathfrak{p}$ *ein* p *enthaltendes maximales Ideal in* $\mathbb{Z}[\zeta_{|G|}]$. *Für Elemente* $x, y \in G$ *sind* $x_{p'}$ *und* $y_{p'}$ *genau dann in* G *konjugiert, wenn* $\chi(x) \equiv \chi(y) \pmod{\mathfrak{p}}$ *für jedes* $\chi \in \mathrm{Irr}(G)$ *gilt.*

Für unsere Zwecke wird die Einteilung von G in Konjugationsklassen des Öfteren zu fein sein. Stattdessen werden wir G in sogenannte $\mathbb{Q}$-Klassen unterteilen.

Definition 1.31. Sei $n := \exp(G)$. Zwei Elemente $g, h \in G$ heißen $\mathbb{Q}$-konjugiert in G, wenn es eine zu n teilerfremde ganze Zahl m und ein $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ mit $\sigma(\zeta_n) = \zeta_n^m$ gibt, sodass g zu h^m konjugiert ist. Die Menge aller in G zu g $\mathbb{Q}$-konjugierten Elemente heißt $\mathbb{Q}$-Klasse von g in G.

Der Name $\mathbb{Q}$-Klasse rührt daher, dass Berman allgemein $\mathbb{K}$-Klassen für Körper $\mathbb{K}$ der Charakteristik 0 bzw. mit zu $|G|$ teilerfremder Charakteristik eingeführt hat [1, 2]. Es sei bemerkt, dass der Begriff „rationale Konjugationsklasse“, den man vielleicht intuitiv mit dem Begriff „$\mathbb{Q}$-Klasse“ identifizieren würde, in der Literatur eine andere Bedeutung hat. Als rationale Konjugationsklassen werden Konjugationsklassen bezeichnet, die bereits $\mathbb{Q}$-Klassen sind.

Eine $\mathbb{Q}$-Klasse ist also eine Vereinigung von Konjugationsklassen von G. Die $\mathbb{Q}$-Klassen von G stehen offenbar in Bijektion zu den Konjugationsklassen zyklischer Untergruppen von G.

Wie für Konjugationsklassen lassen sich auch für $\mathbb{Q}$-Klassen Sektionen definieren. Dazu nutzen wir die Operation von $\mathrm{Gal}(\mathbb{Q}(\zeta_{\exp(G)})/\mathbb{Q})$ auf den Konjugationsklassen von G, die durch $\sigma(\mathrm{cl}_G(x)) = \mathrm{cl}_G(x^t)$ für $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{\exp(G)})/\mathbb{Q})$, $x \in G$ und die ganze Zahl t mit $1 \leq t \leq \exp(G)$ sowie $\sigma(\zeta_{\exp(G)}) = \zeta_{\exp(G)}^t$ definiert ist. Ist $\mathcal{S}$ eine Vereinigung von Konjugationsklassen $\mathcal{C}_1, \ldots, \mathcal{C}_k$ von G, so setzen wir entsprechend $\sigma(\mathcal{S}) = \sigma(\mathcal{C}_1) \cup \ldots \cup \sigma(\mathcal{C}_k)$. Damit operiert $\mathrm{Gal}(\mathbb{Q}(\zeta_{\exp(G)})/\mathbb{Q})$ also auch auf den p- bzw. p'-Sektionen von G. Unser Augenmerk wird im Wesentlichen auf den p'-Sektionen liegen.

Definition 1.32. Seien p eine Primzahl, $\mathcal{S}$ eine p'-Sektion von G und außerdem $\mathcal{G} := \mathrm{Gal}(\mathbb{Q}(\zeta_{\exp(G)})/\mathbb{Q})$. Dann nennt man $\bigcup_{\sigma \in \mathcal{G}} \sigma(\mathcal{S})$ eine rationale p'-Sektion von G.

Eine rationale p'-Sektion ist also eine p'-Sektion von $\mathbb{Q}$-Klassen. Der Begriff „rationale p'-Sektion“ wird auch in der Literatur so verwendet, insbesondere enthält eine rationale p'-Sektion in der Regel nicht nur rationale Konjugationsklassen.

Konjugations- wie $\mathbb{Q}$-Klassen kann man auf folgende Weise algebraische Zahlkörper zuordnen. Seien $\mathcal{C}_1, \ldots, \mathcal{C}_k$ die $\mathbb{Q}$-Klassen und $C_1, \ldots, C_l$ die Konjugationsklassen von G, sodass $C_i \subseteq \mathcal{C}_i$ für $1 \leq i \leq k$ gilt. Für ein beliebiges $x_i \in \mathcal{C}_i$ setzen wir dann $\mathbb{Q}(\mathcal{C}_i) := \{\mathbb{Q}(\chi(x_i)) : \chi \in \mathrm{Irr}(G)\}$. Diese Definition ist offenbar repräsentantenunabhängig und es gilt $\mathbb{Q}(\mathcal{C}_i) = \mathbb{Q}(C_i)$, wenn wir für ein beliebiges $y_i \in C_i$ analog $\mathbb{Q}(C_i) := \{\mathbb{Q}(\chi(y_i)) : \chi \in \mathrm{Irr}(G)\}$ setzen. Damit wird $\bigoplus_{i=1}^{k} \mathbb{Q}(\mathcal{C}_i)$ auf natürliche Weise zu einer $\mathbb{Q}$-Algebra.

Zum Grad einer Körpererweiterung $\mathbb{Q}(\mathcal{C}_i)/\mathbb{Q}$ kann man allein durch Informationen über die Struktur von G gelangen. Die Herleitung des folgenden Isomorphismus ist nicht schwer und z. B. in [38] zu finden.

Lemma 1.33. *Sei C eine Konjugationsklasse von G und $x \in C$. Dann gibt es einen kanonischen Isomorphismus zwischen* $\mathrm{Gal}(\mathbb{Q}(\zeta_{|\langle x\rangle|})/\mathbb{Q}(C))$ *und* $N_G(\langle x\rangle)/C_G(x)$.

1.3 Ganze Darstellungen

Die Theorie ganzer Darstellungen lässt sich als Ausweitung der gewöhnlichen bzw. modularen Darstellungstheorie ansehen. Während in Letzterer Moduln über Körpern untersucht werden, befasst man sich in der Theorie zu ganzen Darstellungen mit Moduln über Ringen.

Die Motivation dazu liefert unter anderem das Folgende: Seien $\mathbb{K}$ ein algebraischer Zahlkörper der Charakteristik 0 und R sein Ganzheitsring. Zu einer endlichen Gruppe G fragt man nun nicht nur nach den $\mathbb{K}G$-Moduln, sondern auch nach den sogenannten RG-Gittern, also den RG-Moduln, die als R-Modul projektiv und endlich erzeugt sind. Abhängig von der Gestalt von $\mathbb{K}$ und R treten diese und damit in Zusammenhang stehende Fragen in der modularen Darstellungstheorie, der Zahlentheorie oder auch der algebraischen K-Theorie auf.

Von Gittern spricht man in diesem Zusammenhang, weil man die RG-Moduln als R-Gitter in den als $\mathbb{K}$-Vektorräumen angesehenen $\mathbb{K}G$-Moduln auffassen kann. Ursprünglich stand „Gitter“ für eine diskrete Untergruppe des Vektorraums $\mathbb{R}^n$, die diesen aufspannt. Als Gruppe sind solche Gitter zu $\mathbb{Z}^n$ isomorph, daher rührt der Begriff „Ganze Darstellung“. Im Allgemeinen lässt man jedoch beliebige Körper $\mathbb{L}$ sowie beliebige Teilringe S von $\mathbb{L}$ zu ($S \neq \mathbb{L}$) und definiert als Gitter das S-Erzeugnis einer Basis eines $\mathbb{L}$-Vektorraums. In diesem liegt das Gitter eventuell nicht diskret, trotzdem spricht man auch in diesem Fall von ganzen Darstellungen.

Zur Untersuchung der RG-Moduln erweist es sich als nützlich, R-Ordnungen zu betrachten. Die Theorie zu Ordnungen und Gittern über diesen Ordnungen ist das, was man im Allgemeinen als „Ganze Darstellungstheorie“ versteht.

1.3.1 Ordnungen

In Abschnitt 1.2 wurde auf die Korrespondenz zwischen gewöhnlichen Darstellungen und (freien) $\mathbb{C}G$-Moduln für eine endliche Gruppe G eingegangen. Aus technischer Sicht sowie mit einem Blick auf mögliche Verallgemeinerungen bietet es sich an, projektive Moduln zu betrachten. Ist R ein Ring, so heißt der R-Modul P projektiv, wenn P ein direkter Summand eines freien R-Moduls ist. Es gibt eine Reihe weiterer äquivalenter Definitionen dafür, dass P projektiv ist, wir werden diese aber nicht benötigen. Stattdessen werden wir uns später sogar wieder nur auf freie Moduln konzentrieren.

Definition 1.34. Sei R ein kommutativer Ring mit 1. Dann nennt man einen endlich erzeugten projektiven R-Modul ein R-Gitter.

Im Fall, dass R ein Dedekindring ist, lassen sich die projektiven R-Moduln sehr einfach beschreiben: Ein endlich erzeugter R-Modul M ist genau dann projektiv, wenn er torsionsfrei ist. Dass M torsionsfrei ist, bedeutet dabei, dass für $r \neq 0$ und $m \neq 0$ stets $rm \neq 0$ gilt.

Definition 1.35. Sei R ein Dedekindring mit Quotientenkörper $\mathbb{K}$, A eine endlichdimensionale $\mathbb{K}$-Algebra und $\Lambda \subseteq A$ ein Teilring, der R enthält. Dann nennt man Λ eine R-Ordnung in A, falls Λ ein R-Gitter ist und außerdem $\mathbb{K} \otimes_R \Lambda = A$ gilt.

Beispiele für Ordnungen sind die Ganzheitsringe algebraischer Zahlkörper, genauer ist $\mathcal{O}_{\mathbb{L}}$ eine $\mathbb{Z}$-Ordnung in der $\mathbb{Q}$-Algebra $\mathbb{L}$, wenn $\mathbb{L}$ ein algebraischer Zahlkörper ist. Ebenso ist $\mathbb{Z}[2i]$ eine $\mathbb{Z}$-Ordnung in $\mathbb{Q}(i)$, dagegen ist $\mathbb{Z}$ keine $\mathbb{Z}$-Ordnung in $\mathbb{Q}(i)$. Des Weiteren ist für einen Dedekindring R und eine endliche Gruppe G der Gruppenring RG eine R-Ordnung in der Gruppenalgebra $\mathbb{K}G$, wenn $\mathbb{K}$ der Quotientenkörper von R ist.

Sei jetzt R ein Dedekindring mit Quotientenkörper $\mathbb{K}$ und A eine $\mathbb{K}$-Algebra. Oftmals lassen sich Aussagen über eine R-Ordnung Λ in A nur schwer über deren direkte Betrachtung gewinnen. Stattdessen hilft es oft, Λ in eine maximale R-Ordnung Λ' in A einzubetten und über die leichter verständliche Struktur von Λ' an Eigenschaften von Λ zu gelangen. Dass Λ' maximal ist, bedeutet dabei, dass es keine R-Ordnung in A gibt, die Λ' echt enthält.

Im Allgemeinen kann man nicht von der Existenz maximaler Ordnungen in A ausgehen. Anders sieht es aus, wenn A eine separable Algebra ist, weshalb wir zunächst sagen, was wir unter einer separablen Algebra verstehen.

Definition 1.36. Sei $\mathbb{K}$ ein Körper. Eine $\mathbb{K}$-Algebra A heißt separabel, falls $\mathbb{L} \otimes_{\mathbb{K}} A$ für jede Körpererweiterung $\mathbb{L}/\mathbb{K}$ eine halbeinfache $\mathbb{L}$-Algebra ist.

Um zu entscheiden, ob eine $\mathbb{K}$-Algebra separabel ist, möchte man natürlich nicht die Halbeinfachheit der $\mathbb{L}$-Algebren $\mathbb{L} \otimes_{\mathbb{K}} A$ für jede Körpererweiterung $\mathbb{L}/\mathbb{K}$ nachprüfen. Tatsächlich genügt es bereits, lediglich eine geeignete Körpererweiterung $\mathbb{L}/\mathbb{K}$ zu betrachten.

Lemma 1.37. *Sei $\mathbb{K}$ ein Körper. Eine $\mathbb{K}$-Algebra A ist genau dann separabel, wenn es eine endliche Körpererweiterung $\mathbb{L}/\mathbb{K}$ gibt, sodass $\mathbb{L} \otimes_{\mathbb{K}} A$ eine zerfallende halbeinfache $\mathbb{L}$-Algebra ist.*

Dass die Algebra $\mathbb{L} \otimes_{\mathbb{K}} A$ zerfällt, bedeutet hierbei, dass $\mathbb{L} \otimes_{\mathbb{K}} A$ isomorph zu einer direkten Summe von Matrixalgebren über $\mathbb{L}$ ist.

Ist A eine separable $\mathbb{K}$-Algebra, so haben wir eben schon angedeutet, dass A maximale Ordnungen enthält. Tatsächlich lässt sich in diesem Fall jede R-Ordnung Λ in A in mindestens eine maximale R-Ordnung in A einbetten. Ist R überdies noch kommutativ, kennt man sogar die Struktur der dann einzigen maximalen R-Ordnung in A.

Satz 1.38. *Seien R ein Dedekindring mit Quotientenkörper $\mathbb{K}$ und A eine endlich erzeugte kommutative separable $\mathbb{K}$-Algebra. Dann enthält der ganze Abschluss von R in A jede R-Ordnung in A und ist somit die einzige maximale R-Ordnung in A.*

Die oben angesprochenen Ganzheitsringe algebraischer Zahlkörper sind also gerade die maximalen Ordnungen, wenn man die Zahlkörper als $\mathbb{Q}$-Algebren auffasst.

1.3.2 Der Charakterring einer endlichen Gruppe

Zur Definition des Charakterrings einer endlichen Gruppe benötigen wir den Begriff des Grothendieckrings. Wir schauen uns dazu zunächst an, wie man die Grothendieckgruppe einer kommutativen Halbgruppe explizit konstruiert. Die Grothendieckgruppe ist ein Begriff aus der algebraischen K-Theorie und wird meist über eine universelle Eigenschaft definiert. Wir benötigen jedoch nur die konkrete Konstruktion und diese auch nur für Halbgruppen mit Kürzungseigenschaft. Genaueres zur Grothendieckgruppe im allgemeinen Fall findet man z. B. in [42].

Sei H eine kommutative Halbgruppe mit Kürzungseigenschaft, d. h., für $x, y, z \in H$ folgt aus $x + y = x + z$ stets $y = z$. Dann kann man auf $H \times H$ eine Äquivalenzrelation $\sim$ durch $(x, y) \sim (\tilde{x}, \tilde{y}) \Leftrightarrow x+\tilde{y} = y+\tilde{x}$ definieren, die Äquivalenzklasse von (x, y) sei $[x, y]$. Es lässt sich zeigen, dass $\mathcal{G}(H) := H \times H/\sim$ mit der Verknüpfung $[x_1, y_1] + [x_2, y_2] := [x_1 + x_2, y_1 + y_2]$ zu einer kommutativen Gruppe wird. Diese nennt man die Grothendieckgruppe von H.

Das neutrale Element in $\mathcal{G}(H)$ ist $[x, x]$ (unabhängig von $x \in H$) und für die Inversen gilt $-[x, y] = [y, x]$. Ferner lässt sich H über den injektiven Halbgruppen-Homomorphismus $H \to \mathcal{G}(H)$, $x \mapsto [x + x, x]$ in $\mathcal{G}(H)$ einbetten. Mit dieser Sichtweise kann man für $x, y \in H$

$$x - y = [x + x, x] - [y + y, y] = [x + x, x] + [y, y + y] = [x + x + y, x + y + y] = [x, y]$$

schreiben. Das liefert $\mathcal{G}(H) = \{x - y : x, y \in H\}$.

Ist auf H außerdem noch eine Multiplikation gegeben, H also ein Halbring, so induziert diese eine Multiplikation auf $\mathcal{G}(H)$. Auf diese Weise wird $\mathcal{G}(H)$ zu einem Ring, der Grothendieckring von H genannt wird.

Sei G eine endliche Gruppe. Die Menge der gewöhnlichen Charaktere von G wird mit der in Abschnitt 1.2 definierten Addition und der durch das Tensorprodukt induzierten Multiplikation zu einem Halbring. Der Charakterring $R(G)$ von G ist definiert als Grothendieckring dieses Halbrings. Wie oben beschrieben ist $R(G)$ die Menge aller Differenzen $\chi - \psi$ von Charakteren χ, ψ von G. Da sich jeder Charakter in eindeutiger Weise als Summe irreduzibler Charaktere von G schreiben lässt, gilt offenbar $R(G) = \mathbb{Z}[\mathrm{Irr}(G)]$.

Insbesondere ist der Charakterring also ein kommutativer Ring, dessen Einselement der triviale Charakter $\mathbb{1}$ ist. Weiterhin ist er als $\mathbb{Z}$-Modul frei und endlich erzeugt, wobei die irreduziblen Charaktere von G eine Basis bilden. Damit ist $R(G)$ eine kommutative $\mathbb{Z}$-Ordnung in der Algebra $\mathbb{Q} \otimes_{\mathbb{Z}} R(G)$.

1.3.3 Darstellungen von Ordnungen

Im gesamten Abschnitt bezeichne wieder G eine endliche Gruppe, R einen Dedekindring mit Quotientenkörper $\mathbb{K}$ und A eine $\mathbb{K}$-Algebra.

Definition 1.39. Sei Λ eine R-Ordnung in A. Ein Λ-Gitter ist ein Λ-Modul, der zusätzlich ein R-Gitter ist.

Ein Λ-Gitter, das eine endliche R-Basis besitzt, induziert in gewohnter Weise eine Matrix-Darstellung von Λ. In diesem Fall spricht man auch von einer ganzen Darstellung bzw. einer R-Darstellung von Λ. Umgekehrt erhält man aus jeder R-Darstellung von Λ ein Λ-Gitter. Der Begriff des Darstellungstyps wird für Ordnungen deswegen wie folgt eingeführt.

Definition 1.40. Der Darstellungstyp einer R-Ordnung Λ in A ist endlich, wenn es nur endlich viele Isomorphieklassen von unzerlegbaren Λ-Gittern gibt. Andernfalls hat Λ unendlichen Darstellungstyp.

Eine bekannte Aussage aus der Zahlentheorie ist, dass die Idealklassengruppe von R endlich ist, wenn $\mathbb{K}$ ein algebraischer Zahlkörper oder eine endliche Körpererweiterung des Funktionenkörpers $\mathbb{F}_q(X)$ für eine Primzahlpotenz q ist. In solch einem Fall nennt man $\mathbb{K}$ auch einen globalen Körper. Die folgende Aussage ist die Verallgemeinerung dieses Resultats auf Ordnungen.

Satz 1.41 (Jordan-Zassenhaus)**.** *Seien R ein Dedekindring, dessen Quotientenkörper $\mathbb{K}$ ein globaler Körper ist, A eine endlich-dimensionale halbeinfache $\mathbb{K}$-Algebra und Λ eine R-Ordnung in A. Dann gibt es zu jedem endlich erzeugten A-Modul V nur endlich viele Isomorphieklassen von Λ-Gittern M, sodass $\mathbb{K} \otimes_R M \cong V$ gilt.*

Ein analoger Satz gilt auch, wenn R ein diskreter Bewertungsring und $\mathbb{K}$ die Komplettierung eines globalen Körpers ist.

Ist A nicht halbeinfach, so lässt sich für $R \neq \mathbb{K}$ zeigen, dass es zu jedem A-Modul $V \neq 0$ unendlich viele Isomorphieklassen von Λ-Gittern M mit $\mathbb{K} \otimes_R M \cong V$ gibt. Um zumindest die Gültigkeit des Satzes von Jordan-Zassenhaus zu garantieren, nehmen wir im Folgenden an, dass $\mathbb{K}$ ein globaler Körper oder die Komplettierung eines globalen Körpers und A eine endlich-dimensionale separable Algebra ist.

Die Frage, ob Λ endlichen oder unendlichen Darstellungstyp hat, kann man mittels eines Lokal-Global-Prinzips beantworten. Sei $\mathfrak{p}$ ein maximales Ideal in R, $\mathbb{K}_\mathfrak{p}$ die entsprechende Komplettierung und $\widehat{R}_\mathfrak{p} = \mathcal{O}_{\mathbb{K}_\mathfrak{p}}$. Für eine R-Ordnung Λ in A setzen wir $\widehat{\Lambda}_\mathfrak{p} = \widehat{R}_\mathfrak{p} \otimes_R \Lambda$. Ist Λ' eine maximale R-Ordnung in A, die Λ enthält, so folgt $\widehat{\Lambda}_\mathfrak{p} \subseteq \widehat{\Lambda}'_\mathfrak{p}$. In den meisten Fällen gilt hier sogar Gleichheit, man kann zeigen, dass die Menge

$$S(\Lambda) = \left\{\mathfrak{p} \text{ maximales Ideal in } R : \widehat{\Lambda}_\mathfrak{p} \text{ keine maximale } \widehat{R}_\mathfrak{p}\text{-Ordnung in } \widehat{\mathbb{K}}_\mathfrak{p} \otimes_\mathbb{K} A\right\}$$

eine endliche Menge ist. Ferner gilt genau dann $S(\Lambda) = \emptyset$, wenn Λ eine maximale R-Ordnung in A ist. Die Frage nach dem Darstellungstyp von Λ lässt sich nun auf die Frage nach den Darstellungstypen der Ordnungen $\widehat{\Lambda}_\mathfrak{p}$ für die $\mathfrak{p} \in S(\Lambda)$ reduzieren:

Satz 1.42 (Jones)**.** *Eine R-Ordnung Λ in A hat genau dann endlichen Darstellungstyp, wenn für jedes $\mathfrak{p} \in S(\Lambda)$ die Ordnung $\widehat{\Lambda}_\mathfrak{p}$ endlichen Darstellungstyp hat.*

Für den Gruppenring $\mathbb{Z}G$ erhält man z. B $S(\mathbb{Z}G) = \{(p) : p \in \mathbb{P},\, p \mid |G|\}$. Ist allgemeiner $\mathcal{O}_\mathbb{L}$ der Ganzheitsring eines algebraischen Zahlkörpers $\mathbb{L}$, so besteht $S(\mathcal{O}_\mathbb{L}G)$ aus den maximalen Idealen, die $|G|$ enthalten. Für ein Primideal $\mathfrak{p} \in S(\mathcal{O}_\mathbb{L}G)$, das die Primzahl $p \in \mathbb{P}$ enthält, lässt sich der Darstellungstyp von $\widehat{\mathcal{O}_\mathbb{L}G}_\mathfrak{p}$ in Abhängigkeit von den p-Sylowgruppen von G und dem Verzweigungsindex $e(\mathfrak{p}/(p))$ bestimmen. Beispielsweise hat $\mathbb{Z}G$ genau dann endlichen Darstellungstyp, wenn für jeden Primteiler p von $|G|$ die p-Sylowgruppen zyklisch der Ordnung höchstens p^2 sind.

Bei der Bestimmung des Darstellungstyps von $\mathbb{Z}_pG$ wird von der Tatsache Gebrauch gemacht, dass $\mathbb{Z}_pG$ genau dann endlichen Darstellungstyp hat, wenn $\mathbb{Z}_pP$ für eine p-Sylowgruppe P endlichen Darstellungstyp hat. Eine ähnliche Reduktion ist für den Charakterring von G im Allgemeinen nicht möglich. Dafür ist $R(G)$ stets eine kommutative Ordnung und bei der Bestimmung des Darstellungstyps kommutativer Ordnungen hilft ein tiefliegender, unabhängig von Jacobinski sowie von Drozd und Roĭter bewiesener Satz.

Sei S ein beliebiger Ring und X ein endlich erzeugter S-Modul. Das Jacobson-Radikal $\mathrm{rad}_S(X)$ bzw. $\mathrm{rad}(X)$ von X ist der Durchschnitt aller maximalen S-Untermoduln von X. Ferner bezeichne $\mu_S(X)$ die minimale Anzahl von Erzeugern von X als S-Modul.

Satz 1.43 (Jacobinski, Drozd-Roĭter)**.** *Seien A kommutativ, Λ eine R-Ordnung und Λ' die maximale R-Ordnung in A. Die Ordnung Λ hat genau dann endlichen Darstellungstyp, wenn gilt:*

$$\mu_\Lambda(\Lambda'/\Lambda) \leq 2 \qquad \textit{und} \qquad \mu_\Lambda(\mathrm{rad}_\Lambda(\Lambda'/\Lambda)) \leq 1\,.$$

In [14] wird ein Überblick über den Beweis des Satzes gegeben. Vollständige Beweise über teilweise verschiedene Zugänge findet man in [33], [18] oder [24].

Eine Strategie zur Bestimmung des Darstellungstyps einer kommutativen Ordnung Λ lautet also wie folgt: Für $\mathfrak{p} \in S(\Lambda)$ bestimme man den Darstellungstyp von $\widehat{\Lambda}_\mathfrak{p}$ mithilfe von Satz 1.43 und schließe daraus mit Satz 1.42 auf den Darstellungstyp von Λ. Eine Variante dieses Vorgehens ist, statt der $\widehat{R}_\mathfrak{p}$-Ordnung $\widehat{\Lambda}_\mathfrak{p}$ die $R_\mathfrak{p}$-Ordnung $\Lambda_\mathfrak{p} := R_\mathfrak{p} \otimes_R \Lambda$ zu betrachten, also mit Lokalisierungen statt Komplettierungen zu arbeiten. Wann dies genügt, zeigt das folgende Resultat aus [41].

Folgerung 1.44 (Reichenbach)**.** *Sei R ein Dedekindring, dessen Quotientenkörper $\mathbb{K}$ ein globaler Körper oder die Komplettierung eines globalen Körpers ist. Sei A eine separable kommutative endlich-dimensionale $\mathbb{K}$-Algebra und Λ eine R-Ordnung in A. Sei $a \in R$ so, dass $a\Lambda' \subseteq \Lambda$ für die maximale R-Ordnung Λ' in A gilt. Die Ordnung Λ hat genau dann endlichen Darstellungstyp, wenn für jedes Primideal $\mathfrak{p}$ in R, welches aR enthält, die $R_\mathfrak{p}$-Ordnung $\Lambda_\mathfrak{p}$ endlichen Darstellungstyp hat.*

Mit den obigen Aussagen lässt sich der Darstellungstyp des Gruppenrings $\mathbb{Z}G$ bestimmen, wenn G abelsch ist. Da $\mathbb{Z}G \cong R(G)$ ist, kennt man also den Darstellungstyp des Charakterrings einer endlichen abelschen Gruppe. Ebenso lässt sich der Darstellungstyp des Burnsiderings $A(G)$ einer beliebigen endlichen Gruppe G über die Sätze 1.43 und 1.42 (bzw. Folgerung 1.44) ermitteln. Dieser ist definiert als Grothendieckring des Halbrings der Isomorphieklassen endlicher G-Mengen, wobei die Addition durch die disjunkte Vereinigung und die Multiplikation durch das direkte Produkt gegeben werden. Im Gegensatz zum Gruppenring kennt man für den Burnsidering kein Verfahren, mit dem man dessen Darstellungstyp ohne die Verwendung von Satz 1.43 bestimmen kann.

Es gibt ein Kriterium dafür, wann genau der Darstellungstyp von $A(G)$ endlich ist. Dieses lässt sich aber nicht allein über die p-Sylowgruppen von G beschreiben (siehe [40]). Hat $A(G)$ endlichen Darstellungstyp, so sind für $p \in \mathbb{P}$ die p-Sylowgruppen von G zyklisch der Ordnung höchstens p^2 oder elementar-abelsch der Ordnung p^2 und alle zyklischen Untergruppen der Ordnung p in G sind konjugiert. Die Umkehrung dieser Aussage stimmt allerdings nicht. Das lässt erahnen, dass auch die Bestimmung des Darstellungstyps vom Charakterring $R(G)$ für einige Gruppen G problematisch werden kann.

1.4 Endliche Gruppen

Die Theorie zu endlichen Gruppen ist so vielfältig und weitverzweigt, dass eine in sich geschlossene Übersicht an dieser Stelle nicht möglich ist. Häufig verwendete Begriffe und Resultate wie Sylowsätze, elementare Ergebnisse zu Gruppenoperationen oder auch den Satz von Feit und Thompson, dass jede endliche Gruppe ungerader Ordnung auflösbar ist, setzen wir als bekannt voraus. Wir werden später einige spezielle Ergebnisse aus verschiedenen Bereichen der Gruppentheorie benötigen und beschränken uns daher im Wesentlichen auf die Angabe dieser Resultate. Zum Beweis der Sätze in Abschnitt 1.4.2 benötigt man die Klassifikation der endlichen einfachen Gruppen.

Alle in diesem Abschnitt betrachteten Gruppen sind endliche Gruppen. Für eine zyklische Gruppe der Ordnung n schreiben wir auch C_n, direkte Produkte von k zyklischen Gruppen der Ordnung n, auch homozyklische Gruppen genannt, werden wir mit C_n^k bezeichnen (für $n \in \mathbb{P}$ sprechen wir auch von elementar-abelschen Gruppen). Außerdem sei D_n die Diedergruppe der Ordnung n und Q_8 die Quaternionengruppe der Ordnung 8.

Sei G eine Gruppe und $p \in \mathbb{P}$. Der größte Normalteiler von G, dessen Ordnung eine p-Potenz ist, wird mit $O_p(G)$ bezeichnet und analog ist $O_{p'}(G)$ der größte Normalteiler von G mit zu p teilerfremder Ordnung. Die Fittinggruppe $F(G)$ von G ist der größte nilpotente Normalteiler von G. Bekanntlich kommutieren Normalteiler mit teilerfremder Ordnung, weswegen man die Fittinggruppe auch als $F(G) = \prod_{p||G|} O_p(G)$ schreiben kann. Ist $G \neq 1$ auflösbar, so gilt daher $F(G) \neq 1$.

Eine ähnliche Rolle wie die Fittinggruppe für eine endliche auflösbare Gruppe spielt die verallgemeinerte Fittinggruppe für eine beliebige endliche Gruppe G. Bevor wir diese definieren können, müssen wir noch sagen, was wir unter einer Komponente von G verstehen. Eine Gruppe H heißt quasieinfach, wenn H eine perfekte zentrale Erweiterung einer nichtabelschen einfachen Gruppe S ist, d. h. $H = H'$ und $H/Z(H) \cong S$ gilt. Als Komponenten von G werden die subnormalen quasieinfachen Untergruppen von G bezeichnet. Für das Erzeugnis aller Komponenten von G schreiben wir $E(G)$. Damit ist $E(G)$ offenbar ein Normalteiler von G.

Die verallgemeinerte Fittinggruppe $F^*(G)$ ist durch $F^*(G) = F(G)E(G)$ definiert. Folglich gilt $F^*(G) \neq 1$ für $G \neq 1$. Je zwei Komponenten von G kommutieren miteinander und außerdem kommutiert jede Komponente auch mit $F(G)$. Die verallgemeinerte Fittinggruppe ist also eine zentrale Erweiterung eines direkten Produkts von p-Gruppen und einfachen Gruppen. Eine wichtige Eigenschaft sowohl der Fitting- (im Fall G auflösbar) als auch der verallgemeinerten Fittinggruppe von G ist, dass beide ihren Zentralisator in G enthalten, d. h., es gilt $C_G(F(G)) \leq F(G)$, wenn G auflösbar ist, und allgemein $C_G(F^*(G)) \leq F^*(G)$.

Als nächstes wenden wir uns den extraspeziellen p-Gruppen zu. Es sei bemerkt, dass für eine nichtabelsche p-Gruppe P stets $Z(P) \cap P' \neq 1$ gilt. Ist außerdem $\Phi(P)$ die Frattinigruppe von P, also der Durchschnitt aller maximaler Untergruppen von P, so gilt weiter $P' \subseteq \Phi(P)$. Die Gruppe P heißt speziell, wenn diese drei charakteristischen Untergruppen übereinstimmen, d. h. $Z(P) = P' = \Phi(P)$. Des Weiteren heißt P extraspeziell, wenn P speziell ist und außerdem $|Z(P)| = p$ gilt.

Die extraspeziellen p-Gruppen zerfallen für jede Primzahl p in zwei unendliche Serien. Die folgende Beschreibung genügt für unsere Belange, es lassen sich auch genauere angeben.

Satz 1.45. *Sei $p \in \mathbb{P}$. Dann hat jede extraspezielle p-Gruppe die Ordnung p^{2n+1} für eine positive ganze Zahl n. Bis auf Isomorphie gibt es dabei genau zwei extraspezielle p-Gruppen der Ordnung p^{2n+1}. Ist p ungerade, so hat eine dieser beiden Gruppen den Exponenten p, die andere den Exponenten p^2. Die extraspeziellen Gruppen gerader Ordnung haben alle den Exponenten 4.*

1.4.1 Suzuki 2-Gruppen

Die Suzuki 2-Gruppen wurden von Higman in [28] eingeführt. Die Motivation dazu erhielt er durch Suzukis Untersuchungen zu einer anderen Klasse von Gruppen, den sogenannten ZT-Gruppen (siehe [49]). Higmans Interesse galt der Klassifikation aller 2-Gruppen, die einen Automorphismus besitzen, der deren Involutionen, also ihre Elemente der Ordnung 2, transitiv permutiert. Dies trifft natürlich zunächst einmal auf alle 2-Gruppen zu, die nur eine Involution besitzen. Diese Gruppen haben die folgende Gestalt.

Satz 1.46 (Burnside)**.** *Sei P eine 2-Gruppe, die lediglich eine Involution besitzt. Dann ist P isomorph zu einer zyklischen Gruppe oder einer verallgemeinerten Quaternionengruppe.*

Eine verallgemeinerte Quaternionengruppe ist dabei eine zu

$$\langle x, y : x^{2n} = y^4 = 1,\, x^n = y^2,\, yxy^{-1} = x^{-1} \rangle$$

für ein $n \geq 2$ isomorphe Gruppe. Für $n = 2$ erhält man die Quaternionengruppe Q_8.

Weiter lässt sich leicht zeigen, dass die abelschen Gruppen, die mehr als eine Involution und einen Automorphismus wie oben beschrieben besitzen, genau die (nichtzyklischen) homozyklischen 2-Gruppen sind. Die Suzuki 2-Gruppen werden deshalb wie folgt definiert.

Definition 1.47. Eine nichtabelsche 2-Gruppe P heißt Suzuki 2-Gruppe, wenn P mehr als eine Involution besitzt und es eine zyklische Untergruppe ungerader Ordnung von $\mathrm{Aut}(P)$ gibt, die die Involutionen von P transitiv permutiert.

Die Voraussetzung, dass es eine zyklische Untergruppe von $\mathrm{Aut}(P)$ gibt, die die Involutionen von P transitiv permutiert, könnte man noch deutlich abschwächen und würde trotzdem genau dieselbe Klasse von Gruppen definieren.

Satz 1.48 (Thompson)**.** *Sei G eine auflösbare Gruppe und P eine 2-Sylowgruppe von G, die mehr als eine Involution besitzt. Sind alle Involutionen in G konjugiert, so ist P isomorph zu einer homozyklischen Gruppe oder einer Suzuki 2-Gruppe.*

Interessanterweise wären ähnliche Definitionen für p-Gruppen mit einer ungeraden Primzahl p nicht sinnvoll. In diesen Fällen gäbe es solche Gruppen nämlich gar nicht [45]:

Satz 1.49 (Shult)**.** *Sei $p \in \mathbb{P}$ und P eine p-Gruppe, sodass $\mathrm{Aut}(P)$ transitiv auf den Untergruppen der Ordnung p von P operiert. Dann ist P abelsch oder eine 2-Gruppe.*

Es lässt sich zeigen, dass jede Suzuki 2-Gruppe eine spezielle Gruppe vom Exponenten 4 ist, deren nichttriviale Zentrumselemente genau ihre Involutionen sind. Ist P eine Suzuki 2-Gruppe mit $|Z(P)| = q$, so gilt außerdem $|P| = q^2$ oder $|P| = q^3$.

Eine weitere Eigenschaft, die allen Suzuki 2-Gruppen gemein ist, betrifft deren Automorphismen. Ist G eine Gruppe mit einer abelschen p-Sylowgruppe P ($p \in \mathbb{P}$), so sind zwei Elemente aus P nach einem Satz von Burnside genau dann in G konjugiert, wenn sie bereits in $N_G(P)$ konjugiert sind. Dieselbe Aussage gilt auch, wenn P keine abelsche, sondern eine Suzuki 2-Gruppe ist. Dieses Resultat wird in der Sprache der Fusionssysteme z. B. in [12] bewiesen. Man sagt auch, dass abelsche Gruppen und Suzuki 2-Gruppen resistent sind (tatsächlich ist dies noch eine etwas stärkere Formulierung).

Die Suzuki 2-Gruppen lassen sich in vier Typen einteilen. Wie diese Einteilung genau verläuft, erfährt man z. B. in [28]. Die Gruppen vom Typ A sind beispielsweise genau die Suzuki 2-Gruppen P, für die $|P| = |Z(P)|^2$ gilt. Jede dieser Gruppen ist isomorph zu einer der Matrizengruppen

$$A(n,\Theta) := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & a^\Theta \\ 0 & 0 & 1 \end{pmatrix} : a, b \in \mathbb{F}_{2^n} \right\}$$

für eine positive ganze Zahl n und ein nichttriviales $\Theta \in \mathrm{Aut}(\mathbb{F}_{2^n})$ mit ungerader Ordnung. Zu den Gruppen vom Typ B gehören unter anderem die 2-Sylowgruppen der einfachen projektiven speziellen unitären Gruppen $\mathrm{PSU}(3, 2^k)$. (Für $k = 1$ ist die Gruppe $\mathrm{PSU}(3, 2^k)$ nicht einfach und ihre 2-Sylowgruppe ist zu Q_8 isomorph).

Die Suzuki 2-Gruppen vom Typ A und die 2-Sylowgruppen von $\mathrm{PSU}(3, 2^k)$ spielen in einem weiteren Satz, in dem es um transitive Operationen geht, eine Rolle. Fordert man, dass nicht wie bei Suzuki 2-Gruppen nur alle Involutionen einer 2-Gruppe P, sondern sämtliche zyklische Untergruppen gleicher Ordnung von P in $\mathrm{Aut}(P)$ konjugiert sind, so gelangt man schließlich zur folgenden Liste [54].

Satz 1.50 (Wilkens)**.** *Sei P eine 2-Gruppe, in der zu je zwei zyklischen Untergruppen A und B derselben Ordnung ein Automorphismus $\alpha \in \mathrm{Aut}(P)$ existiert, sodass $\alpha(A) = B$ gilt. Dann trifft einer der folgenden Fälle zu:*

1. *P ist homozyklisch,*
2. *P ist isomorph zu einer Suzuki 2-Gruppe vom Typ A,*
3. *P ist isomorph zu einer 2-Sylowgruppe von $\mathrm{PSU}(3, 2^k)$ für ein $k \in \mathbb{N}$,*
4. *P ist isomorph zur Suzuki 2-Gruppe $\langle x_1, x_2, x_3, x_4, x_5, x_6\rangle$ der Ordnung 2^9 mit $x_i^4 = [x_i^2, x_j] = 1$ und $x_1^2 = x_4^2 = [x_1, x_4]$, $x_2^2 = x_5^2 = [x_2, x_5]$, $x_1^2x_2^2 = x_3^2 = x_6^2 = [x_3, x_6]$, $[x_1, x_3] = x_2^2[x_1, x_2] = [x_1, x_5]$, $[x_1, x_6] = x_1^2$, $[x_2, x_3] = x_1^2x_2^2 = [x_5, x_6]$, $[x_2, x_4] = x_2^2$, $[x_2, x_6] = x_1^2x_2^2[x_1, x_2] = [x_3, x_4]$, $[x_3, x_5] = [x_1, x_2] = [x_4, x_5]$.*

1.4.2 Endliche einfache Gruppen

Die Klassifikation der endlichen einfachen Gruppen erforderte eine Vielzahl von Arbeiten. Mittlerweile wird es im Allgemeinen als bewiesen angesehen, dass jede endliche einfache Gruppe isomorph zu einer der folgenden ist:

1. einer zyklischen Gruppe der Ordnung p für ein $p \in \mathbb{P}$,
2. einer alternierenden Gruppe A_n vom Grad $n \geq 5$,
3. einer Gruppe aus einer der 16 unendlichen Serien von einfachen Gruppen vom Lie-Typ, die sich über sogenannte Dynkin-Diagramme klassifizieren lassen,
4. einer von 26 sporadischen einfachen Gruppen.

Wir bezeichnen die nichtabelschen einfachen Gruppen in folgender Weise: Für die projektiven speziellen linearen Gruppen vom Grad n über einem endlichen Körper mit p^k Elementen schreiben wir $\mathrm{PSL}(n, p^k)$ und analog für die projektiven symplektischen Gruppen $\mathrm{PSp}(n, p^k)$. Die projektiven speziellen unitären Gruppen von Grad n über einem Körper mit p^{2k} Elementen bezeichnen wir, wie in der Literatur oft üblich, mit $\mathrm{PSU}(n, p^k)$. Alle anderen auftretenden einfachen Gruppen erhalten die Bezeichnung, unter der sie auch im Atlas [9] zu finden sind, die weiteren Gruppen vom Lie-Typ werden wir also nach den jeweils zugehörigen Dynkin-Diagrammen benennen.

Zu einer endlichen Gruppe lässt sich ihr Schur-Multiplikator definieren. Dieser wurde ursprünglich im Zusammenhang mit projektiven gewöhnlichen Darstellungen eingeführt (siehe z. B. [32]). Wir werden jedoch nur auf Schur-Multiplikatoren endlicher einfacher Gruppen zu sprechen kommen, und zwar wenn es darum geht, welche perfekten zentralen Erweiterungen gewisse einfache Gruppen haben können. Deshalb führen wir ihn wie folgt ein. Sei G einfach, dann gibt es eine bis auf Isomorphie eindeutig bestimmte maximale perfekte zentrale Erweiterung C von G. Die Untergruppe $Z(C)$ wird Schur-Multiplikator $M(G)$ von G genannt.

Die Schur-Multiplikatoren der endlichen einfachen Gruppen sind allesamt bekannt, man findet sie z. B. in [9]. Insbesondere weiß man, dass der Exponent von $M(G)$ die Ordnung von G teilt. Diese Aussage bleibt auch richtig, wenn man den Schur-Multiplikator für eine beliebige endliche Gruppe G definiert.

Unser nächster Blick gilt den Automorphismen einfacher Gruppen. Für eine beliebige Gruppe G bezeichne $\mathrm{Aut}(G)$ die Gruppe der Automorphismen von G und

$$\mathrm{Inn}(G) := \{\varphi \in \mathrm{Aut}(G) : \text{es gibt ein } g \in G, \text{ sodass } \varphi(x) = gxg^{-1} \text{ für alle } x \in G\}$$

den darin enthaltenen Normalteiler der inneren Automorphismen von G. Die äußere Automorphismengruppe von G ist $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$. Über deren Struktur weiß man für einfache Gruppen G Folgendes:

Satz 1.51 (Schreier-Vermutung)**.** *Die äußere Automorphismengruppe einer endlichen einfachen Gruppe ist auflösbar.*

Eine weitere Klassifikationsaussage, die man mithilfe der Klassifikation der endlichen einfachen Gruppen beweisen kann, betrifft die 2-transitiven Gruppen (siehe [31, 27, 13]). Wir werden diese Klassifikation nur für die transitiven linearen Gruppen benötigen, also die Untergruppen von $\mathrm{GL}(n,p)$, die transitiv auf den Vektoren $\neq 0$ von $\mathbb{F}_p^n$ operieren ($p \in \mathbb{P}$, $n \in \mathbb{N}$ beliebig). Im Zusammenhang damit führen wir noch die semilineare Gruppe $\Gamma\mathrm{L}(p^k)$ über einem Körper mit p^k Elementen ein. Diese entsteht durch Erweiterung der allgemeinen linearen Gruppe $\mathrm{GL}(1,p^k)$ mit Galois-Automorphismen, genauer ist

$$\Gamma\mathrm{L}(p^k) = \{f \in \mathrm{Hom}(\mathbb{F}_{p^k}, \mathbb{F}_{p^k}) : f(x) = a\sigma(x) \text{ für gewisse } a \in \mathbb{F}_{p^k}^\times \text{ und } \sigma \in \mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)\}.$$

Die Gruppe $\Gamma\mathrm{L}(p^k)$ besitzt den Normalteiler

$$\Gamma\mathrm{L}_0(p^k) = \{f \in \mathrm{Hom}(\mathbb{F}_{p^k}, \mathbb{F}_{p^k}) : f(x) = ax \text{ für ein } a \in \mathbb{F}_{p^k}^\times\} \cong \mathbb{F}_{p^k}^\times$$

und für die Faktorgruppe gilt $\Gamma\mathrm{L}(p^k)/\Gamma\mathrm{L}_0(p^k) \cong \mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)$. Daher ist $\Gamma\mathrm{L}(p^k)$ isomorph zum semidirekten Produkt $\mathbb{F}_{p^k}^\times \rtimes \mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p)$.

Satz 1.52. *Sei $H \leq \mathrm{GL}(n,p)$ eine Untergruppe, die transitiv auf den Vektoren von $\mathbb{F}_p^n \setminus \{0\}$ operiert. Dann ist H isomorph zu einer Gruppe G, auf die eine der folgenden Aussagen zutrifft:*

1. *$G \leq \Gamma\mathrm{L}(p^n)$,*
2. *$\mathrm{SL}(k,q) \trianglelefteq G$ und $p^n = q^k$ für ein $k \in \mathbb{N}$ mit $k > 1$,*
3. *$\mathrm{Sp}(k,q) \trianglelefteq G$ und $p^n = q^k$ für ein $k \in 2\mathbb{N}$,*
4. *$G_2(q)' \trianglelefteq G$, $p = 2$ und $2^n = q^6$,*
5. *$p = 3$, $n = 2$ und $Q_8 \trianglelefteq G$*
6. *$n = 2$, $p \in \{5, 7, 11, 23\}$ und $\mathrm{SL}(2,3) \trianglelefteq G$,*
7. *$n = 2$, $p \in \{11, 19, 29, 59\}$ und $\mathrm{SL}(2,5) \trianglelefteq G$,*
8. *$p = 3$, $n = 4$ und entweder $S \trianglelefteq G$ für eine extraspezielle Gruppe S der Ordnung 32 oder $\mathrm{SL}(2,5) \trianglelefteq G$,*
9. *$p = 2$, $n = 4$ und $G \cong A_6$ oder $G \cong A_7$,*
10. *$p = 3$, $n = 6$ und $G \cong \mathrm{SL}(2,13)$,*
11. *$p = 2$, $n = 6$ und $G \cong \mathrm{PSU}(3,3)$.*

Schließlich geben wir noch zwei Resultate zu den Konjugationsklassen von Involutionen einfacher Gruppen an. Beide Ergebnisse sind in [56] zu finden.

Satz 1.53. *Sei G eine nichtabelsche einfache Gruppe, in der alle Involutionen konjugiert sind. Dann ist G isomorph zu einer der Gruppen aus der folgenden Liste:*

(i) Alternierende Gruppen: A_5, A_6, A_7;

(ii) Gruppen vom Lie-Typ: $\mathrm{PSL}(2,q)$, $\mathrm{PSL}(3,q)$, $\mathrm{PSL}(4,q)$, $\mathrm{PSU}(3,q)$, $\mathrm{PSU}(4,q)$, ${}^3D_4(q)$, $G_2(q)$, ${}^2G_2(3^{2n+1})$, ${}^2B_2(2^{2n+1})$;

(iii) Sporadische Gruppen: M_{11}, M_{22}, M_{23}, J_1, J_3, McL, $O'N$, Ly, Th.

Satz 1.54. *Sei G eine einfache Gruppe, die mindestens zwei Konjugationsklassen von Involutionen besitzt. Dann sind die Involutionen von G nicht alle* $\mathrm{Aut}(G)$*-konjugiert.*

2 Eigenschaften des Charakterrings und seiner maximalen Ordnung

Ab jetzt bezeichne G stets eine endliche Gruppe. Weiter seien $R(G)$ ihr Charakterring und $R(G)'$ die maximale Ordnung in $\mathbb{Q} \otimes R(G)$ (sofern nichts anderes gesagt wird, meinen wir immer Tensorprodukte über $\mathbb{Z}$). Unser Ziel wird es sein, den Darstellungstyp von $R(G)$ zu bestimmen. Dies wollen wir mittels Anwendung von Folgerung 1.44, wobei wir $R = \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}$ und $\Lambda = R(G)$ setzen, erreichen. Demnach müssen wir also für gewisse Primzahlen p den Darstellungstyp der $\mathbb{Z}_{(p)}$-Ordnung $R(G)_p := \mathbb{Z}_{(p)} \otimes R(G)$ bestimmen, was wir durch Anwendung von Satz 1.43 mit $R = \mathbb{Z}_{(p)}$, $\mathbb{K} = \mathbb{Q}$ und $\Lambda = R(G)_p$ tun wollen. Die meisten Voraussetzungen von Satz 1.43 und Folgerung 1.44 sind dann trivialerweise erfüllt. Es verbleibt lediglich zu zeigen, dass $\mathbb{Q} \otimes R(G)$ und $\mathbb{Q} \otimes_{\mathbb{Z}_{(p)}} R(G)_p$ separabel sind sowie dass eine ganze Zahl a existiert, sodass $aR(G)' \subseteq R(G)$ gilt.

Lemma 2.1. *Die Algebren $\mathbb{Q} \otimes R(G)$ und $\mathbb{Q} \otimes_{\mathbb{Z}_{(p)}} R(G)_p$, $p \in \mathbb{P}$, sind separabel.*

Beweis. Laut Deiml ist die Algebra $\mathbb{Q}(\zeta_{|G|}) \otimes R(G)$ eine zerfallende halbeinfache $\mathbb{Q}(\zeta_{|G|})$-Algebra [15, Satz 3.2]. Nach Lemma 1.37 sind $\mathbb{Q} \otimes R(G)$ und $\mathbb{Q} \otimes R(G)_p$ folglich separabel. □

Lemma 2.2. *Für den Charakterring $R(G)$ und seine maximale Ordnung $R(G)'$ in $\mathbb{Q} \otimes R(G)$ gilt $|G|R(G)' \subseteq R(G)$.*

Beweis. Sei $\varepsilon = \zeta_{\exp(G)}$. Wir zeigen, dass für jede Klassenfunktion $\varphi \in (\mathbb{Z}[\varepsilon] \otimes R(G))'$ die Funktion $|G|\varphi$ in $\mathbb{Z}[\varepsilon] \otimes R(G)$ liegt. Dazu genügt es zu zeigen, dass für ein beliebiges $g \in G$ die Funktion $|G|\vartheta_g$ mit

$$\vartheta_g(x) = \begin{cases} 1, & x \sim_G g \\ 0, & \text{sonst} \end{cases}$$

in $\mathbb{Z}[\varepsilon] \otimes R(G)$ liegt. Mithilfe der Orthogonalitätsrelationen lässt sich ϑ_g leicht angeben:

$$\vartheta_g = \frac{1}{|C_G(g)|} \sum_{\chi \in \mathrm{Irr(G)}} \chi(g^{-1})\chi\,.$$

Daraus liest man sofort $|G|\vartheta_g \in \mathbb{Z}[\varepsilon] \otimes R(G)$ ab. Demzufolge gilt $|G|(\mathbb{Z}[\varepsilon] \otimes R(G))' \subseteq \mathbb{Z}[\varepsilon] \otimes R(G)$ und daher natürlich auch $|G|R(G)' \subseteq R(G)$. □

Folgerung 2.3. *Es gilt $|G|R(G)'_p \subseteq R(G)_p$.*

Mit den Bezeichnungen aus dem Beweis von Lemma 2.2 erhält man für die Funktion $\vartheta_1 \in R(G)'$

$$\vartheta_1 = \frac{1}{|C_G(1)|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi = \frac{1}{|G|} \cdot \mathbb{1} + \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)\setminus\{\mathbb{1}\}} \chi(1)\chi\,,$$

wobei $\mathbb{1}$ für den trivialen Charakter von G steht. Folglich ist jedes $a \in \mathbb{N}$, das $aR(G)' \subseteq R(G)$ erfüllt, mindestens so groß wie $|G|$. Mittels Lemma 2.2 lässt sich nun auch eine Aussage darüber treffen, für welche Primzahlen p man den Darstellungstyp der $\mathbb{Z}_{(p)}$-Ordnung $R(G)_p$ bestimmen muss, um auf den Darstellungstyp von $R(G)$ schließen zu können: Es sind genau die Primteiler von $|G|$.

Im Allgemeinen lassen sich über die genaue Struktur des Charakterrings $R(G)$ nur wenige Aussagen treffen. Die maximale Ordnung $R(G)'$ können wir dagegen als direkte Summe von Ganzheitsringen gewisser algebraischer Zahlkörper schreiben.

Definition 2.4. Sei $\mathcal{S}$ eine Vereinigung von $\mathbb{Q}$-Klassen von G. Für einen Ring T algebraischer Zahlen definiert man

$$\mathrm{Ch}_T(\mathcal{S}) := \left\{ \psi = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \chi : a_\chi \in T,\ \psi(z) = 0 \text{ für } z \notin \mathcal{S} \right\}.$$

Ferner sei $\mathrm{Ch}(\mathcal{S}) := \mathrm{Ch}_{\mathbb{Z}}(\mathcal{S})$.

Satz 2.5. *Seien $\mathcal{C}_1, \ldots, \mathcal{C}_k$ die $\mathbb{Q}$-Klassen von G und $\{x_1, \ldots, x_k\}$ ein Repräsentantensystem dieser $\mathbb{Q}$-Klassen mit $x_i \in \mathcal{C}_i$ für $i = 1, \ldots, k$. Dann ist die Abbildung*

$$\mathbb{Q} \otimes R(G) \to \bigoplus_{i=1}^{k} \mathbb{Q}(\mathcal{C}_i)\,, \quad a \otimes \psi \mapsto (a\psi(x_1), \ldots, a\psi(x_k)) \tag{2.1}$$

ein $\mathbb{Q}$-Algebra-Isomorphismus.

Beweis. Die Abbildung (2.1) ist offenbar ein Homomorphismus. Weiter gibt es für $\psi \in R(G)$ zu jedem $x \in \mathcal{C}_i$ einen Automorphismus $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mathcal{C}_i)/\mathbb{Q})$, sodass $\psi(x) = \sigma(\psi(x_i))$ gilt. Das Bild von $a \otimes \psi \in \mathbb{Q} \otimes R(G)$ ist daher genau dann $(0, \ldots, 0)$, wenn $a = 0$ bzw. $\psi(x_i) = 0$ für alle $i = 1, \ldots, k$ ist. Folglich ist die obige Abbildung (2.1) injektiv.

Sei nun $\mathcal{C}$ eine Vereinigung von $\mathbb{Q}$-Klassen von G. Da der $\mathbb{Z}$-Rang von $\mathrm{Ch}(\mathcal{C})$ nach Suzuki mit der Anzahl der Konjugationsklassen in $\mathcal{C}$ übereinstimmt [48], entspricht die Dimension des $\mathbb{Q}$-Vektorraums $\mathbb{Q} \otimes \mathrm{Ch}(\mathcal{C}_i)$ der Anzahl der in $\mathcal{C}_i$ enthaltenen Konjugationsklassen.

Sei C_i die Konjugationsklasse von G, in der x_i liegt. Nach Lemma 1.33 gibt es einen Isomorphismus zwischen $\mathrm{Gal}(\mathbb{Q}(\zeta_{|\langle x_i \rangle|})/\mathbb{Q}(C_i))$ und $N_G(\langle x_i \rangle)/C_G(x_i)$. Die Gleichung

$$[\mathbb{Q}(\zeta_{|\langle x_i \rangle|}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{|\langle x_i \rangle|}) : \mathbb{Q}(C_i)] \cdot [\mathbb{Q}(C_i) : \mathbb{Q}]$$

lässt sich demnach in der Form

$$\varphi(|\langle x_i\rangle|) = |N_G(\langle x_i\rangle) : C_G(x_i)| \cdot [\mathbb{Q}(C_i) : \mathbb{Q}]$$

schreiben, wobei φ für die Eulersche φ-Funktion steht. Nun ist $\varphi(|\langle x_i\rangle|)$ aber auch gleich der Anzahl der Elemente von $\langle x_i\rangle$, die dieselbe Ordnung wie x_i haben, und $|N_G(\langle x_i\rangle) : C_G(x_i)|$ entspricht der Anzahl von Elementen in $\langle x_i\rangle$, die in G zu x_i konjugiert sind. Somit ist $[\mathbb{Q}(\mathcal{C}_i) : \mathbb{Q}]$ die Anzahl der in $\mathcal{C}_i$ enthaltenen Konjugationsklassen, also hat $\mathbb{Q} \otimes \mathrm{Ch}(\mathcal{C}_i)$ die Dimension $[\mathbb{Q}(\mathcal{C}_i) : \mathbb{Q}]$.

Andererseits besitzt $\mathbb{Q}(\mathcal{C}_i)$ als $\mathbb{Q}$-Vektorraum ebenfalls die Dimension $[\mathbb{Q}(\mathcal{C}_i) : \mathbb{Q}]$. Da wie bereits gesehen $\mathbb{Q} \otimes \mathrm{Ch}(\mathcal{C}_i)$ injektiv nach $0 \oplus \cdots \oplus 0 \oplus \mathbb{Q}(\mathcal{C}_i) \oplus 0 \oplus \cdots \oplus 0$ abgebildet wird, ist die Abbildung (2.1) sogar eine Bijektion. □

Folgerung 2.6. *Die Abbildung* (2.1) *induziert einen Isomorphismus*

$$R(G)' \cong \bigoplus_{i=1}^{k} \mathcal{O}_{\mathbb{Q}(\mathcal{C}_i)}.$$

Beweis. Dies folgt unmittelbar aus Satz 2.5, da $R(G)'$ und $\bigoplus_{i=1}^{k} \mathcal{O}_{\mathbb{Q}(\mathcal{C}_i)}$ die maximalen Ordnungen der kommutativen $\mathbb{Q}$-Algebren $\mathbb{Q} \otimes R(G)$ bzw. $\bigoplus_{i=1}^{k} \mathbb{Q}(\mathcal{C}_i)$ sind. □

Bemerkung 2.7. Mit Folgerung 2.6 und Lemma 2.2 lässt sich schnell die Struktur der Einheitengruppe von $R(G)$ berechnen. Für einen Ring R bezeichne $U(R)$ dessen Einheitengruppe. Nach Lemma 2.2 ist $|G|R(G)'$ in $R(G)$ enthalten. Daher erhalten wir eine exakte Folge

$$0 \longrightarrow U(R(G)) \xrightarrow{f} U(R(G)/|G|R(G)') \oplus U(R(G)') \xrightarrow{g} U(R(G)'/|G|R(G)')\,,$$

wobei $f(u) = (u + |G|R(G)', u)$ und $g(u + |G|R(G)', v) = uv^{-1} + |G|R(G)'$ gelte. Da $R(G)/|G|R(G)'$ und $R(G)'/|G|R(G)'$ jeweils endlich sind, stimmt der Rang von $U(R(G))$ also mit dem von $U(R(G)')$ überein. Nach Anwendung von Folgerung 2.6 lässt sich letzterer mithilfe des Dirichletschen Einheitensatzes schnell angeben. Laut diesem entspricht der Rang der Einheitengruppe des Ganzheitsrings eines algebraischen Zahlkörpers $\mathbb{K}$ der Summe $r + s - 1$, wobei r die Anzahl der reellen Einbettungen und s die Anzahl der Paare komplex-konjugierter Einbettungen von $\mathbb{K}$ ist (siehe z. B. [39]).

Zudem ist bekannt, dass jede Torsionseinheit in $R(G)$ die Gestalt $\pm\lambda$ für einen linearen Charakter $\lambda \in \mathrm{Irr}(G)$ hat und die Gruppe der Torsionseinheiten von $R(G)$ demnach isomorph zu $C_2 \times G/G'$ ist. Insgesamt erhalten wir also folgendes Resultat:

Satz 2.8. *Seien $\mathcal{C}_1, \ldots, \mathcal{C}_k$ die $\mathbb{Q}$-Klassen von G. Für $i = 1, \ldots, k$ bezeichne r_i die Anzahl reeller Einbettungen und s_i die Anzahl der Paare komplex-konjugierter Einbettungen von $\mathbb{Q}(\mathcal{C}_i)$. Dann gilt*

$$U(R(G)) \cong \mathbb{Z}/2\mathbb{Z} \oplus G/G' \oplus \bigoplus_{i=1}^{k} \mathbb{Z}^{r_i+s_i-1}\,.$$

Beispiel 2.9. Wir bestimmen die Einheitengruppe $U(R(D_{10}))$ des Charakterrings der Diedergruppe D_{10} mit zehn Elementen. Seien $x, y \in D_{10}$, sodass $|\langle x\rangle| = 5$ und $|\langle y\rangle| = 2$ gilt, und $\mathbb{1}, \lambda, \chi_1, \chi_2$ die irreduziblen Charaktere der D_{10}, wobei λ der nichttriviale lineare Charakter ist und $\chi_k(x) = \zeta_5^k + \zeta_5^{-k}$ für $k = 1, 2$ gilt. Die Torsionseinheiten sind dann $\pm\mathbb{1}$ und $\pm\lambda$.

Wir wollen nun die Einheiten unendlicher Ordnung in $R(D_{10})$ finden. Auf $1_{D_{10}}$ sowie den Involutionen hat jeder Charakter von D_{10} natürlich ganzzahlige Werte. Ist $\eta \in R(D_{10})$ eine Einheit, so hat η auf den Elementen der Ordnung ≤ 2 also nur Werte aus $\{-1, 1\}$.

Die Elemente x und x^2 liegen in einer $\mathbb{Q}$-Klasse und es gilt $\mathbb{Q}(\mathrm{cl}_G(x)) = \mathbb{Q}(\zeta_5 + \zeta_5^4) = \mathbb{Q}(\sqrt{5})$. Bekanntlich besitzt $\mathbb{Q}(\sqrt{5})$ genau zwei reelle und keine komplex-konjugierten Einbettungen. Nach Satz 2.8 ist der Rang der Einheitengruppe von $R(D_{10})$ daher 1.

Die Fundamentaleinheit von $\mathbb{Q}(\sqrt{5})$ lautet $\varepsilon = \frac{1+\sqrt{5}}{2} = 1 + \zeta_5 + \zeta_5^4$ (siehe z. B. [4]), die Erzeuger der Einheitengruppe von $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ modulo Torsionseinheiten sind also ε, $-\varepsilon$, ε^{-1} und $-\varepsilon^{-1}$. Ist $\mathfrak{p}$ das 5 enthaltende Primideal von $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$, so gilt aber $\varepsilon \equiv 3 \pmod{\mathfrak{p}}$ und dementsprechend folgt $-\varepsilon \equiv \varepsilon^{-1} \equiv 2 \pmod{\mathfrak{p}}$ sowie $-\varepsilon^{-1} \equiv 3 \pmod{\mathfrak{p}}$. Für jeden Charakter $\psi \in R(D_{10})$ mit $\psi(x) \in \{\varepsilon, -\varepsilon, \varepsilon^{-1}, -\varepsilon^{-1}\}$ gilt nach Lemma 1.30 daher $\psi(1_{D_{10}}) \equiv \pm 2 \pmod 5$. Somit kann ψ keine Einheit sein.

Dagegen gibt es eine Einheit η in $R(D_{10})$ mit $\eta(x) = \varepsilon^2$. Es gilt nämlich

$$(\mathbb{1} + \chi_1)(1_{D_{10}}) = 3\,, \qquad (\mathbb{1} + \chi_1)(x) = \varepsilon \qquad \text{und} \qquad (\mathbb{1} + \chi_1)(y) = 1$$

und demzufolge

$$(\mathbb{1} + \chi_1)^2(1_{D_{10}}) = 9\,, \qquad (\mathbb{1} + \chi_1)^2(x) = \varepsilon^2 \qquad \text{sowie} \qquad (\mathbb{1} + \chi_1)^2(y) = 1\,.$$

Sei ϱ der reguläre Charakter von D_{10}. Setzen wir $\eta := (\mathbb{1} + \chi_1)^2 - \varrho$, so ergibt sich

$$\eta(1_{D_{10}}) = -1\,, \qquad \eta(x) = \varepsilon^2 \qquad \text{und} \qquad \eta(y) = 1\,.$$

Damit ist η ein Erzeuger von $U(R(D_{10}))$ modulo Torsionseinheiten. Man kann schnell nachrechnen, dass $\eta = \mathbb{1} - \chi_2$ gilt, also erhalten wir schließlich

$$U(R(D_{10})) = \langle -\mathbb{1}\rangle \times \langle \lambda\rangle \times \langle \mathbb{1} - \chi_2\rangle\,.$$

Nach dem kurzen Einschub zur Einheitengruppe von $R(G)$ wollen wir nun dazu kommen, wie uns Satz 2.1 und Folgerung 2.6 bei der Berechnung des Darstellungstyps von $R(G)$ helfen können. Die Ordnung $\bigoplus_{i=1}^k \mathcal{O}_{\mathbb{Q}(\mathcal{C}_i)}$ hat gegenüber $R(G)'$ einen entscheidenden Vorteil: Während für $\chi, \psi \in R(G)'$ im Allgemeinen unklar ist, welcher Funktion in $R(G)'$ das Produkt $\chi\psi$ entspricht (d. h. in welche Linearkombination irreduzibler Charaktere sich $\chi \otimes \psi$ zerlegen lässt), werden bei der Multiplikation zweier Elemente $a, b \in \bigoplus_{i=1}^k \mathcal{O}_{\mathbb{Q}(\mathcal{C}_i)}$ mit $a = (a_1, \ldots, a_k)$, $b = (b_1, \ldots, b_k)$ einfach deren Komponenten multipliziert: $ab = (a_1 b_1, \ldots, a_k b_k)$. Daher identifizieren wir

Klassenfunktionen aus $R(G)'$ im Folgenden immer mit Elementen in $\bigoplus_{i=1}^{k} \mathcal{O}_{\mathbb{Q}(\mathcal{C}_i)}$, bzw. Funktionen aus der Algebra $\mathbb{Q} \otimes R(G)$ mit Elementen in $\bigoplus_{i=1}^{k} \mathbb{Q}(\mathcal{C}_i)$.

Mit dieser Sichtweise stellt sich die Frage, welche Elemente aus $\mathbb{Z}_{(p)} \otimes \bigoplus_{i=1}^{k} \mathcal{O}_{\mathbb{Q}(\mathcal{C}_i)}$ auch in $R(G)_p$ liegen, wenn p ein Primteiler von $|G|$ ist. Wir versuchen zunächst, diese Frage für Funktionen mit ganzzahligen Werten, die nur auf wenigen $\mathbb{Q}$-Klassen von 0 verschieden sind, zu beantworten.

Lemma 2.10. *Seien $p \in \mathbb{P}$ und $\mathcal{S} := \{x \in G : p \nmid |C_G(x)|\}$. Dann gilt*

$$R(G)'_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}) = \mathrm{Ch}_{\mathbb{Z}_{(p)}}(\mathcal{S})\,.$$

Beweis. Seien $\varepsilon = \zeta_{\exp(G)}$ und $\{z_1, \ldots, z_k\}$ ein Repräsentantensystem für die Konjugationsklassen in $\mathcal{S}$. Es genügt zu zeigen, dass jedes Element φ_1 aus $\mathrm{Ch}(\mathcal{S})$, das auf allen Elementen aus $\mathcal{S}$ Werte in $p\mathbb{Z}[\varepsilon]$ annimmt, die Gestalt $\varphi_1 = p\varphi_2$ für ein $\varphi_2 \in \mathrm{Ch}(\mathcal{S})$ hat. Sei also $\varphi_1(z_i) = pr_i$, wobei $r_i \in \mathbb{Z}[\varepsilon]$ gelte. Mit den Bezeichnungen aus dem Beweis von Lemma 2.2 gilt dann

$$\varphi_1 = \sum_{i=1}^{k} pr_i\vartheta_{z_i} = p \sum_{\chi \in \mathrm{Irr}(G)} \left(\sum_{i=1}^{k} \frac{r_i}{|C_G(z_i)|} \chi(z_i^{-1}) \right) \chi\,.$$

Die Nenner $|C_G(z_i)|$ der inneren Summen sind nach Voraussetzung allesamt teilerfremd zu p. Damit und wegen $\varphi_1 \in \mathrm{Ch}(\mathcal{S})$ müssen die inneren Summen jeweils in $\mathbb{Z}$ liegen und folglich ist

$$\varphi_2 := \sum_{\chi \in \mathrm{Irr}(G)} \left(\sum_{i=1}^{k} \frac{r_i}{|C_G(z_i)|} \chi(z_i^{-1}) \right) \chi$$

ein Element aus $\mathrm{Ch}(\mathcal{S})$, das $\varphi_1 = p\varphi_2$ erfüllt. □

Die $\mathbb{Q}$-Klassen, die nur Elemente, deren Zentralisatoren zu p teilerfremde Ordnung haben, besitzen, sind also für die Bestimmung des Darstellungstyps irrelevant. Die übrigen $\mathbb{Q}$-Klassen unterteilen wir in p'-Sektionen.

Lemma 2.11. *Seien p eine Primzahl und $x \in G$ ein Element mit zu p teilerfremder Ordnung. Dann liegt die Funktion ν_x mit*

$$\nu_x(g) = \begin{cases} 1, & g_{p'} \text{ liegt in der } \mathbb{Q}\text{-Klasse von } x \\ 0, & \text{sonst} \end{cases}$$

in $R(G)_p$.

Beweis. Seien $g \in G$ mit $g_{p'} = x$ und $\mathcal{S}_g$ die $\mathbb{Q}$-Klasse von g. Dann lässt sich $\mathcal{S}_g$ in Konjugationsklassen $C_1, \ldots, C_k$ zerlegen. Seien $y_1, \ldots, y_k \in G$ Repräsentanten

von $C_1, \ldots, C_k$. Für die Klassenfunktion $\vartheta_{\mathcal{S}_g}$ von G mit $\vartheta_{\mathcal{S}_g}(y) = 1$ für $y \in \mathcal{S}_g$ und $\vartheta_{\mathcal{S}_g}(y) = 0$ für $y \in G \setminus \mathcal{S}_g$ gilt dann

$$\begin{aligned}\vartheta_{\mathcal{S}_g} &= \sum_{i=1}^{k} \vartheta_{y_i} = \sum_{i=1}^{k} \frac{1}{|C_G(g)|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(y_i^{-1})\chi = \frac{1}{|C_G(g)|} \sum_{\chi \in \mathrm{Irr}(G)} \left(\sum_{i=1}^{k} \chi(y_i^{-1}) \right) \chi \\ &= \frac{1}{|C_G(g)|} \sum_{\chi \in \mathrm{Irr}(G)} \left(\sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mathrm{cl}_G(y_1))/\mathbb{Q})} \sigma\left(\chi(y_1^{-1})\right) \right) \chi \\ &= \sum_{\chi \in \mathrm{Irr}(G)} \frac{\mathrm{Tr}_{\mathbb{Q}(\mathrm{cl}_G(y_1))/\mathbb{Q}}\left(\chi(y_1^{-1})\right)}{|C_G(g)|} \chi \,.\end{aligned}$$

Die Koeffizienten der irreduziblen Charaktere in der obigen Summe liegen allesamt in $\mathbb{Q}$, also ist $\vartheta_{\mathcal{S}_g}$ ein Element aus $R(G)'_p$.

Bezeichne $\mathcal{S}$ die rationale p'-Sektion von x in G. Dann ist $\mathcal{S}$ eine Vereinigung von $\mathbb{Q}$-Klassen $\mathcal{S}_1, \ldots, \mathcal{S}_\ell$ von G. Folglich gilt $\nu_x = \vartheta_{\mathcal{S}_1} + \ldots + \vartheta_{\mathcal{S}_\ell}$, wobei $\vartheta_{\mathcal{S}_j}$ auf den Elementen von $\mathcal{S}_j$ den Wert 1 hat und sonst verschwindet, $j \in \{1, \ldots, \ell\}$. Da jedes $\vartheta_{\mathcal{S}_j}$ in $R(G)'_p$ liegt, ist auch ν_x ein Element aus $R(G)'_p$.

Sei andererseits ε eine r-te Einheitswurzel, wobei r dem p'-Anteil von $|G|$ entspricht, und $\mathfrak{p}$ ein maximales Ideal in $\mathbb{Z}[\varepsilon]$, das p enthält. Dann liegt die Funktion $\tilde{\nu}_x$, mit $\tilde{\nu}_x(g) = 1$, wenn $g_{p'}$ in G zu x konjugiert ist, und $\tilde{\nu}_x(g) = 0$ sonst, nach Lemma 1.29 in $(\mathbb{Z}[\varepsilon])_\mathfrak{p} \otimes R(G)$. Für ein Repräsentantensystem $\{\tilde{x}_1, \ldots, \tilde{x}_r\}$ der Konjugationsklassen, die in der $\mathbb{Q}$-Klasse von x liegen, ist daher $\nu_x = \tilde{\nu}_{\tilde{x}_1} + \ldots + \tilde{\nu}_{\tilde{x}_r}$ und es folgt $\nu_x \in R(G)'_p \cap ((\mathbb{Z}[\varepsilon])_\mathfrak{p} \otimes R(G)) = R(G)_p$. □

Bemerkung 2.12. Um den Darstellungstyp von $R(G)_p$ zu bestimmen, kann man die rationalen p'-Sektionen von G also separat betrachten. Lemma 2.11 besagt nämlich, dass eine Funktion $\varphi \in \mathbb{Q} \otimes R(G)$ genau dann in $R(G)_p$ liegt, wenn $\nu_x\varphi$ für jedes $x \in G$ mit zu p teilerfremder Ordnung in $R(G)_p$ enthalten ist. Hat man verschiedene rationale p'-Sektionen $\mathcal{S}_1, \ldots, \mathcal{S}_k$ und sind

$$\begin{aligned}&\alpha_1, \beta_1 \text{ Erzeuger des } R(G)_p\text{-Moduls } (R(G)'_p \cap \mathrm{Ch}_\mathbb{Q}(\mathcal{S}_1))/(R(G)_p \cap \mathrm{Ch}_\mathbb{Q}(\mathcal{S}_1)) \,, \\ &\quad \vdots \\ &\alpha_k, \beta_k \text{ Erzeuger des } R(G)_p\text{-Moduls } (R(G)'_p \cap \mathrm{Ch}_\mathbb{Q}(\mathcal{S}_k))/(R(G)_p \cap \mathrm{Ch}_\mathbb{Q}(\mathcal{S}_k)) \,,\end{aligned}$$

so erzeugen $\alpha_1 + \ldots + \alpha_k$ und $\beta_1 + \ldots + \beta_k$ demnach den $R(G)_p$-Modul

$$(R(G)'_p \cap \mathrm{Ch}_\mathbb{Q}(\mathcal{S}_1 \cup \ldots \cup \mathcal{S}_k))/(R(G)_p \cap \mathrm{Ch}_\mathbb{Q}(\mathcal{S}_1 \cup \ldots \cup \mathcal{S}_k)) \,.$$

Analog wird das Radikal von $R(G)'_p/R(G)_p$ genau dann von höchstens einem Element erzeugt, wenn $\mathrm{rad}((R(G)'_p \cap \mathrm{Ch}_\mathbb{Q}(\mathcal{S}))/(R(G)_p \cap \mathrm{Ch}_\mathbb{Q}(\mathcal{S})))$ für jede rationale p'-Sektion $\mathcal{S}$ zyklisch ist.

Aus dieser Überlegung erhalten wir eine erste notwendige Bedingung dafür, dass $R(G)$ endlichen Darstellungstyp hat.

Satz 2.13. *Sei G eine Gruppe, die für ein $p \in \mathbb{P}$ eine rationale p'-Sektion $\mathcal{S}$ mit $a+1$ verschiedenen $\mathbb{Q}$-Klassen besitzt. Dann hat ein minimales Erzeugendensystem des $R(G)_p$-Moduls $R(G)'_p/R(G)_p$ mindestens a Erzeuger.*

Beweis. Seien $\varepsilon = \zeta_{\exp(G)}$ und $\mathcal{C}_1, \ldots, \mathcal{C}_{a+1}$ die verschiedenen $\mathbb{Q}$-Klassen von $\mathcal{S}$. Wie im Beweis zu Lemma 2.11 kann man zeigen, dass es für $j = 1, \ldots, a+1$ Funktionen φ_j aus $R(G)'_p$ mit $\varphi_j(x) = 1$ für $x \in \mathcal{C}_j$ und $\varphi_j(x) = 0$ sonst gibt. Sicherlich liegen die φ_j nicht in $R(G)_p$, da für $x_j \in \mathcal{C}_j$ und $x_k \in \mathcal{C}_k$, $j \neq k$, stets $\varphi_j(x_j) \not\equiv \varphi_j(x_k) \pmod{\mathfrak{p}}$ gilt, wenn $\mathfrak{p}$ ein maximales Ideal aus $\mathbb{Z}[\varepsilon]$, das p enthält, ist.

Seien nun $\psi_1, \ldots, \psi_n \in R(G)'_p$ so, dass $\psi_1 + R(G)_p, \ldots, \psi_n + R(G)_p$ Erzeuger des $R(G)_p$-Moduls $R(G)'_p/R(G)_p$ sind. Dann existieren für jedes $j \in \{1, \ldots, a+1\}$ also $\lambda_{1,j}, \ldots, \lambda_{n+1,j} \in R(G)_p$, sodass $\lambda_{1,j}\psi_1 + \ldots + \lambda_{n,j}\psi_n + \lambda_{n+1,j} = \varphi_j$ ist. Seien $x_1 \in \mathcal{C}_1, \ldots, x_{a+1} \in \mathcal{C}_{a+1}$ und F die durch

$$F : R(G)'_p \to (\mathbb{Z}[\varepsilon]/\mathfrak{p})^{a+1}, \quad \vartheta \mapsto (\vartheta(x_1) + \mathfrak{p}, \ldots, \vartheta(x_{a+1}) + \mathfrak{p})$$

gegebene Abbildung. Dann sind die Vektoren $F(\varphi_1), \ldots, F(\varphi_{a+1})$ linear unabhängig im $\mathbb{Z}[\varepsilon]/\mathfrak{p}$-Vektorraum $(\mathbb{Z}[\varepsilon]/\mathfrak{p})^{a+1}$, bilden dort also eine Basis. Weiter induzieren die $F(\lambda_{i,j})$ Multiplikationen mit Skalaren in $(\mathbb{Z}[\varepsilon]/\mathfrak{p})^{a+1}$, da für $x, y \in \mathcal{S}$ stets $\lambda_{i,j}(x) \equiv \lambda_{i,j}(y) \pmod{\mathfrak{p}}$ gilt. Daher müssen auch $F(\psi_1), \ldots, F(\psi_n), F(\mathbb{1})$ ein Erzeugendensystem von $(\mathbb{Z}[\varepsilon]/\mathfrak{p})^{a+1}$ bilden, was $n \geq a$ erzwingt. □

Folgerung 2.14. *Sei G eine Gruppe, die für eine Primzahl p eine rationale p'-Sektion mit mindestens vier $\mathbb{Q}$-Klassen enthält. Dann hat $R(G)$ unendlichen Darstellungstyp. Insbesondere hat der Charakterring einer endlichen Gruppe, die für eine Primzahl p ein Element der Ordnung p^3 enthält, unendlichen Darstellungstyp.*

Nachdem wir eine Klasse von Funktionen aus $R(G)'_p$ über den p'-Anteil der Elemente aus G definiert haben, wollen wir nun zu Funktionen aus $R(G)'_p$ kommen, in denen der p-Anteil der Gruppenelemente die wesentliche Rolle spielt.

Definition 2.15. Seien p eine Primzahl und G eine Gruppe mit durch p teilbarer Ordnung. Für $i \in \mathbb{N}_0$ werde die Klassenfunktion μ_i definiert durch

$$\mu_i(g) := \begin{cases} 1, & |\langle g_p \rangle| = p^i \\ 0, & \text{sonst} \end{cases} \quad \text{für } g \in G.$$

Lemma 2.16. *Sei $|G|$ durch p teilbar und $k \in \mathbb{N}$ die größte Zahl, sodass p^k ein Teiler von $\exp(G)$ ist. Für $i = 0, \ldots, k$ ist dann $\mu_i \in R(G)'_p \setminus R(G)_p$.*

Beweis. Wie oben erhalten wir $\mu_i \in R(G)'_p$ für $i = 1, \ldots, k$, da μ_i als Funktion der $\mathbb{Q}$-Klassen von G angesehen werden kann. Läge μ_i dagegen in $R(G)_p$, so müsste für $g \in G$ stets $\mu_i(g) \equiv \mu_i(g_{p'}) \pmod{\mathfrak{p}}$ gelten, wobei $\mathfrak{p}$ ein p enthaltendes maximales Ideal von $\mathbb{Z}[\zeta_{\exp(G)}]$ ist. Nun enthält G jedoch ein Element x der Ordnung p^i, also gilt $\mu_i(x) \equiv 1 \not\equiv 0 \equiv \mu_i(1_G) \pmod{\mathfrak{p}}$ für $i > 0$. Weiter liegt ein Element y der Ordnung p in G, sodass auch μ_0 wegen $\mu_0(y) \equiv 0 \not\equiv 1 \equiv \mu_0(1_G) \pmod{\mathfrak{p}}$ nicht in $R(G)_p$ ist. □

Zum Abschluss des Kapitels beweisen wir noch eine Art Orthogonalitätsrelation für die Charaktere von G. Aus dieser lassen sich unter anderem Funktionen aus $R(G)'_p$ gewinnen, die lediglich auf einer zyklischen Untergruppe von G (und deren Konjugierten) bzw. nur auf deren Erzeugern von 0 verschieden sind.

Lemma 2.17. *Seien $x \in G$ und ε eine $|\langle x\rangle|$-te Einheitswurzel. Die Zahl $a_{\chi(x)}(\varepsilon)$ gebe an, wie oft ε als Summand in $\chi(x)$ für $\chi \in \mathrm{Irr}(G)$ auftaucht. Dann gilt für $g \in G$*

$$\sum_{\chi\in\mathrm{Irr}(G)} a_{\chi(x)}(\varepsilon)\chi(g) = \begin{cases} \frac{|C_G(g)|}{|\langle x\rangle|} \cdot \sum\limits_{\sigma\in\mathrm{Gal}\left(\mathbb{Q}(\zeta_{|\langle g\rangle|})/\mathbb{Q}(\mathrm{cl}_G(g))\right)} \sigma(\varepsilon^k)\,, & g \sim_G x^k \textit{ für ein } k \in \mathbb{Z} \\ 0\,, & \textit{sonst} \end{cases}$$
$$= \begin{cases} \frac{|N_G(\langle g\rangle)|\cdot|C_G(x)|}{|N_G(\langle x\rangle)|\cdot|\langle x\rangle|} \cdot \sum\limits_{\sigma\in\mathrm{Gal}\left(\mathbb{Q}(\zeta_{|\langle x\rangle|})/\mathbb{Q}(\mathrm{cl}_G(x))\right)} \sigma(\varepsilon^k)\,, & g \sim_G x^k \textit{ für ein } k \in \mathbb{Z} \\ 0\,, & \textit{sonst} \end{cases}.$$

Beweis. Sei λ der Charakter aus $\mathrm{Irr}(\langle x\rangle)$, für den $\lambda(x) = \varepsilon$ gilt. Das führt zu

$$\begin{aligned}
&\sum_{\chi\in\mathrm{Irr}(G)} a_{\chi(x)}(\varepsilon)\chi(g) \\
&= \sum_{\chi\in\mathrm{Irr}(G)} \langle\chi,\lambda\rangle_{\langle x\rangle}\chi(g) = \sum_{\chi\in\mathrm{Irr}(G)} \frac{1}{|\langle x\rangle|} \sum_{h\in\langle x\rangle} \lambda(h)\chi(h^{-1})\chi(g) \\
&= \frac{1}{|\langle x\rangle|} \sum_{h\in\langle x\rangle} \lambda(h) \sum_{\chi\in\mathrm{Irr}(G)} \chi(h^{-1})\chi(g) = \frac{1}{|\langle x\rangle|} \sum_{\substack{h\in\langle x\rangle \\ h\sim_G g}} \lambda(h)|C_G(g)| \\
&= \begin{cases} \frac{|C_G(g)|}{|\langle x\rangle|} \sum\limits_{\sigma\in\mathrm{Gal}\left(\mathbb{Q}(\zeta_{|\langle g\rangle|})/\mathbb{Q}(\mathrm{cl}_G(g))\right)} \sigma(\varepsilon^k)\,, & g \sim_G x^k \text{ für ein } k \in \mathbb{Z} \\ 0\,, & \text{sonst} \end{cases} \\
&= \begin{cases} \frac{\left|\mathrm{Gal}\left(\mathbb{Q}(\zeta_{|\langle g\rangle|})/\mathbb{Q}(\mathrm{cl}_G(g))\right)\right|}{\left|\mathrm{Gal}\left(\mathbb{Q}(\zeta_{|\langle x\rangle|})/\mathbb{Q}(\mathrm{cl}_G(x))\right)\right|} \cdot \frac{|C_G(g)|}{|\langle x\rangle|} \cdot \sum\limits_{\sigma\in\mathrm{Gal}\left(\mathbb{Q}(\zeta_{|\langle x\rangle|})/\mathbb{Q}(\mathrm{cl}_G(x))\right)} \sigma(\varepsilon^k)\,, & g \sim_G x^k \text{ für ein } k \in \mathbb{Z} \\ 0\,, & \text{sonst} \end{cases} \\
&= \begin{cases} \frac{|N_G(\langle g\rangle)|\cdot|C_G(x)|}{|N_G(\langle x\rangle)|\cdot|\langle x\rangle|} \cdot \sum\limits_{\sigma\in\mathrm{Gal}\left(\mathbb{Q}(\zeta_{|\langle x\rangle|})/\mathbb{Q}(\mathrm{cl}_G(x))\right)} \sigma(\varepsilon^k)\,, & g \sim_G x^k \text{ für ein } k \in \mathbb{Z} \\ 0\,, & \text{sonst} \end{cases}.
\end{aligned}$$

□

3 Sylowgruppen von Gruppen, deren Charakterring endlichen Typ hat

Wir wollen herausfinden, welche Gestalt die Sylowgruppen von G haben können, wenn $R(G)$ endlichen Darstellungstyp hat. Dazu beginnen wir mit einem trivialen Lemma, das wir nichtsdestotrotz in vielen der folgenden Beweise zur Reduktion verwenden werden.

Lemma 3.1. *Sei N ein Normalteiler von G. Dann liegen für eine Primzahl p in G/N nur höchstens so viele $\mathbb{Q}$-Klassen von p-Elementen wie es $\mathbb{Q}$-Klassen von p-Elementen in G gibt. Weiter enthält für ein p-Element $x \in G$ die $\mathbb{Q}$-Klasse von x in G mindestens so viele Konjugationsklassen wie die $\mathbb{Q}$-Klasse xN in G/N.*

Beweis. Gibt es ein $g \in G$, sodass $gxg^{-1} = y$ ist, dann folgt natürlich sofort $gNxNg^{-1}N = gxg^{-1}N = yN$. Sind $C_1, \ldots, C_k$ die Konjugationsklassen von G, so sind $\overline{C}_1, \ldots, \overline{C}_k$ demzufolge die Konjugationsklassen von G/N, wobei $\overline{C}_i = \overline{C}_j$ für $i \neq j$ durchaus möglich ist. Zudem besitzt natürlich jedes p-Element $\overline{x} \in G/N$ ein Urbild $x \in G$, das ebenfalls ein p-Element ist. □

Über die abelschen Sylowgruppen von G kann man relativ leicht eine sehr restriktive Aussage treffen. Wir erhalten den folgenden

Satz 3.2. *Sei p eine Primzahl und $P \in \mathrm{Syl}_p(G)$ abelsch. Ist der Darstellungstyp von $R(G)$ endlich, so ist P zyklisch der Ordnung $\leq p^2$ oder elementar-abelsch.*

Beweis. Wir nehmen an, dass P weder zyklisch der Ordnung $\leq p^2$ noch elementar-abelsch ist, und zeigen, dass es in diesem Fall mindestens vier $\mathbb{Q}$-Klassen von p-Elementen in G gibt. Folgerung 2.14 impliziert dann die Behauptung.

Weil P als abelsche p-Sylowgruppe von G resistent ist, können wir $P \trianglelefteq G$ annehmen. Dass der Exponent von P höchstens p^2 sein darf, wissen wir bereits aus Folgerung 2.14. Somit ist P isomorph zu einem direkten Produkt $A := Z_1 \times \ldots \times Z_r$ von zyklischen Gruppen $Z_1, \ldots, Z_r$ der Ordnung p oder p^2. Wir identifizieren A im Folgenden mit P.

Angenommen, nicht alle Z_i haben die gleiche Ordnung, also o. B. d. A. $|Z_1| = p$ und $|Z_2| = p^2$. Wir schreiben $Z_1 = \langle z_1 \rangle$ und $Z_2 = \langle z_2 \rangle$. Dann gibt es kein $x \in A$, sodass $x^p = (z_1, 0, \ldots, 0)$ ist, dagegen gilt $(0, z_2, 0, \ldots, 0)^p = (0, z_2^p, 0, \ldots, 0)$. Daher liegen $(z_1, 0, \ldots, 0)$ und $(0, z_2^p, 0, \ldots, 0)$ nicht in derselben $\mathbb{Q}$-Klasse von G und folglich sind die $\mathbb{Q}$-Klassen von G mit den Repräsentanten 1_G, $(z_1, 0, \ldots, 0)$, $(0, z_2^p, 0, \ldots, 0)$ und $(0, z_2, 0, \ldots, 0)$ alle verschieden.

Damit verbleibt nur noch auszuschließen, dass P homozyklisch vom Exponenten p^2 ist. Ist $P \cong C_{p^2}^n$ für ein $n \in \mathbb{N}$ mit $n \geq 2$, so hat P genau $p^{2n}-1-(p^n-1) = p^n(p^n-1)$ Elemente der Ordnung p^2 und deswegen genau $p^{n-1}\frac{p^n-1}{p-1}$ zyklische Untergruppen der Ordnung p^2. Da alle zyklischen Untergruppen der Ordnung p^2 in G konjugiert sein müssen, operiert G transitiv auf der Menge M dieser zyklischen Untergruppen. Dies liefert für $H \in M$ eine Bijektion zwischen $G/\mathrm{Stab}_G(H)$ und M. Nun ist P als abelsche Gruppe aber sicherlich in $\mathrm{Stab}_G(H)$ enthalten, also ist p kein Teiler von $|G : \mathrm{Stab}_G(H)|$. Wegen $n \geq 2$ teilt p dagegen $|M| = p^{n-1}\frac{p^n-1}{p-1}$, was $|G : \mathrm{Stab}_G(H)| = |M|$ widerspricht. □

3.1 Nichtabelsche Kompositionsfaktoren

In diesem Abschnitt wollen wir uns anschauen, welche nichtabelschen Kompositionsfaktoren G besitzen kann, wenn $R(G)$ endlichen Darstellungstyp hat. Zusätzlich zur Bestimmung der möglichen Isomorphietypen eines solchen Kompositionsfaktors werden wir zeigen, dass eine eventuell in G vorhandene Komponente eine Hallgruppe von G sein muss.

Bevor wir uns um die Gestalt möglicher nichtabelscher Kompositionsfaktoren kümmern, schränken wir erst einmal deren Anzahl ein.

Lemma 3.3. *Sei G eine Gruppe gerader Ordnung, sodass $R(G)$ endlichen Darstellungstyp hat. Dann besitzt G genau eine Konjugationsklasse von Involutionen.*

Beweis. Die Konjugationsklasse eines Elements der Ordnung 2 stimmt offenbar mit dessen $\mathbb{Q}$-Klasse überein. Nach Folgerung 2.14 darf G also höchstens zwei Konjugationsklassen von Involutionen enthalten – wenn es ein Element der Ordnung 4 in G gibt, sogar nur eine.

Sei $P \in \mathrm{Syl}_2(G)$ mit $\exp(P) = 2$, d. h., P ist elementar-abelsch. Angenommen, es gibt zwei Konjugationsklassen von Elementen der Ordnung 2 in G. Dann gibt es auch zwei Konjugationsklassen C_1, C_2 von Involutionen in $N_G(P)$, weil P als abelsche Gruppe resistent ist. Für $x \in C_1$ gilt $|C_1| = \frac{|N_G(P)|}{|C_{N_G(P)}(x)|}$. Da P abelsch ist, muss $P \leq C_{N_G(P)}(x)$ gelten, also ist $\frac{|N_G(P)|}{|C_{N_G(P)}(x)|}$ und damit $|C_1|$ ungerade. Analog dazu muss auch $|C_2|$ ungerade sein. Damit wäre aber $|P| = 1 + |C_1| + |C_2|$ ungerade, was für eine nichttriviale 2-Gruppe unmöglich ist. □

Lemma 3.4. *Sei G eine nichtauflösbare Gruppe mit höchstens drei $\mathbb{Q}$-Klassen von 2-Elementen. Dann hat G keinen Normalteiler, der zu einem direkten Produkt mindestens zweier einfacher Gruppen isomorph ist.*

Beweis. Angenommen $S_1 \times \ldots \times S_n$ wäre ein solcher Normalteiler von G, wobei die S_i einfache Untergruppen sind ($i = 1, \ldots, n$). Dann existieren nach dem Satz von Feit und Thompson Involutionen $t_1 \in S_1, \ldots, t_n \in S_n$. Die Zentralisatoren von $(t_1, \ldots, t_n)$ und $(t_1, \ldots, t_{n-1}, 1_{S_n})$ in G haben offenbar unterschiedliche Ordnungen. Folglich sind $(t_1, \ldots, t_n)$ und $(t_1, \ldots, t_{n-1}, 1_{S_n})$ nicht in G konjugiert.

Daher besitzt G mindestens zwei Konjugationsklassen von Involutionen. Dann kann G aber kein Element der Ordnung 4 und keine weitere Konjugationsklasse von Involutionen enthalten. Also besitzt G genau zwei Konjugationsklassen von Elementen der Ordnung 2 und die 2-Sylowgruppen von G sind elementar-abelsch. Dieselbe Argumentation wie im Beweis von Lemma 3.3 liefert jetzt den Widerspruch, dass es eine 2-Sylowgruppe ungerader Ordnung in G geben müsste. □

Proposition 3.5. *Sei G eine Gruppe, deren Charakterring $R(G)$ endlichen Darstellungstyp hat. Dann hat G höchstens einen nichtabelschen Kompositionsfaktor.*

Beweis. Ist G auflösbar, so hat G natürlich keinen nichtabelschen Kompositionsfaktor, wir nehmen also an, dass G nicht auflösbar ist. Da $R(G)$ endlichen Darstellungstyp hat, darf es nach Folgerung 2.14 in G nur maximal drei $\mathbb{Q}$-Klassen von 2-Elementen geben. Nach Lemma 3.1 hat auch $G/F(G)$ dann höchstens drei $\mathbb{Q}$-Klassen von 2-Elementen, ebenso $(G/F(G))/F(G/F(G))$ usw.

Wir können daher annehmen, dass $F^*(G) = E(G)$ ein direktes Produkt einfacher Gruppen ist und G höchstens drei $\mathbb{Q}$-Klassen von 2-Elementen hat. Nach Lemma 3.4 ist $F^*(G)$ einfach und wegen $C_G(F^*(G)) \leq F^*(G)$ ist $C_G(F^*(G))$ trivial. Daher ist $G/F^*(G)$ isomorph zu einer Untergruppe von $\mathrm{Out}(F^*(G))$, welche gemäß der Schreier-Vermutung auflösbar ist. □

Nun wollen wir die Frage beantworten, wie dieser Kompositionsfaktor aussehen kann, wenn er isomorph zu einer Komponente ist. Eine wesentliche Rolle werden dabei wieder die Involutionen einnehmen.

Satz 3.6. *Seien N ein nichtabelscher quasieinfacher Normalteiler von G und der Darstellungstyp von $R(G)$ endlich. Dann ist* $\mathrm{ggT}(|N|, |G : N|) = 1$ *und N ist isomorph zu einer der folgenden Gruppen:*

1. $\mathrm{PSL}(2, q)$, *wobei $q > 2$ gerade und $q^2 - 1$ kubikfrei ist,*
2. $\mathrm{PSL}(2, q)$, *wobei $q > 3$ ungerade ist und keine der Zahlen q, $q + 1$ und $q - 1$ von 16 oder der dritten Potenz einer ungeraden Primzahl geteilt wird,*
3. $\mathrm{SL}(2, p)$, *wobei $p > 3$ eine ungerade Primzahl ist und $p+1$ sowie $p-1$ kubikfrei sind,*
4. A_7,
5. J_1.

Beweis. Sei N vorerst eine einfache Gruppe. Wir untersuchen als erstes, welchen Isomorphietyp N haben kann. Nach Lemma 3.3 und Satz 1.54 ist N eine der einfachen Gruppen aus der Liste in Satz 1.53. Zudem wissen wir dank Lemma 3.3, dass in $G \setminus N$ keine Involution liegen kann, denn diese wäre nicht zu den Involutionen aus N konjugiert. Gibt es in N ein Element der Ordnung 4, so muss die Gruppe G/N außerdem ungerade Ordnung haben, sonst gibt es mindestens vier $\mathbb{Q}$-Klassen von 2-Elementen in G.

Wir betrachten die Gruppen der Liste aus Satz 1.53 jetzt im Einzelnen.

• A_5, A_6, A_7

Wegen $A_5 \cong \mathrm{PSL}(2,5)$ und $A_6 \cong \mathrm{PSL}(2,9)$ stehen alle infrage kommenden alternierenden Gruppen in der obigen Liste. Ist N eine dieser alternierenden Gruppen, so ist also nichts zu zeigen.

• $\mathrm{PSL}(2,q)$

Sei $N \cong \mathrm{PSL}(2,q)$, wobei q gerade ist. Dann besitzt N sowohl Elemente der Ordnung $q-1$ als auch der Ordnung $q+1$. Nach Folgerung 2.14 dürfen diese von keiner dritten Potenz einer Primzahl geteilt werden bzw., anders formuliert, q^2-1 muss kubikfrei sein.

Wir setzen im Folgenden also $N \cong \mathrm{PSL}(2,q)$ mit $q = p^k$, wobei p eine ungerade Primzahl ist, voraus. Dann gibt es Elemente der Ordnung $\frac{q+1}{2}$ und $\frac{q-1}{2}$. Die Zahlen $q+1$ und $q-1$ dürfen demnach weder von der dritten Potenz einer ungeraden Primzahl noch von 16 geteilt werden.

Sei jetzt $k \geq 3$. In N gibt es genau zwei Konjugationsklassen von Elementen der Ordnung p. Wir wählen Repräsentanten x und y dieser beiden Klassen. Die Automorphismengruppe von N wird unter anderem in [55] beschrieben, insbesondere folgt, dass G eine zu $\mathrm{PGL}(2,q)$ isomorphe Untergruppe enthalten muss, damit x und y in G konjugiert sein können. Allerdings hat das Bild der Diagonalmatrix $\mathrm{diag}(1,-1) \in \mathrm{GL}(2,q)$ in $\mathrm{PGL}(2,q)$ immer noch die Ordnung 2, also liegen in $\mathrm{PGL}(2,q)$ zwei Klassen von Involutionen, von denen nur eine Elemente aus N beinhaltet. Daher können diese Klassen in G nicht konjugiert sein. Dies widerspricht jedoch Lemma 3.3, also liegen x und y auch in G in verschiedenen Klassen.

Ist $q \equiv 1 \pmod 4$, so gilt $\chi(1) \equiv \chi(x) \equiv \chi(y) \pmod{p^2}$ für jeden irreduziblen Charakter $\chi \in \mathrm{Irr}(N)$ und somit auch für $\chi \in \mathrm{Irr}(G)$. Demzufolge liegen die Funktionen φ_1 und φ_2 mit

$$\varphi_1(g) = \begin{cases} p, & g \sim x \\ p, & g \sim y \\ 0, & \text{sonst} \end{cases} \qquad \text{und} \qquad \varphi_2(g) = \begin{cases} p, & g \sim x \\ -p, & g \sim y \\ 0, & \text{sonst} \end{cases}$$

in $\mathrm{rad}(R(G)'_p) \setminus R(G)_p$.

Angenommen es gäbe ein $\alpha \in \mathrm{rad}(R(G)'_p)$, zu dem $\eta_1, \eta_2, \psi_1, \psi_2 \in R(G)_p$ existieren, sodass $\varphi_1 = \eta_1\alpha + \psi_1$ und $\varphi_2 = \eta_2\alpha + \psi_2$ gilt. Wegen $\varphi_2(x) \not\equiv \varphi_2(y) \pmod{p^2}$

muss dann $\alpha(x) \not\equiv \alpha(y) \pmod{p^2}$ sein, denn es gilt $\eta_2(x) \equiv \eta_2(y) \pmod{p^2}$ sowie $\psi_2(x) \equiv \psi_2(y) \pmod{p^2}$. Andererseits ist $(\varphi_1 - \psi_1)(x) \equiv (\varphi_1 - \psi_1)(y) \pmod{p^2}$. Damit $\eta_1\alpha(x) \equiv \eta_2\alpha(y) \pmod{p^2}$ sein kann, müssen also $\eta_1(x)$ und $\eta_1(y)$ durch p teilbar sein. Dann folgt aber auch $\eta_1\alpha(1) \equiv \eta_1\alpha(x) \pmod{p^2}$. Dagegen erhalten wir $(\varphi_1 - \psi_1)(1) \not\equiv (\varphi_1 - \psi_1)(x) \pmod{p^2}$, denn während $\psi_1(1) - \psi_1(x)$ durch p^2 teilbar ist, gilt $\varphi_1(1) \not\equiv \varphi_1(x) \pmod{p^2}$. Folglich kann $\mathrm{rad}(R(G)'_p/R(G)_p)$ nicht zyklisch sein, also hätte $R(G)$ unendlichen Darstellungstyp.

Die Argumentation im Fall $q \equiv 3 \pmod 4$ verläuft ähnlich. Sei $\mathfrak{p}$ das maximale Ideal von $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$, welches p enthält. Dann gilt $\chi(1) \equiv \chi(x) \equiv \chi(y) \pmod{\mathfrak{p}^3}$ für jeden irreduziblen Charakter $\chi \in \mathrm{Irr}(N)$ und demnach auch für $\chi \in \mathrm{Irr}(G)$. Daher liegen die Funktionen φ_1 und φ_2 mit

$$\varphi_1(g) = \begin{cases} p, & g \sim x \\ p, & g \sim y \\ 0, & \text{sonst} \end{cases} \qquad \text{und} \qquad \varphi_2(g) = \begin{cases} \sqrt{-p}, & g \sim x \\ -\sqrt{-p}, & g \sim y \\ 0, & \text{sonst} \end{cases}$$

in $\mathrm{rad}(R(G)'_p) \setminus R(G)_p$. Analog zum Fall $q \equiv 1 \pmod 4$ lässt sich zeigen, dass zu keinem $\alpha \in \mathrm{rad}(R(G)'_p)$ Funktionen $\eta_1, \eta_2, \psi_1, \psi_2 \in R(G)_p$ existieren, sodass $\varphi_1 = \eta_1\alpha + \psi_1$ und $\varphi_2 = \eta_2\alpha + \psi_2$ gilt. Das bedeutet, dass $\mathrm{rad}(R(G)'_p/R(G)_p)$ nicht zyklisch ist und $R(G)$ folglich unendlichen Darstellungstyp hat.

• $\mathrm{PSL}(3,q)$ und $\mathrm{PSU}(3,q)$

Die Charaktertafeln der Gruppen $\mathrm{PSL}(3,q)$ und $\mathrm{PSU}(3,q)$ wurden in [46] bestimmt. Ist q ungerade, so enthalten sowohl $\mathrm{PSL}(3,q)$ als auch $\mathrm{PSU}(3,q)$ Elemente der Ordnung 8, also hat $R(G)$ unendlichen Darstellungstyp, wenn N isomorph zu einer dieser Gruppen ist. Sei nun q gerade. Da $\mathrm{PSU}(3,2)$ auflösbar ist und wegen $\mathrm{PSL}(3,2) \cong \mathrm{PSL}(2,7)$ können wir $q > 2$ annehmen.

Wir betrachten zunächst den Fall $q \geq 8$ und $N \cong \mathrm{PSL}(3,q)$ mit $q \equiv 2 \pmod 3$ bzw. $N \cong \mathrm{PSU}(3,q)$ mit $q \equiv 1 \pmod 3$. Wir setzen $\delta = 1$, falls $N \cong \mathrm{PSL}(3,q)$ und $\delta = -1$, falls $N \cong \mathrm{PSU}(3,q)$. Dann beinhaltet N mindestens drei $\mathbb{Q}$-Klassen von Elementen der Ordnung $q - \delta$. Repräsentanten dieser $\mathbb{Q}$-Klassen sind z. B. die Diagonalmatrizen $x = \mathrm{diag}(\zeta, \zeta, \zeta^{-2})$, $y = \mathrm{diag}(\zeta, \zeta^2, \zeta^{-3})$ und $z = \mathrm{diag}(\zeta, \zeta^{-1}, 1)$, wobei ζ eine Einheitswurzel der Ordnung $q - \delta$ ist. Weiter ist $|C_N(x)|$ im Gegensatz zu $|C_N(y)|$ und $|C_N(z)|$ gerade, daher kann x auch in G weder zu y noch zu z $\mathbb{Q}$-konjugiert sein. Zudem sind z und z^{-1} in N konjugiert, während y und y^{-1} in verschiedenen Konjugationsklassen von N liegen. Da N Elemente der Ordnung 4 enthält, ist $|G : N|$ ungerade. Das bedeutet, dass y und z auch in G nicht in derselben $\mathbb{Q}$-Klasse sind.

Sei jetzt $N \cong \mathrm{PSL}(3,q)$ mit $q \equiv 1 \pmod 3$ bzw. $N \cong \mathrm{PSU}(3,q)$ mit $q \equiv 2 \pmod 3$. Dann besitzt N drei $\mathbb{Q}$-Klassen von Elementen der Ordnung 4. Diese Klassen müssen in G zusammenfallen, also durch äußere Automorphismen von N aufeinander abgebildet werden. Die äußeren Automorphismen von N findet man wieder in [55], insbesondere folgt, dass G eine zu $\mathrm{PGL}(3,q)$ bzw. $\mathrm{PGU}(3,q)$ isomorphe Untergruppe enthalten muss.

Wir identifizieren N zunächst mit $\mathrm{PSL}(3,q)$. Die Elemente

$$X := \begin{pmatrix} 1 & & \\ & \omega & \\ & & \omega^2 \end{pmatrix}, \quad Y := \begin{pmatrix} \omega & & \\ & \omega & \\ & & \omega^2 \end{pmatrix} \quad \text{und} \quad Z := \begin{pmatrix} \omega & 1 & \\ & \omega & \\ & & \omega^2 \end{pmatrix}$$

liegen für ein $\omega \in \mathbb{F}_q$ mit $\omega^3 = 1$ und $\omega \neq 1$ in $\mathrm{GL}(3,q)$. Ihre Bilder $\overline{X}, \overline{Y}, \overline{Z}$ in $\mathrm{PGL}(3,q)$ sind offenbar verschieden und dort auch paarweise nicht $\mathbb{Q}$-konjugiert, weil Z in $\mathrm{GL}(3,q)$ zu keiner Diagonalmatrix konjugiert ist (siehe z. B. [47]) und X im Gegensatz zu Y in $\mathrm{SL}(3,q)$ liegt.

Offenbar beinhaltet die $\mathbb{Q}$-Klasse von $\overline{X}$ in G genau die Elemente der Ordnung 3 aus N. Daher kann $\overline{X}$ auch in G nicht $\mathbb{Q}$-konjugiert zu $\overline{Y}$ oder $\overline{Z}$ sein. Wären zudem $\overline{Y}$ und $\overline{Z}$ in G nicht $\mathbb{Q}$-konjugiert, so lägen mindestens vier $\mathbb{Q}$-Klassen von 3-Elementen in G. Falls sie andererseits $\mathbb{Q}$-konjugiert in G wären, würde G/N transitiv auf der Menge der beiden $\mathbb{Q}$-Klassen von $\overline{Y}$ und $\overline{Z}$ operieren. Daher müsste G/N gerade Ordnung haben, womit es mindestens vier $\mathbb{Q}$-Klassen von 2-Elementen in G gäbe. Beide Fälle sind nach Folgerung 2.14 nicht möglich.

Nach Ennola [21] ist jede Konjugationsklasse von $\mathrm{GU}(3,q)$ der Durchschnitt von $\mathrm{GU}(3,q)$ mit einer Konjugationsklasse von $\mathrm{GL}(3,q)$. Deshalb enthält G auch dann mindestens vier $\mathbb{Q}$-Klassen von 2-Elementen oder mindestens vier $\mathbb{Q}$-Klassen von 3-Elementen, wenn G eine zu $\mathrm{PGU}(3,q)$ isomorphe Untergruppe besitzt.

Schließlich verbleibt nur noch der Fall $N \cong \mathrm{PSU}(3,4)$. Dann besitzt N zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung 5. Seien x und y Repräsentanten dieser beiden Klassen. Dann ist einer dieser Repräsentanten (o. B. d. A. y) in N zu seinem Inversen konjugiert, während dies für den anderen nicht gilt. Die Ordnung von G/N ist ungerade, weil N Elemente der Ordnung 4 enthält. Damit liegen x und y auch in G in verschiedenen $\mathbb{Q}$-Klassen und die $\mathbb{Q}$-Klassen von x und y zerfallen in G jeweils in genauso viele Konjugationsklassen wie in N. Für die folgende Argumentation können wir daher $G = N$ annehmen.

Sei $\mathfrak{p}$ das maximale Ideal von $\mathcal{O}_{\mathbb{Q}(\zeta_5)}$, das die 5 enthält. Für jeden irreduziblen Charakter $\chi \in \mathrm{Irr}(G)$ gilt $\chi(1) \equiv \chi(x) \pmod{\mathfrak{p}^2}$, denn mithilfe von GAP lässt sich schnell nachprüfen, dass 25 ein Teiler von $N_{\mathbb{Q}(\zeta_5)/\mathbb{Q}}(\chi(1) - \chi(x))$ ist. Entsprechend gilt $\eta(1) \equiv \eta(x) \pmod{\mathfrak{p}^2}$ auch für jedes $\eta \in R(G)_5$. Sei $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Dann liegen die Funktionen φ_1, φ_2, φ_3 und φ_4 mit

$$\varphi_1(g) = \begin{cases} 1, & g = 1 \\ 0, & \text{sonst} \end{cases}, \qquad \varphi_2(g) = \begin{cases} 1, & g \sim x^k \text{ für ein } k \in \{1,\dots,4\} \\ 0, & \text{sonst} \end{cases},$$

$$\varphi_3(g) = \begin{cases} \pi, & g \sim x \\ 0, & g \nsim x^k \text{ für ein } k \in \{1,\dots,4\} \end{cases} \quad \text{und}$$

$$\varphi_4(g) = \begin{cases} 1, & g \sim y^k \text{ für ein } k \in \{1,\dots,4\} \\ 0, & \text{sonst} \end{cases}$$

alle in $R(G)'_5 \setminus R(G)_5$. Es lässt sich zeigen, dass zu keinen Funktionen $\alpha_1, \alpha_2 \in R(G)'_5$ Elemente $\eta_i, \xi_i, \psi_i \in R(G)$, $i = 1, \ldots, 4$, existieren, sodass das Gleichungssystem

$$\begin{aligned} \eta_1\alpha_1 + \xi_1\alpha_2 + \psi_1 &= \varphi_1\,, & \eta_2\alpha_1 + \xi_2\alpha_2 + \psi_2 &= \varphi_2 \\ \eta_3\alpha_1 + \xi_3\alpha_2 + \psi_3 &= \varphi_3\,, & \eta_4\alpha_1 + \xi_4\alpha_2 + \psi_4 &= \varphi_4 \end{aligned}$$

erfüllt ist. Die Rechnung ist etwas langwierig, wir verzichten an dieser Stelle darauf. Prinzipiell funktioniert sie so ähnlich wie die obige Rechnung im Abschnitt zur $\mathrm{PSL}(2, q)$ mit $q \equiv 1 \pmod 4$. Bei der Rechnung hier muss man die Gleichungen modulo $\mathfrak{p}^2$ statt modulo p^2 betrachten und außerdem noch die Fälle unterscheiden, ob nur eine der Zahlen $\alpha_1(x)$ und $\alpha_2(x)$ oder beide in $\mathfrak{p} \setminus \mathfrak{p}^2$ liegen.

Da der $R(G)_5$-Modul $R(G)'_5/R(G)_5$ also mindestens drei Erzeuger benötigt, hat $R(G)$ auch im Fall $N \cong \mathrm{PSU}(3, 4)$ unendlichen Darstellungstyp.

• $\mathrm{PSL}(4, q)$ und $\mathrm{PSU}(4, q)$

Die Gruppen $\mathrm{PSL}(4, q)$ und $\mathrm{PSU}(4, q)$ enthalten für ungerade q allesamt Elemente der Ordnung 8, weil schon $\mathrm{PSL}(3, q)$ bzw. $\mathrm{PSU}(3, q)$ für ungerade q Elemente der Ordnung 8 besitzen. Somit kann N zu keiner dieser Gruppen isomorph sein, wenn $R(G)$ endlichen Darstellungstyp hat. Außerdem gibt es für gerade q in den Gruppen $\mathrm{PSL}(4, q)$ (nach [19]) und $\mathrm{PSU}(4, q)$ (nach [20]) jeweils zwei Klassen von Involutionen. Wenn N für ein gerades q zu $\mathrm{PSL}(4, q)$ oder $\mathrm{PSU}(4, q)$ isomorph ist, enthält somit auch G nach Satz 1.53 mindestens zwei Klassen von Involutionen. Folglich hätte $R(G)$ unendlichen Darstellungstyp.

• ${}^3D_4(q)$

Die Konjugationsklassen der Gruppen ${}^3D_4(q)$ wurden in [16] bestimmt. Insbesondere lässt sich diesem Artikel entnehmen, dass es in ${}^3D_4(q)$ Elemente der Ordnung 8 gibt. Ist $N \cong {}^3D_4(q)$, so hat $R(G)$ demnach unendlichen Darstellungstyp.

• $G_2(q)$

Auch die Gruppen $G_2(q)$ enthalten allesamt Elemente der Ordnung 8, wie man [37] (für ungerade q) und [10] (für gerade q) entnehmen kann. Somit ist N nicht zu $G_2(q)$ isomorph, wenn $R(G)$ endlichen Darstellungstyp hat.

• ${}^2G_2(3^{2n+1})$

Sei nun $N \cong {}^2G_2(3^{2n+1})$. Nach [52] sind die 3-Sylowgruppen von N nichtabelsch vom Exponenten 9 und zwei verschiedene Sylowgruppen $P_1, P_2 \in \mathrm{Syl}_3(N)$ schneiden sich trivial. Zudem gibt es sowohl in $Z(P_1)$ als auch in $P_1 \setminus Z(P_1)$ Elemente der Ordnung 3. Folglich liegen diese in verschiedenen $\mathbb{Q}$-Klassen von G, weshalb in G mindestens vier $\mathbb{Q}$-Klassen von 3-Elementen zu finden sind und $R(G)$ unendlichen Darstellungstyp hat.

• ${}^2B_2(2^{2n+1})$

Unter den Gruppen vom Lie-Typ verbleiben jetzt nur noch die Suzuki-Gruppen. Sei N zu einer der Suzuki-Gruppen ${}^2B_2(2^{2n+1})$ isomorph und $P \in \mathrm{Syl}_2(N)$. Nach [49] gilt dann $|P| = |Z(P)|^2$ und die Involutionen von P werden durch eine zyklische Untergruppe von N transitiv permutiert. Nach [28] ist P damit eine Suzuki 2-Gruppe vom Typ A. In Proposition 3.11 zeigen wir, dass die 2-Sylowgruppe einer beliebigen endlichen Gruppe H nicht zu einer Suzuki 2-Gruppe vom Typ A isomorph sein kann, wenn $R(H)$ endlichen Darstellungstyp hat. Da die Ordnung von G/N ungerade sein muss, kann N demnach zu keiner der Gruppen ${}^2B_2(2^{2n+1})$ isomorph sein.

• Sporadische Gruppen

Sei N schließlich eine sporadische einfache Gruppe aus der Liste in Satz 1.53. Ist $N \in \{M_{11}, M_{22}, M_{23}, J_3, McL, O'N, Ly, Th\}$, so besitzt N laut [9] Elemente der Ordnung 8, womit $R(G)$ unendlichen Darstellungstyp hat. Demzufolge muss $N = J_1$ gelten.

Nachdem wir die Betrachtung für einfache Gruppen N abgeschlossen haben, setzen wir jetzt voraus, dass N eine quasieinfache Gruppe mit $Z(N) \neq 1$ ist. Nach Lemma 3.1 hat $N/Z(N)$ mindestens genauso viele $\mathbb{Q}$-Klassen von p-Elementen wie N für $p \in \mathbb{P}$. Wir müssen demnach nur die Fälle, dass $N/Z(N)$ isomorph zu $\mathrm{PSL}(2,q)$, A_7, J_1, $\mathrm{PSU}(3,4)$ oder ${}^2B_2(2^{2n+1})$ ist, untersuchen.

Die Schurmultiplikatoren von $\mathrm{PSL}(2,2^n)$ $(n > 2)$, $\mathrm{PSU}(3,4)$, ${}^2B_2(2^{2n+1})$ $(n > 1)$ und J_1 sind trivial. Ist $N/Z(N)$ isomorph zu einer dieser Gruppen, so folgt also $Z(N) = 1$. Der Schurmultiplikator von ${}^2B_2(8)$ ist zu C_2^2 isomorph. Aus $N/Z(N) \cong {}^2B_2(8)$ und $Z(N) \neq 1$ folgt demnach, dass es in G mehr als drei $\mathbb{Q}$-Klassen von 2-Elementen gibt. Schließlich ist $\mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5)$, es verbleibt also, $N/Z(N) \cong A_7$ und $N/Z(N) \cong \mathrm{PSL}(2,q)$, $q > 3$ ungerade, zu betrachten.

Ist $N/Z(N)$ zu A_6 oder A_7 isomorph, so gibt es bereits je zwei $\mathbb{Q}$-Klassen von 2- bzw. 3-Elementen in $N/Z(N)$ und der Schurmultiplikator von $N/Z(N)$ ist zu C_6 isomorph. Wären die beiden $\mathbb{Q}$-Klassen von Elementen der Ordnung 3 in G konjugiert, so müsste G/N gerade Ordnung haben. Damit lägen in G aber zu viele $\mathbb{Q}$-Klassen von 2-Elementen, denn sowohl A_6 als auch A_7 enthalten Elemente der Ordnung 4. Im Fall $Z(N) \neq 1$ gäbe es dementsprechend zu viele $\mathbb{Q}$-Klassen von 2- bzw. 3-Elementen in G, als dass $R(G)$ endlichen Darstellungstyp haben könnte.

Sei $N/Z(N) \cong \mathrm{PSL}(2,q)$, $q > 3$ ungerade. Wegen $\mathrm{PSL}(2,9) \cong A_6$ nehmen wir zudem $q \neq 9$ an. Dann ist der Schurmultiplikator von $N/Z(N)$ zu C_2 isomorph und im Fall $Z(N) \neq 1$ folgt damit $N \cong \mathrm{SL}(2,q)$. Ist $q = p^k$ für ein $k \geq 3$, so folgt mit derselben Begründung wie für $\mathrm{PSL}(2,q)$, dass $R(G)$ unendlichen Darstellungstyp hat. Da $\mathrm{SL}(2,q)$ Elemente der Ordnung $q+1$ und $q-1$ enthält, impliziert Folgerung 2.14, dass $q-1$ und $q+1$ kubikfrei sein müssen. Für jede ungerade Primzahl p ist p^2-1 aber durch 8 teilbar, also kann $N/Z(N)$ nur dann zu $\mathrm{SL}(2,q)$ isomorph sein, wenn q bereits prim ist.

Zum Abschluss zeigen wir noch, dass $|N|$ und $|G : N|$ teilerfremd sind. Da N zu einer der Gruppen $\mathrm{PSL}(2, q)$, $\mathrm{SL}(2, p)$, A_7 oder J_1 isomorph sein muss, gibt es kein nichttriviales Element ungerader Ordnung in N, das eine 2-Sylowgruppe von N zentralisiert. Wie bereits bemerkt, darf $G \setminus N$ keine Involution enthalten.

Angenommen es existieren p-Elemente $x \in N$ und $y \in G \setminus N$ für eine ungerade Primzahl p. Kommutiert y mit jedem Element aus N, so liegen y und xy in verschiedenen $\mathbb{Q}$-Klassen von G, da y im Gegensatz zu xy eine 2-Sylowgruppe von G zentralisiert. Weiter können beide Elemente natürlich nicht in der $\mathbb{Q}$-Klasse von x in G liegen, da sie nicht in N enthalten sind. Folglich hätte G mindestens vier $\mathbb{Q}$-Klassen von p-Elementen und $R(G)$ somit unendlichen Darstellungstyp.

Sicherlich liegt auch kein Element der Ordnung 4, das N zentralisiert, in $G \setminus N$, denn dessen Quadrat müsste in N liegen. Daher operiert jedes Element aus $G \setminus N$, dessen Ordnung nicht teilerfremd zu $|N|$ ist, nichttrivial auf N.

Die äußere Automorphismengruppe der J_1 ist trivial und die der A_7 hat die Ordnung 2. Da A_7 Elemente der Ordnung 4 besitzt, folgt sofort $G = N$, wenn N zu einer dieser beiden Gruppen isomorph ist.

Weiter hat $\mathrm{PSL}(2, \ell^f)$ für eine ungerade Primzahl ℓ eine Gruppe der Ordnung $2f$ als äußere Automorphismengruppe. Wir haben bereits gesehen, dass N zu keiner der Gruppen $\mathrm{PSL}(2, \ell^f)$ mit $f > 2$ isomorph ist und G keine zu $\mathrm{PGL}(2, \ell^f)$ isomorphe Untergruppe enthält, wenn $R(G)$ endlichen Darstellungstyp hat. Somit kann es für $f = 1$ kein Element in $G \setminus N$ geben, das nichttrivial auf N operiert, und im Fall $f = 2$ müsste solch ein Element ein 2-Element sein. Ist $f = 2$, so liegen in N jedoch Elemente der Ordnung $\frac{\ell^2-1}{2}$ und damit Elemente der Ordnung 4. Daher ist $|G : N|$ ungerade.

Ebenso wenig kann es Elemente aus $G \setminus N$ geben, die nichttrivial auf N operieren, wenn N zu $\mathrm{SL}(2, \ell)$ isomorph ist: Auch in diesem Fall muss $|G : N|$ natürlich ungerade sein und jeder nichttriviale Automorphismus ungerader Ordnung der $\mathrm{SL}(2, \ell)$ induziert einen ebensolchen der $\mathrm{PSL}(2, \ell)$.

Sei also $N \cong \mathrm{PSL}(2, 2^f)$, dann ist die äußere Automorphismengruppe von N eine zyklische Gruppe der Ordnung f. Wir müssen den Fall betrachten, dass p ein Teiler von f und gleichzeitig ein Teiler von $2^f + 1$ oder $2^f - 1$ ist. Wir zeigen, dass dann auch p^2 ein Teiler von $2^f + 1$ bzw. $2^f - 1$ ist. Da es in N Elemente der Ordnung $2^f + 1$ und $2^f - 1$ gibt, bedeutet das, dass G mindestens vier $\mathbb{Q}$-Klassen von p-Elementen enthält, $R(G)$ also unendlichen Darstellungstyp hat.

Sei zunächst p ein Teiler von $2^f - 1$. Da p zusätzlich ein Teiler von f ist, gibt es eine natürliche Zahl k, sodass $f = kp$ gilt. Dann folgt $2^k \equiv (2^k)^p \equiv 2^f \equiv 1 \pmod{p}$. Damit ist aber in

$$2^{kp} - 1 = \left(2^k - 1\right) \cdot \left(2^{k(p-1)} + 2^{k(p-2)} + \ldots + 2^k + 1\right)$$

nicht nur der erste, sondern auch der zweite Faktor durch p teilbar, weil dessen p Summanden allesamt kongruent zu 1 modulo p sind. Folglich wird $2^f - 1$ von p^2 geteilt.

Sei jetzt p ein Teiler von f sowie von $2^f + 1$. Dann gibt es eine natürliche Zahl k, sodass $f = kp$ gilt und wir erhalten $2^k \equiv (2^k)^p \equiv 2^f \equiv -1 \pmod{p}$. Auch hier sind dann in

$$2^{kp} + 1 = \left(2^k + 1\right) \cdot \left(2^{k(p-1)} - 2^{k(p-2)} + - \ldots - 2^k + 1\right)$$

beide Faktoren durch p teilbar, weil p eine ungerade Primzahl und somit $2^{k(p-i)} \equiv (-1)^{i+1} \pmod{p}$ für $i \in \{1, \ldots, p\}$ ist. Folglich wird $2^f + 1$ von p^2 geteilt.

Damit sind nun alle Fälle, in denen $\mathrm{ggT}(|N|, |G : N|) > 1$ gelten könnte, ausgeschlossen, was den Beweis des Satzes abschließt. □

Folgerung 3.7. *Seien N ein nichtabelscher quasieinfacher Normalteiler von G und der Darstellungstyp von $R(G)$ endlich. Sei weiter $P \in \mathrm{Syl}_p(G)$ für eine ungerade Primzahl p, die $|N|$ teilt. Dann ist P abelsch.*

Beweis. Die p-Sylowgruppen von G sind nach Satz 3.6 mit den p-Sylowgruppen von N identisch, daher gehen wir einfach die dortige Liste der Gruppen durch. Für eine ungerade Primzahl p ist die p-Sylowgruppe von $\mathrm{PSL}(2, q)$ zyklisch, falls q keine p-Potenz ist, bzw. elementar-abelsch, wenn q eine p-Potenz ist. Ebenso ist jede p-Sylowgruppe von $\mathrm{SL}(2, q)$ für eine Primzahl q zyklisch. Außerdem sind für ungerade Primzahlen p die p-Sylowgruppen von A_7 und J_1 bekanntlich ebenfalls abelsch. □

Die Charakterringe der Gruppen in der Liste von Satz 3.6 haben übrigens tatsächlich alle endlichen Darstellungstyp. Wir werden in Abschnitt 4.1 sehen, dass $R(G)_p$ endlichen Darstellungstyp hat, wenn die p-Sylowgruppen von G zyklisch der Ordnung $\leq p^2$ sind. Demzufolge müssen wir $R(G)_p$ nur für die Primzahlen p betrachten, für die die p-Sylowgruppen von G nicht zyklisch sind.

Zu jeder Gruppe aus der obigen Liste und jeder solchen Primzahl p kann man mit einem Blick auf die jeweilige Charaktertafel (siehe Anhang bzw. [9] für J_1) feststellen, dass jede rationale p'-Sektion höchstens zwei $\mathbb{Q}$-Klassen enthält und jede dieser $\mathbb{Q}$-Klassen bereits eine Konjugationsklasse ist. Ist G eine Gruppe aus der Liste, so ist es zudem sowohl für $G \cong \mathrm{PSL}(2, p^2)$ leicht zu zeigen, dass $\mathrm{rad}(R(G)'_p/R(G)_p)$ zyklisch ist, als auch für $G \cong \mathrm{PSL}(2, p^f)$, dass $\mathrm{rad}(R(G)'_2/R(G)_2)$ zyklisch ist ($f \in \{1, 2\}$). Ebenso werden $\mathrm{rad}(R(A_7)'_2/R(A_7)_2)$ und $\mathrm{rad}(R(A_7)'_3/R(A_7)_3)$ von jeweils einem Element erzeugt. Mit diesen Aussagen folgt die Behauptung dann schnell.

3.2 2-Sylowgruppen

Jetzt wollen wir zur Liste der Gruppen kommen, die als 2-Sylowgruppen einer Gruppe G, deren Charakterring endlichen Darstellungstyp hat, auftreten können. Zuvor geben wir noch ein Lemma zu den Untergruppen von $\Gamma\mathrm{L}(p^n)$, die transitiv auf den eindimensionalen Unterräumen von $\mathbb{F}_p^n$ operieren ($p \in \mathbb{P}$, $n \in \mathbb{N}$), sowie eines, mit dessen Hilfe wir die Suzuki 2-Gruppen vom Typ A als 2-Sylowgruppen von G ausschließen werden, an.

Lemma 3.8. *Seien $p \in \mathbb{P}$, $n \in \mathbb{N}$ und G eine Untergruppe von $\Gamma\mathrm{L}(p^n)$, die transitiv auf den eindimensionalen Unterräumen von $\mathbb{F}_p^n$ operiert. Für jeden Primteiler p_i von $d := \mathrm{ggT}\left(\frac{p^n-1}{p-1}, p-1\right)$ sei außerdem $r_i \in \mathbb{Z}$ die größte Zahl, sodass $p_i^{r_i}$ ein Teiler von $p-1$ ist. Dann wird $\exp(G)$ von*

$$\frac{p^n-1}{p-1} \cdot \prod_{\substack{p_i \in \mathbb{P} \\ p_i \mid d}} p_i^{r_i}$$

geteilt.

Beweis. Wir betrachten die Operation von $\Gamma\mathrm{L}(p^n)$ auf $\mathbb{F}_p^n$ genauer. Für die Elemente aus $\Gamma\mathrm{L}_0(p^n)$ entspricht sie der Operation der Gruppe

$$H := \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_{p^n}^\times \right\} \quad \text{auf der Gruppe} \quad V := \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{F}_{p^n} \right\}$$

durch Konjugation. Die Elemente aus H, deren Ordnung $p-1$ teilt, stehen für Multiplikationen mit Elementen aus $\mathbb{F}_p^\times$. Eine echte Untergruppe von H, deren Ordnung kein Vielfaches von

$$\frac{p^n-1}{p-1} \cdot \prod_{\substack{p_i \in \mathbb{P} \\ p_i \mid d}} p_i^{r_i}$$

ist, kann daher das Element $X := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ nicht auf ein Element der Form $Y^j := \begin{pmatrix} 1 & jy \\ 0 & 1 \end{pmatrix}$ für einen Erzeuger y von $\mathbb{F}_{p^n}^\times$ und $j \in \{1, \ldots, p-1\}$ abbilden.

Für jeden Automorphismus $\alpha \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ gilt $\alpha(1) = 1$. Folglich kann keine Untergruppe von $\Gamma\mathrm{L}(p^n)$, die von Elementen aus $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ sowie Elementen einer Untergruppe von $\Gamma\mathrm{L}_0(p^n)$, deren Ordnung kein Vielfaches von

$$\frac{p^n-1}{p-1} \cdot \prod_{\substack{p_i \in \mathbb{P} \\ p_i \mid d}} p_i^{r_i}$$

ist, erzeugt wird, transitiv auf den eindimensionalen Unterräumen von $\mathbb{F}_p^n$ operieren. Nun hat jedoch jede weitere Untergruppe von $\Gamma\mathrm{L}(p^n)$ einen durch

$$\frac{p^n-1}{p-1} \cdot \prod_{\substack{p_i \in \mathbb{P} \\ p_i \mid d}} p_i^{r_i}$$

teilbaren Exponenten, weswegen auch der Exponent von G durch diese Zahl teilbar sein muss. □

Bemerkung 3.9. Auf analoge Weise kann man zeigen, dass der Exponent einer Untergruppe von $\Gamma\mathrm{L}(p^n)$, die transitiv auf den Vektoren von $\mathbb{F}_p^n \setminus \{0\}$ operiert, ein Vielfaches von $p^n - 1$ sein muss.

Lemma 3.10. *Sei $P \in \mathrm{Syl}_2(G)$ eine Suzuki 2-Gruppe vom Typ A. Dann sind die Elemente der Ordnung 4 in G nichtreell.*

Beweis. Aufgrund der Resistenz der Suzuki 2-Gruppen können wir $P \trianglelefteq G$ annehmen. Da dann G auf P operiert und $|G : P|$ ungerade ist, kann ein Element $x \in P$ der Ordnung 4 nur dann zu seinem Inversen konjugiert sein, wenn es bereits ein $y \in P$ mit $yxy^{-1} = x^{-1}$ gibt. Bekanntlich ist P isomorph zur Matrizengruppe

$$A(n,\Theta) := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & a^\Theta \\ 0 & 0 & 1 \end{pmatrix} : a, b \in \mathbb{F}_{2^n} \right\}$$

für eine positive ganze Zahl n und ein $\Theta \in \mathrm{Aut}(\mathbb{F}_{2^n})$ mit ungerader Ordnung > 1. Offenbar gilt

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & a^\Theta \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a & b + a^{1+\Theta} \\ 0 & 1 & a^\Theta \\ 0 & 0 & 1 \end{pmatrix}.$$

Sei $A \in A(n,\Theta)$ ein Element der Ordnung 4, d. h., es existieren $a, b \in \mathbb{F}_{2^n}$ mit $a \neq 0$, sodass

$$A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & a^\Theta \\ 0 & 0 & 1 \end{pmatrix}.$$

Wären A und A^{-1} konjugiert, so gäbe es $c, d \in \mathbb{F}_{2^n}$ mit

$$\begin{aligned} \begin{pmatrix} 1 & a & b + a^{1+\Theta} \\ 0 & 1 & a^\Theta \\ 0 & 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & c & d \\ 0 & 1 & c^\Theta \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & a^\Theta \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & c & d + c^{1+\Theta} \\ 0 & 1 & c^\Theta \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a + c & b + d + a^\Theta c \\ 0 & 1 & a^\Theta + c^\Theta \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & c & d + c^{1+\Theta} \\ 0 & 1 & c^\Theta \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a & d + c^{1+\Theta} + ac^\Theta + c^{1+\Theta} + b + d + a^\Theta c \\ 0 & 1 & a^\Theta \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a & b + ac^\Theta + a^\Theta c \\ 0 & 1 & a^\Theta \\ 0 & 0 & 1 \end{pmatrix}, \end{aligned}$$

d. h., es existiert ein $c \in \mathbb{F}_{2^n}$ mit $a^{1+\Theta} = a^\Theta c + ac^\Theta$. Insbesondere ist $c \neq a$. Nun gilt

$$\begin{aligned} & a^{1+\Theta} = a^\Theta c + ac^\Theta && \Leftrightarrow && a^\Theta c = a(a^\Theta + c^\Theta) \\ \Leftrightarrow \quad & a^{-1}c = 1 + (a^{-1}c)^\Theta && \Leftrightarrow && (a^{-1}c)^\Theta = 1 + a^{-1}c\,. \end{aligned}$$

Die letzte Gleichung bedeutet jedoch

$$(a^{-1}c)^{\Theta^2} = (1 + a^{-1}c)^\Theta = 1 + 1 + a^{-1}c = a^{-1}c\,.$$

Das steht wegen $a^{-1}c \neq 1$ im Widerspruch dazu, dass Θ von ungerader Ordnung ist. □

Proposition 3.11. *Seien $P \in \mathrm{Syl}_2(G)$ und der Darstellungstyp von $R(G)$ endlich. Dann kann P nicht isomorph zu einer Suzuki 2-Gruppe vom Typ A sein.*

Beweis. Angenommen, P wäre eine Suzuki 2-Gruppe vom Typ A. Dann sind die Elemente der Ordnung 4 in P und damit auch in G nach Lemma 3.10 nichtreell. Weil $Z(P) = P' = \Omega_1(P)$ gilt (siehe [28] – $\Omega_1(P)$ steht hier für das Erzeugnis aller Involutionen von P), kann ein linearer Charakter $\lambda \in \mathrm{Irr}(P)$ nur die Werte 1 oder -1 auf den Elementen der Ordnung 4 annehmen und es gilt $\chi(z) = \pm\chi(1)$ für $z \in Z(P)$ und $\chi \in \mathrm{Irr}(P)$. Zudem ist der Grad jedes nichtlinearen irreduziblen Charakters von P eine 2er-Potenz, weswegen alle Werte nichtlinearer Charaktere im 2 enthaltenden maximalen Ideal von $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$, genauer in $(1+i)\mathbb{Z}[i]$, liegen.

Sei $x \in P$ ein Element der Ordnung 4. Ist χ der Charakter der irreduziblen Darstellung ϱ, so sind die Eigenwerte von $\varrho(x^2)$ also entweder alle gleich 1 oder alle gleich -1. Daher liegen alle Eigenwerte von $\varrho(x)$ entweder in $\{1,-1\}$ oder in $\{i,-i\}$. Folglich liegt $\chi(x)$ nicht nur in $(1+i)\mathbb{Z}[i]$, sondern sogar im von 2 erzeugten Ideal. Dementsprechend liegt für jeden nichtlinearen Charakter $\psi \in \mathrm{Irr}(G)$ auch $\psi(x)$ in $\mathbb{Z} + 2\mathbb{Z}[i]$. Weiter existiert ein irreduzibler Charakter $\varphi \in \mathrm{Irr}(G)$ mit $\varphi(x) \notin \mathbb{R}$, weil x nichtreell ist. Damit folgt sofort $\mathbb{Q}(\mathrm{cl}_G(x)) = \mathbb{Q}(i)$. Folglich liegt die Funktion φ_x mit

$$\varphi_x(g) = \begin{cases} 1+i, & g \sim_G x \\ 1-i, & g \sim_G x^{-1} \\ 0, & \text{sonst} \end{cases}$$

in $\mathrm{rad}(R(G)_2') \setminus R(G)_2$.

Ferner liegt natürlich auch die Funktion φ_1 mit $\varphi_1(1) = 2$ und $\varphi_1(g) = 0$ sonst in $\mathrm{rad}(R(G)_2') \setminus R(G)_2$. Angenommen der $R(G)_2$-Modul $\mathrm{rad}(R(G)_2'/R(G)_2)$ wäre zyklisch. Dann gäbe es Funktionen $\alpha \in \mathrm{rad}(R(G)_2')$ und $\eta_1, \eta_2, \xi_1, \xi_2 \in R(G)_2$ mit $\eta_1\alpha + \xi_1 = \varphi_1$ und $\eta_2\alpha + \xi_2 = \varphi_x$. Da $\alpha(x)$ und $\varphi_x(x)$ beide in $(1+i)\mathbb{Z}[i]$ liegen, muss auch $\xi_2(x) \in (1+i)\mathbb{Z}[i]$ gelten. Dann ist aber $\xi_2(x)$ sogar in $2\mathbb{Z}[i]$ enthalten, womit $\alpha(x) \in (1+i)\mathbb{Z}[i] \setminus 2\mathbb{Z}[i]$ folgt.

Des Weiteren muss $(\eta_1\alpha + \xi_1)(x) = 0$ gelten. Wie eben folgt $\xi_1(x) \in 2\mathbb{Z}[i]$, also muss auch $\eta_1\alpha(x) \in 2\mathbb{Z}[i]$ sein. Wegen $\alpha(x) \in (1+i)\mathbb{Z}[i] \setminus 2\mathbb{Z}[i]$ gilt somit $\eta_1(x) \in (1+i)\mathbb{Z}[i]$ und daher $\eta_1(1) \in 2\mathbb{Z}$. Sicherlich gilt auch $\alpha(1) \in 2\mathbb{Z}$, also ist $\eta_1\alpha(1) \equiv 0 \pmod 4$. Damit muss $\xi_1(1) \equiv 2 \pmod 4$ sein.

Weil $x^2 \in Z(P) \cap P'$ ist, gilt für jeden Charakter $\psi \in \mathrm{Irr}(P)$ die Kongruenz $\psi(1) \equiv \psi(x^2) \pmod 4$. Demzufolge erhalten wir auch $\chi(1) \equiv \chi(x^2) \pmod 4$ für jedes $\chi \in \mathrm{Irr}(G)$, denn χ_P ist eine $\mathbb{Z}$-Linearkombination irreduzibler Charaktere von P. Wegen $\xi_1 \in R(G)_2$ ergibt sich also $\xi_1(x^2) \equiv \xi_1(1) \equiv 2 \pmod 4$.

Dagegen ist $\eta_1\alpha(x^2)$ durch 4 teilbar, weil mit $\eta_1(1)$ auch $\eta_1(x)$ gerade ist und α in $\mathrm{rad}(R(G)_2')$ liegt. Das bedeutet aber, dass $(\eta_1\alpha + \xi_1)(x^2) \equiv 2 \not\equiv 0 \equiv \varphi_1(x^2) \pmod 4$ ist. Folglich ist der $R(G)_2$-Modul $\mathrm{rad}(R(G)_2'/R(G)_2)$ nicht zyklisch, womit $R(G)$ unendlichen Darstellungstyp hat. □

Nun haben wir alles Notwendige beisammen, um die Liste möglicher 2-Sylowgruppen angeben zu können.

Satz 3.12. *Sei G eine Gruppe gerader Ordnung, deren Charakterring $R(G)$ endlichen Darstellungstyp hat. Dann sind die 2-Sylowgruppen von G isomorph zu einer der folgenden Gruppen:*

1. *C_2^n für ein $n \in \mathbb{N}$, wobei $2^n - 1$ kubikfrei ist,*
2. *C_4,*
3. *Q_8,*
4. *einer 2-Sylowgruppe von $\mathrm{PSU}(3, 2^n)$ für ein $n \geq 2$, wobei $2^{2n} - 1$ kubikfrei ist,*
5. *der Suzuki 2-Gruppe $S = \langle x_1, x_2, x_3, x_4, x_5, x_6 \rangle$ der Ordnung 2^9 mit $x_i^4 = [x_i^2, x_j] = 1$ und $x_1^2 = x_4^2 = [x_1, x_4]$, $x_2^2 = x_5^2 = [x_2, x_5]$, $x_1^2 x_2^2 = x_3^2 = x_6^2 = [x_3, x_6]$, $[x_1, x_3] = x_2^2[x_1, x_2] = [x_1, x_5]$, $[x_1, x_6] = x_1^2$, $[x_2, x_3] = x_1^2 x_2^2 = [x_5, x_6]$, $[x_2, x_4] = x_2^2$, $[x_2, x_6] = x_1^2 x_2^2 [x_1, x_2] = [x_3, x_4]$, $[x_3, x_5] = [x_1, x_2] = [x_4, x_5]$,*
6. *D_8.*

Beweis. Sei $P \in \mathrm{Syl}_2(G)$. Ist $E(G) \neq 1$, so ist $E(G)$ nach Satz 3.6 eine Hallgruppe von G. Also kann man $G = E(G) \rtimes H$ für eine geeignete Untergruppe H schreiben und P ist eine 2-Sylowgruppe von $E(G)$. Da G nach Proposition 3.5 nur einen nichtabelschen Kompositionsfaktor haben kann, folgt mit Satz 3.6, dass P entweder elementar-abelsch oder isomorph zu Q_8 bzw. D_8 ist.

Sei G nicht auflösbar, aber $E(G) = 1$. Die 2-Sylowgruppe von $G/O_{2'}(G)$ ist isomorph zu der von G und nach Lemma 3.1 enthält $G/O_{2'}(G)$ höchstens so viele $\mathbb{Q}$-Klassen von 2-Elementen wie G. Wir können also $O_{2'}(G) = 1$ annehmen und erhalten entweder den schon betrachteten Fall $E(G) \neq 1$ oder $F^*(G) = O_2(G)$.

Sei also $F^*(G) = O_2(G)$. Da G unserer Annahme gemäß nicht auflösbar ist, muss $O_2(G)$ eine echte Untergruppe von P sein. Die Elemente aus $P \setminus O_2(G)$ können zu den nichttrivialen Elementen aus $O_2(G)$ nicht konjugiert sein, da $O_2(G)$ ein Normalteiler von G ist. Somit darf es nach Folgerung 2.14 nur eine $\mathbb{Q}$-Klasse von nichttrivialen Elementen in $O_2(G)$ geben, d. h., alle Elemente $\neq 1$ in $O_2(G)$ sind in G konjugiert. Folglich operiert G transitiv auf $O_2(G) \setminus \{1\}$ und es gilt $C_G(O_2(G)) = O_2(G)$. Damit muss $G/O_2(G)$ isomorph zu einer Gruppe aus der Liste in Satz 1.52 sein und alle nichttrivialen 2-Elemente in $G/O_p(G)$ sind konjugiert.

Der einzig mögliche Fall ist daher der, dass $G/O_2(G)$ einen zu $\mathrm{SL}(2, 2^m)$ isomorphen Normalteiler besitzt, wobei $m \in \mathbb{N}$ so gewählt werden muss, dass $O_2(G) \cong C_2^{2m}$ gilt. Nach [11, Lemma 4.2] existiert dann jedoch eine Involution in $G \setminus O_2(G)$. Lemma 3.3 impliziert nun, dass $R(G)$ unendlichen Darstellungstyp hat. Der Fall $F^*(G) = O_2(G)$ kann also nicht auftreten, wenn G nicht auflösbar ist.

Wir nehmen schließlich an, dass G auflösbar ist. Besitzt P lediglich eine Involution, so ist P nach Satz 1.46 isomorph zu einer zyklischen Gruppe oder einer verallgemeinerten Quaternionengruppe. Die einzigen dieser Gruppen, deren Exponent nicht

von 8 geteilt wird, sind die zyklischen Gruppen der Ordnung 2 und 4 sowie die Quaternionengruppe Q_8. Somit muss P zu einer dieser Gruppen isomorph sein, wenn P nur eine Involution beinhaltet.

Es verbleibt der Fall, dass P mehr als eine Involution besitzt. Nach Satz 1.48 kann P dann nur homozyklisch oder eine Suzuki 2-Gruppe sein.

Ist P homozyklisch, so muss P nach Satz 3.2 elementar-abelsch sein, d. h. $P \cong C_2^n$ für eine positive ganze Zahl n. Nach Lemma 3.3 sind alle Elemente der Ordnung 2 in P konjugiert. Demnach operiert $G/C_G(P)$ transitiv auf $P \setminus \{1\}$, ist also eine lineare transitive Gruppe. Nach Satz 1.52 ist $G/C_G(P)$ daher eine Untergruppe von $\Gamma\mathrm{L}(2^n)$ und es folgt nach Lemma 3.8, dass $\exp(G/C_G(P))$ ein Vielfaches von $2^n - 1$ ist. Daher darf $2^n - 1$ von keiner dritten Potenz einer Primzahl geteilt werden.

Falls P eine Suzuki 2-Gruppe ist, hat P den Exponenten 4. Folgerung 2.14 und die Tatsache, dass P resistent ist, implizieren, dass alle zyklischen Untergruppen gleicher Ordnung von P in G konjugiert sind. Laut Satz 1.50 ist P daher vom Typ A oder isomorph zu S bzw. einer 2-Sylowgruppe von $\mathrm{PSU}(3, 2^n)$. Eine Suzuki 2-Gruppe vom Typ A kann aber nach Proposition 3.11 keine 2-Sylowgruppe von G sein.

Sei schließlich P eine 2-Sylowgruppe von $\mathrm{PSU}(3, 2^n)$ für ein $n \in \mathbb{N}$ mit $n \geq 2$. Dann ist P resistent, also operiert $N_G(P)$ transitiv auf den Elementen der Ordnung 4 von P. Demzufolge muss $N_G(P)/Z(P)$ transitiv auf $P/Z(P)$ operieren. Die Gruppe $P/Z(P)$ ist elementar-abelsch der Ordnung $\frac{2^{3n}}{2^n} = 2^{2n}$. Der Exponent von G ist nach Lemma 3.8 damit sowohl durch $2^n - 1$ teilbar, weil alle Involutionen aus P in G konjugiert sind, als auch durch $2^n + 1$. Das impliziert, dass $2^{2n} - 1$ kubikfrei sein muss. □

Zu jeder 2-Gruppe P aus der Liste in Satz 3.12 gibt es tatsächlich eine Gruppe G, sodass P eine 2-Sylowgruppe von G ist und $R(G)$ endlichen Darstellungstyp hat. Für $P \cong C_2$ bzw. $P \cong C_4$ kann man $G = P$ wählen, ist $P \cong Q_8$, so erfüllt $G \cong \mathrm{SL}(2, 3)$ die Eigenschaften und im Fall $P \cong D_8$ tut dies beispielsweise $G \cong \mathrm{PSL}(2, 7)$. Für $P \cong C_2^n$ und $G \cong C_2^n \rtimes C_{2^n-1}$, wobei C_{2^n-1} auf C_2^n wie $\Gamma\mathrm{L}_0(2^n)$ auf $\mathbb{F}_2^n$ operiert, hat $R(G)$ genau dann endlichen Darstellungstyp, wenn $2^n - 1$ kubikfrei ist.

Sei S die Suzuki 2-Gruppe der Ordnung 2^9 aus der Liste in Satz 3.12, die keine 2-Sylowgruppe von $\mathrm{PSU}(3, 8)$ ist. In [54] zeigt Wilkens, dass es eine (nichtabelsche) Gruppe Y der Ordnung 63 mit zyklischer 3-Sylowgruppe gibt, sodass in der Gruppe $G := S \rtimes Y$ die zyklischen Untergruppen gleicher Ordnung von S konjugiert sind. Zudem sind alle Elemente aus S reell, also hat $R(G)$ endlichen Darstellungstyp.

Schließlich existiert ein Automorphismus der Ordnung $2^{2n}-1$, sodass die von ihm erzeugte Gruppe die Konjugationsklassen von zyklischen Untergruppen der Ordnung 4 einer 2-Sylowgruppe P von $\mathrm{PSU}(3, 2^n)$ sowie die nichttrivialen Zentrumselemente transitiv permutiert (siehe z. B. [54]). Ist $2^{2n} - 1$ kubikfrei, so hat der Charakterring des entsprechenden semidirekten Produkts $P \rtimes C_{2^{2n}-1}$ endlichen Darstellungstyp.

3.3 Sylowgruppen ungerader Ordnung

Nach den möglichen Sylowgruppen gerader Ordnung wollen wir jetzt die möglichen Sylowgruppen ungerader Ordnung einer Gruppe G, deren Charakterring endlichen Darstellungstyp hat, bestimmen. Wir werden schlussendlich zu der Aussage gelangen, dass die Sylowgruppen ungerader Ordnung von G abelsch sind. Einen ersten Schritt hin zu dieser Aussage gehen wir mit dem folgenden Lemma.

Lemma 3.13. *Seien $p \in \mathbb{P}$ ungerade, $P \in \mathrm{Syl}_p(G)$ nichtabelsch und der Darstellungstyp von $R(G)$ endlich. Besitzt G drei $\mathbb{Q}$-Klassen von p-Elementen, so sind alle nichttrivialen Elemente aus $Z(P)$ in G konjugiert.*

Beweis. Wir zeigen zunächst, dass die Elemente aus $Z(P) \setminus \{1\}$ allesamt in einer der beiden nichttrivialen $\mathbb{Q}$-Klassen von p-Elementen liegen.

Besitzt G eine Komponente, deren Ordnung von p geteilt wird, so enthält $E(G)$ nach Satz 3.6 eine p-Sylowgruppe von G. Folgerung 3.7 impliziert dann jedoch, dass P abelsch ist. Also folgt $p \nmid |E(G)|$. Ist $E(G) \neq 1$, so hat $G/E(G)$ demnach zu P isomorphe p-Sylowgruppen und nach Lemma 3.1 höchstens so viele $\mathbb{Q}$-Klassen von p-Elementen wie G. Zudem ist für ein p-Element $x \in G$ die Konjugationsklasse $xE(G)$ in $G/E(G)$ rational, wenn die Konjugationsklasse von x in G rational ist.

Wir nehmen daher im Folgenden $E(G) = 1$ an. Da die p-Sylowgruppen von G und $G/O_{p'}(G)$ isomorph sind, setzen wir außerdem $O_{p'}(G) = \{1\}$ voraus. Lemma 3.1 liefert auch hier, dass es in $G/O_{p'}(G)$ höchstens so viele $\mathbb{Q}$-Klassen wie in G gibt und dass das Bild einer rationalen Konjugationsklasse von G eine rationale Konjugationsklasse in $G/O_{p'}(G)$ ist.

Sei also $F^*(G) = O_p(G)$, dann folgt $C_G(O_p(G)) \leq O_p(G)$. Im Fall $O_p(G) < P$ ist daher $Z(P) \leq O_p(G)$ und da die Elemente aus $P \setminus O_p(G)$ in G nicht zu denen aus $O_p(G)$ konjugiert sein können, gibt es zwei nichttriviale $\mathbb{Q}$-Klassen von p-Elementen. Von diesen kann nur eine Elemente aus $O_p(G)$ enthalten und nur in dieser können auch Elemente aus $Z(P)$ liegen. Im Fall $O_p(G) = P$ ist P ein Normalteiler von G, weswegen auch $Z(P)$ ein Normalteiler von G sein muss. Da P nichtabelsch ist, müssen die Elemente aus $P \setminus Z(P)$ demnach in einer anderen $\mathbb{Q}$-Klasse von G liegen. Natürlich gilt auch $P \setminus Z(P) \neq \emptyset$, sodass es tatsächlich eine $\mathbb{Q}$-Klasse in G gibt, die keine Elemente aus $Z(P)$ enthält.

Es verbleibt also zu zeigen, dass die $\mathbb{Q}$-Klasse von G, die die nichttrivialen Elemente aus $Z(P)$ beinhaltet, eine rationale Konjugationsklasse ist. Bekanntlich existiert ein $z \in Z(P) \cap P'$ mit $z \neq 1$. Wir zeigen, dass dieses z in einer rationalen Konjugationsklasse von G liegen muss.

Wir nehmen an, dass die Konjugationsklasse von z in G nicht rational ist. Das p enthaltende maximale Ideal von $\mathcal{O}_{\mathbb{Q}(\mathrm{cl}_G(z))}$ bezeichnen wir mit $\mathfrak{p}$.

Für jeden linearen Charakter $\lambda \in \mathrm{Irr}(P)$ gilt $\lambda(z) = 1$ wegen $z \in P'$. Außerdem gibt es bekanntlich zu jedem $\psi \in \mathrm{Irr}(P)$ ein $k \in \mathbb{Z}$, sodass $\psi(z) = \psi(1) \cdot \zeta_p^k$ ist. Da P

eine p-Gruppe ist, muss $\psi(1)$ hierbei eine p-Potenz sein. Die Einschränkung eines Charakters $\chi \in \mathrm{Irr}(G)$ auf P lässt sich schreiben als $\chi_P = a_1\psi_1 + \ldots + a_r\psi_r$ für geeignete $a_1, \ldots, a_r \in \mathbb{Z}$ und $\psi_1, \ldots, \psi_r \in \mathrm{Irr}(P)$. Seien $\psi_1, \ldots, \psi_m$ die nichtlinearen Charaktere in dieser Linearkombination und $\psi_{m+1}, \ldots, \psi_r$ die linearen. Für $j = 1, \ldots, m$ sei $k_j \in \{0, \ldots, p-1\}$ die Zahl, für die $\psi_j(z) = \psi_j(1) \cdot \zeta_p^{k_j}$ ist, und $d_j \in \mathbb{N}$ so, dass $\psi_j(1) = d_j \cdot p$ gilt. Dann ergibt sich

$$\begin{aligned}\chi(1) - \chi(z) &= \sum_{j=1}^{m} a_j(\psi_j(1) - \psi_j(z)) + \sum_{j=m+1}^{r} a_j(\psi_j(1) - \psi_j(z)) \\ &= \sum_{j=1}^{m} a_j \left(pd_j - pd_j\zeta_p^{k_j}\right) = \sum_{j=1}^{m} a_j d_j p \left(1 - \zeta_p^{k_j}\right) .\end{aligned}$$

Sei $\mathfrak{P}$ das maximale Ideal in $\mathbb{Z}[\zeta_p]$, das p enthält. Dann liegt jeder Summand der obigen Summe in $p\mathfrak{P}$. Folglich ist $\chi(1) - \chi(z)$ ein Element aus $p\mathfrak{p}$. Das Ideal $p\mathcal{O}_{\mathbb{Q}(\mathrm{cl}_G(z))}$ ist wegen $[\mathbb{Q}(\mathrm{cl}_G(z)) : \mathbb{Q}] > 1$ in $\mathfrak{p}^2$ enthalten. Damit folgt $\chi(1) \equiv \chi(z) \pmod{\mathfrak{p}^3}$. Für jede Funktion $\eta \in R(G)_p$ mit $\eta(z) \in \mathfrak{p}$ gilt daher ebenso $\eta(1) \equiv \eta(z) \pmod{\mathfrak{p}^3}$. Für einen Erzeuger π von $\mathfrak{p}$ liegen die Funktionen $\varphi_1, \varphi_2 \in R(G)'_p$ mit

$$\varphi_1(g) = \begin{cases} \pi, & g \sim z \\ 0, & \text{sonst} \end{cases} \qquad \varphi_2(g) = \begin{cases} \pi^2, & g \sim z \\ 0, & \text{sonst} \end{cases}$$

also in $\mathrm{rad}(R(G)'_p) \setminus R(G)_p$.

Seien $\alpha \in \mathrm{rad}(R(G)'_p)$ und $\eta_1, \eta_2, \xi_1, \xi_2 \in R(G)_p$ mit $\eta_1\alpha + \xi_1 = \varphi_1$ und $\eta_2\alpha + \xi_2 = \varphi_2$. Wegen $\alpha(z) \in \mathfrak{p}$ muss auch $\xi_1(z)$ in $\mathfrak{p}$ liegen. Dann ist $\xi_1(z)$ aber sogar schon in $\mathfrak{p}^3$, was $\alpha(z) \in \mathfrak{p} \setminus \mathfrak{p}^2$ impliziert.

Analog zu $\xi_1(z)$ muss auch $\xi_2(z)$ ein Element von $\mathfrak{p}$ sein. Damit gilt aber $\xi_2(z) \in \mathfrak{p}^3$, also muss $\eta_1\alpha(z) \in \mathfrak{p}^2$ gelten. Das würde jedoch $\eta_1(z) \in \mathfrak{p}$ bedeuten, was wegen $\eta_1 \in R(G)_p$ nicht möglich ist. Demzufolge ist der $R(G)_p$-Modul $\mathrm{rad}(R(G)'_p/R(G)_p)$ nicht zyklisch, im Widerspruch dazu, dass $R(G)$ endlichen Darstellungstyp hat. Die Elemente aus der $\mathbb{Q}$-Klasse von z können also nicht in verschiedenen Konjugationsklassen von G liegen. □

Im ersten Teil des obigen Beweises wird implizit auch gezeigt, dass es mindestens (und damit nach Folgerung 2.14 genau) drei $\mathbb{Q}$-Klassen von p-Elementen in G geben muss, wenn P nichtabelsch ist und $R(G)$ endlichen Darstellungstyp hat. Die Voraussetzung in Lemma 3.13, dass G drei $\mathbb{Q}$-Klassen hat, könnten wir also auch weglassen.

Bemerkung 3.14. Bevor wir nun zu unserer eigentlichen Aussage, dass die p-Sylowgruppen von G für eine ungerade Primzahl p abelsch sind, kommen, merken wir noch an, dass die Gruppe $\mathrm{SL}(2,5)$ auf einer zyklischen Gruppe nur trivial operieren kann. Das folgt daraus, dass die Automorphismengruppe einer zyklischen Gruppe auflösbar ist, während $\mathrm{SL}(2,5)$ bekanntlich nicht auflösbar und zudem perfekt ist.

Satz 3.15. *Seien $p \in \mathbb{P}$ ungerade und $P \in \mathrm{Syl}_p(G)$. Ist der Darstellungstyp von $R(G)$ endlich, so ist P abelsch.*

Beweis. Wir nehmen an, dass P nichtabelsch ist und $R(G)$ endlichen Darstellungstyp hat. Wie im Beweis von Lemma 3.13 können wir auch hier $p \nmid E(G)$ folgern. Ist $E(G) \neq 1$, so hat $G/E(G)$ also zu P isomorphe p-Sylowgruppen und nach Lemma 3.1 höchstens so viele $\mathbb{Q}$-Klassen von p-Elementen wie G. Außerdem ist für ein p-Element $x \in G$ die Konjugationsklasse $xE(G)$ in $G/E(G)$ rational, wenn die Konjugationsklasse von x in G rational ist.

Analoge Aussagen gelten für $G/O_{p'}(G)$. Wir nehmen daher im Folgenden $E(G) = 1$ und $O_{p'}(G) = 1$ an, d. h. $F^*(G) = O_p(G)$ und somit $C_G(O_p(G)) \leq O_p(G)$.

Wir betrachten zunächst den Fall $O_p(G) < P$. Wegen $C_G(O_p(G)) \leq O_p(G)$ folgt $Z(P) \leq O_p(G)$. Da $O_p(G)$ ein Normalteiler von G ist, kann kein Element aus $P \setminus O_p(G)$ zu einem aus $O_p(G)$ konjugiert sein. Somit darf es nur eine $\mathbb{Q}$-Klasse von Elementen in $P \setminus O_p(G)$ geben. Ebenso kann es auch nur eine $\mathbb{Q}$-Klasse nichttrivialer Elemente in $O_p(G)$ geben. Nach Lemma 3.13 sind außerdem alle nichttrivialen Elemente aus $Z(P)$ in G konjugiert, also permutiert G die Elemente aus $O_p(G) \setminus \{1\}$ transitiv. Zusammen mit Satz 1.49 folgt daraus, dass $O_p(G)$ elementar-abelsch sein muss und $O_P(G)$ isomorph zu einer der Gruppen aus der Liste von Satz 1.52 ist. Bevor wir die Gruppen dieser Liste im einzelnen betrachten, stellen wir noch drei etwas allgemeinere Überlegungen an.

(i) Sei $m \in \mathbb{N}$ so, dass $O_p(G) \cong C_p^m$ gilt. Die Anzahl der Elemente der Ordnung p in $G \setminus O_p(G)$ muss dann durch p^m teilbar sein. Angenommen, die p-Sylowgruppen von $G/O_p(G)$ wären zyklisch und $G \setminus O_p(G)$ enthielte ein Element der Ordnung p. Für ein Element $x \in P \cap (G \setminus O_p(G))$ ist $|C_G(x)|$ wegen $Z(P) \leq O_p(G)$ mindestens durch p^2 teilbar. Somit ist

$$|\mathrm{cl}_G(x)| = |G : C_G(x)| \not\equiv 0 \pmod{p^m}.$$

In der $\mathbb{Q}$-Klasse von x in G liegen genau $r \cdot |\mathrm{cl}_G(x)|$ Elemente für ein $r \in \{1, \ldots, p-1\}$. Folglich enthält die $\mathbb{Q}$-Klasse von x eine nicht durch p^m teilbare Anzahl an Elementen, womit die Elemente der Ordnung p aus $G \setminus O_p(G)$ in mindestens zwei verschiedene $\mathbb{Q}$-Klassen zerfallen. Damit lägen jedoch zu viele $\mathbb{Q}$-Klassen von Elementen der Ordnung p in G.

(ii) Wir nehmen als nächstes $O_p(G) \cong C_p^2$ an und betrachten den Fall, dass $G/O_p(G)$ elementar-abelsche p-Sylowgruppen vom Rang $\ell > 1$ hat. Seien $Q = P/O_p(G) \in \mathrm{Syl}_p(G/O_p(G))$ und $x_1, \ldots, x_\ell$ Erzeuger von Q. Wir bezeichnen die zyklischen Untergruppen der Ordnung p von $O_p(G)$ mit $Z_1, \ldots, Z_{p+1}$. Wegen $Z(P) \leq O_p(G)$ operiert Q auf einer dieser zyklischen Gruppen trivial, sei dies o. B. d. A. Z_{p+1}. Da $C_G(O_p(G)) \leq O_p(G)$ gilt, darf ferner kein Element aus Q trivial auf ganz $O_p(G)$ operieren. Jedes Element aus Q muss also $Z_1, \ldots, Z_p$ nichttrivial permutieren. Es gelte o. B. d. A. $x_1 Z_1 x_1^{-1} = Z_2$. Da auch x_2 die Gruppen $Z_1, \ldots, Z_p$ zyklisch permutiert, gibt es ein $j \in \{1, \ldots, p-1\}$,

sodass $x_2^j Z_2 x_2^{-j} = Z_1$ gilt. Dann zentralisiert jedoch das Element $x_2^j x_1$ nicht nur Z_{p+1}, sondern auch Z_1 und operiert somit auf ganz $O_p(G)$ trivial. Folglich kann auch dieser Fall nicht eintreten.

(iii) Sei jetzt wieder $O_p(G) \cong C_p^m$. Angenommen die Elemente der Ordnung p aus $O_p(G)$ haben jeweils Zentralisatoren ungerader Ordnung in G und ein Element der Ordnung p aus $G/O_p(G)$ kommutiert mit einer Involution aus $G/O_p(G)$. Dann gibt es ein Element $\bar{x}$ der Ordnung $2p$ in $G/O_p(G)$. Ein Urbild x von $\bar{x}$ in G hat demnach die Ordnung $2p$ oder $2p^2$. Hätte x die Ordnung $2p^2$, so hätten alle p-Elemente aus $G \setminus O_p(G)$ die Ordnung p^2. Das Element x^{2p} müsste daher in $O_p(G)$ liegen. Damit wäre aber $|C_G(x^{2p})|$ ungerade, was im Widerspruch dazu steht, dass die Ordnung von x gerade ist. Das impliziert, dass es in $G \setminus O_p(G)$ Elemente der Ordnung p gibt.

Wir gehen nun die Liste der Gruppen aus Satz 1.52 durch. Sei $O_p(G) \cong C_p^m$. Zuerst operiere $G/O_p(G)$ auf $O_p(G)$ wie eine Untergruppe von $\Gamma\mathrm{L}(p^m) \cong C_{p^m-1} \rtimes C_m$ auf $\mathbb{F}_p^m$, also $G/O_p(G) \cong C_r \rtimes C_s$ mit $r \mid p^m - 1$ und $s \mid m$. Da die Operation transitiv ist, muss $G/O_p(G)$ ein Element der Ordnung 2 enthalten. Weiter ist p ein Teiler von $|G/O_p(G)|$, d. h. $p \mid s$. Hat C_r gerade Ordnung, so enthält $Z(G/O_p(G))$ offenbar eine Involution. Ist andererseits die Ordnung von C_s gerade, so enthält bereits C_s Elemente der Ordnung 2 und p, die kommutieren. In beiden Fällen gibt es nach (iii) ein Element der Ordnung p in $G \setminus O_p(G)$. Des Weiteren sind die p-Sylowgruppen von $G/O_p(G)$ offenbar zyklisch, womit G nach (i) mindestens vier $\mathbb{Q}$-Klassen von Elementen der Ordnung p enthält.

Sei $k \geq 2$ und $G/O_p(G)$ enthalte einen zu $\mathrm{SL}(k, q)$ isomorphen Normalteiler. Nach Satz 3.6 muss $k = 2$ und $q \in \mathbb{P}$, also $m = 2$ gelten. Aufgrund von (ii) besitzt $G/O_p(G)$ daher zyklische p-Sylowgruppen. Weil $G/O_p(G)$ eine zu $\mathrm{SL}(2, p)$ isomorphe Untergruppe enthält, haben die Elemente der Ordnung p aus $G/O_p(G)$ Zentralisatoren gerader Ordnung. Aus (iii) folgt nun, dass es in G Elemente der Ordnung p gibt, und wegen (i) muss es in G mindestens vier $\mathbb{Q}$-Klassen von p-Elementen geben.

Der Fall, dass $G/O_p(G)$ einen zu $\mathrm{Sp}(k, q)$ isomorphen Normalteiler hat ($p^m = q^k$, $k \in 2\mathbb{N}$) führt ebenso auf $m = 2$ und kann dementsprechend ebenfalls nicht eintreten.

Gilt $p = 3$ und $O_3(G) \cong C_3^2$ und besitzt $G/O_3(G)$ einen zu Q_8 isomorphen Normalteiler, so enthält $Z(G/O_3(G))$ ein Element der Ordnung 2. Nach (iii) und (i) können die 3-Sylowgruppen von $G/O_3(G)$ nicht zyklisch sein. Wegen (ii) können sie aber auch nicht elementar-abelsch vom Rang > 1 sein, was auch diesen Fall ausschließt.

Seien $p \in \{5, 7, 11, 23\}$, $O_p(G) \cong C_{p^2}$ und $G/O_p(G)$ enthalte einen zu $\mathrm{SL}(2, 3)$ isomorphen Normalteiler H. Dann folgt aus (ii), dass $G/O_p(G)$ zyklische p-Sylowgruppen haben muss. Die Involution aus H liegt offenbar in $Z(G/O_p(G))$. Nach (iii) und (i) gäbe es somit mindestens vier $\mathbb{Q}$-Klassen von p-Elementen in G.

Ähnlich kann man auch im Fall, dass $p \in \{11, 19, 29, 59\}$ und $O_p(G) \cong C_{p^2}$ ist sowie $G/O_p(G)$ einen zu $\mathrm{SL}(2, 5)$ isomorphen Normalteiler besitzt, argumentieren. Aus (ii) folgt wieder, dass $G/O_p(G)$ zyklische p-Sylowgruppen haben muss, und

weil ein Element der Ordnung p nur trivial auf $\mathrm{SL}(2,5)$ operieren kann, gibt es in $G/O_p(G)$ Elemente der Ordnung $2p$. Nach (iii) und (i) kann daher auch dieser Fall nicht auftreten.

Sei $p = 3$ und $O_3(G) \cong C_3^4$. Nach Satz 3.12 kann $G/O_3(G)$ keine extraspezielle 2-Sylowgruppe der Ordnung 32 als Normalteiler haben. Also besitzt $G/O_3(G)$ einen zu $\mathrm{SL}(2,5)$ isomorphen Normalteiler H. Die Operation von H auf $O_3(G) \setminus \{1\}$ ist aber nicht transitiv; $O_3(G) \setminus \{1\}$ zerfällt unter dieser Operation in zwei Bahnen. Damit $G/O_3(G)$ transitiv auf $O_3(G)\setminus\{1\}$ operieren kann, muss $(G/O_3(G))/H$ gerade Ordnung haben. Damit lägen aber zu viele $\mathbb{Q}$-Klassen von 2-Elementen in $G/O_3(G)$ und folglich auch in G.

Schließlich folgt auch im Fall $p = 3$, $O_3(G) \cong C_3^6$ und $G/O_p(G) \cong \mathrm{SL}(2,13)$ nach (iii) und (i), dass es in G zu viele $\mathbb{Q}$-Klassen von 3-Elementen gibt, als dass $R(G)$ endlichen Darstellungstyp haben könnte.

Wir dürfen also $P \trianglelefteq G$ annehmen. Mit Lemma 3.13 folgt, dass alle nichttrivialen Elemente aus $Z(P)$ konjugiert sind und alle Elemente aus $P \setminus Z(P)$ eine $\mathbb{Q}$-Klasse bilden. Nach Satz 1.49 sind daher sowohl $Z(P)$ als auch $P/Z(P)$ elementar-abelsch und außerdem gilt $\exp(P) = p$. Weil alle nichttrivialen Elemente von $Z(P)$ in G konjugiert sind, gibt es keine Untergruppe $1 < H < Z(P)$, die ein Normalteiler von G ist, d. h. $Z(P) \leq P'$. Andererseits ist $P/Z(P)$ abelsch, also $\Phi(P) \leq Z(P)$ und wegen $\exp(P) = p$ gilt sogar $P' = \Phi(P) = Z(P)$, d. h., P ist speziell.

Sei also $Z(P) \cong C_p^k$ und $P/Z(P) \cong C_p^\ell$. Da alle Elemente aus $P \setminus Z(P)$ in einer $\mathbb{Q}$-Klasse von G liegen, haben die Zentralisatoren dieser Elemente alle dieselbe Ordnung. Damit gilt auch $|C_P(x)| = |C_P(y)|$ für $x, y \in P \setminus Z(P)$. Wir wählen j so, dass $|C_P(x)| = p^j$ ist. Die Länge der P-Konjugationsklassen der Elemente aus $P \setminus Z(P)$ ist also $p^{k+\ell-j}$. Wegen

$$p^{k+\ell} = 1 \cdot p^k + p^{k+\ell-j}\left(p^{j-k} - p^{j-\ell}\right)$$

gibt es in P genau $p^{j-k} - p^{j-\ell} = p^{j-\ell}(p^{\ell-k} - 1)$ Konjugationsklassen von Elementen aus $P \setminus Z(P)$. Die Anzahl der P-Konjugationsklassen, und damit auch die Anzahl der $\mathbb{Q}$-Klassen in P, ist also genau dann nicht durch p teilbar, wenn $j = \ell$ gilt. Dass die Anzahl der $\mathbb{Q}$-Klassen in P von Elementen aus $P \setminus Z(P)$ nicht durch p teilbar ist, ist aber eine notwendige Bedingung: G permutiert diese Klassen transitiv. Ist M die Menge dieser Klassen, so gibt es also für $\mathcal{C} \in M$ eine Bijektion zwischen M und $G/\mathrm{Stab}_G(\mathcal{C})$. Da natürlich P in $\mathrm{Stab}_G(\mathcal{C})$ liegt, kann $|G : \mathrm{Stab}_G(\mathcal{C})|$ und somit auch $|M|$ nicht durch p teilbar sein. Folglich gilt $|C_P(x)| = p^\ell$ für $x \in P \setminus Z(P)$. Dies liefert

$$|\{[x,y] : y \in P\}| = \frac{p^{k+\ell}}{|C_P(x)|} = \frac{p^{k+\ell}}{p^\ell} = p^k = |Z(P)|\,.$$

Da $P' = Z(P)$ gilt, existiert also zu jedem $z \in Z(P)$ ein $y \in P$ mit $z = [x,y]$.

Sei H eine maximale Untergruppe von $Z(P)$. Dann ist sicher $\exp(P/H) = p$. Für $z \in Z(P) \setminus H$ gibt es, wie eben gezeigt, $x, y \in P$, sodass $z = [x,y]$. Folglich liegt die Nebenklasse zH in $(P/H)'$, weswegen $(P/H)' = Z(P)/H$ zyklisch ist. Genauso gibt

es zu jedem $x \in P$ ein $y \in P$, sodass $[x, y]$ in $Z(P) \setminus H$ liegt. Die Nebenklasse xH kann daher nicht in $Z(P/H)$ enthalten sein. Somit muss auch $Z(P/H) = Z(P)/H$ gelten, d. h. $Z(P/H) = (P/H)' \cong C_p$. Die Faktorgruppe P/H ist daher extraspeziell. Satz 1.45 liefert jetzt sofort, dass ℓ gerade ist.

Nun ist $P/Z(P)$ also eine elementar-abelsche Gruppe von geradem Rang, deren zyklische Untergruppen durch $G/Z(P)$ transitiv permutiert werden. Nach Satz 1.52 operiert $G/C_G(P)$ auf $P/Z(P)$ wie eine Untergruppe von $\Gamma\mathrm{L}(p^\ell)$ auf $\mathbb{F}_p^\ell$ oder wie eine der Ausnahmegruppen, falls $|P/Z(P)| = 3^4$ oder $p \in \{3, 5, 7, 11, 19, 23, 29, 59\}$ und P eine extraspezielle Gruppe der Ordnung p^3 vom Exponenten p ist, denn in allen anderen möglichen Fällen gäbe es in G zu viele Klassen von Elementen der Ordnung p.

Wir nehmen zunächst an, dass $G/C_G(P)$ auf $P/Z(P)$ wie eine Untergruppe von $\Gamma\mathrm{L}(p^\ell)$ auf $\mathbb{F}_p^\ell$ operiert. Nach Lemma 3.8 hat $G/C_G(P)$ einen durch

$$\frac{p^\ell - 1}{p - 1} \cdot \prod_{\substack{p_i \in \mathbb{P} \\ p_i \mid d}} p_i^{r_i}$$

teilbaren Exponenten, wobei $d := \mathrm{ggT}\big(\frac{p^n-1}{p-1}\,,\, p-1\big)$ und $r_i \in \mathbb{Z}$ jeweils die größte Zahl ist, sodass $p - 1$ von $p_i^{r_i}$ geteilt wird. Nun ist aber ℓ gerade und somit $\frac{p^\ell-1}{p-1}$ ebenfalls gerade sowie $p^\ell - 1$ durch 8 teilbar. Folglich besitzt $G/C_G(P)$ ein Element der Ordnung 8 und der Darstellungstyp von $R(G)$ ist unendlich.

Damit muss $|P/Z(P)| = 3^4$ oder P eine extraspezielle Gruppe der Ordnung p^3 vom Exponenten p sein, wobei $p \in \{5, 7, 11, 19, 23, 29, 59\}$ ist.

- Ist $|P/Z(P)| = 3^2$, so hat $G/C_G(P)$ einen zu Q_8 isomorphen Normalteiler. Damit die Elemente der Ordnung 4 von G allesamt konjugiert sind, müsste es in $G \setminus P$ Elemente der Ordnung 3 geben, was jedoch unmöglich ist.
- Angenommen $|P/Z(P)| = 3^4$. Da $|G/C_G(P)|$ teilerfremd zu 3 sein muss, hat $G/C_G(P)$ einen Normalteiler, der zu einer extraspeziellen Gruppe der Ordnung 32 isomorph ist. Damit hat $R(G)$ nach Satz 3.12 unendlichen Darstellungstyp.
- Ist $p \in \{7, 23\}$, so muss $G/C_G(P)$ ein Element der Ordnung 8 beinhalten, damit alle zyklischen Untergruppen in $P/Z(P)$ konjugiert sind. Dann hätte $R(G)$ jedoch unendlichen Darstellungstyp.
- Sei $p = 5$, dann muss $G/C_G(P)$ einen zu $H \cong \mathrm{SL}(2, 3)$ isomorphen Normalteiler enthalten. Außer auf den zyklischen Untergruppen von $P/Z(P)$ muss $G/C_G(P)$ wegen Lemma 3.13 auch noch transitiv auf den nichttrivialen Elementen von $Z(P)$ operieren. Auf einer zyklischen Gruppe der Ordnung 5 kann $\mathrm{SL}(2, 3)$ jedoch nur trivial operieren, da die Elemente der Ordnung 3 trivial operieren und sich jedes Element der Ordnung 4 als Produkt zweier Elemente der Ordnung 3 schreiben lässt. Also müsste $|(G/C_G(P))/H|$ gerade sein, womit es in G zu viele $\mathbb{Q}$-Klassen von 2-Elementen gäbe.

- Für $p = 11$ enthält $G/C_G(P)$ einen zu $\mathrm{SL}(2,3)$ oder $\mathrm{SL}(2,5)$ isomorphen Normalteiler H. Nun kann weder $\mathrm{SL}(2,5)$ (wegen Bemerkung 3.14) noch $\mathrm{SL}(2,3)$ nichttrivial auf C_{11} operieren: Die Elemente der Ordnung 3 aus $\mathrm{SL}(2,3)$ müssen trivial auf C_{11} operieren und jedes Element der Ordnung 4 aus $\mathrm{SL}(2,3)$ lässt sich als Produkt zweier Elemente der Ordnung 3 schreiben. Sind nicht alle Elemente der Ordnung 11 aus $Z(P)$ in G konjugiert, hätte $R(G)$ wieder nach Lemma 3.13 unendlichen Darstellungstyp. Also müsste $|(G/C_G(P))/H|$ gerade sein, womit zu viele Klassen von Involutionen in G lägen.

- Damit für $p = 19$ alle Elemente aus $Z(P)$ in G konjugiert sein können, müsste G, und somit auch $G/C_G(P)$, ein Element der Ordnung 9 enthalten. Weiter besitzt $G/C_G(P)$ einen zu $\mathrm{SL}(2,5)$ isomorphen Normalteiler H.
  Sei $x \in G/C_G(P)$ ein Element der Ordnung 9. Angenommen x^3 läge in H. Dann würde x^3 keine 2-Sylowgruppe von H zentralisieren. Da die 2-Sylowgruppen von H zu Q_8 isomorph sind, dürfte x daher in keinem Normalisator einer 2-Sylowgruppe von H enthalten sein. Das widerspricht aber der Tatsache, dass es in H genau fünf 2-Sylowgruppen gibt. Also liegt x^3 nicht in H, was bedeutet, dass $G/C_G(P)$, und somit auch G, mindestens zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung 3 und mindestens eine $\mathbb{Q}$-Klasse von Elementen der Ordnung 9 enthielte. Folglich hätte $R(G)$ unendlichen Darstellungstyp.

- Im Fall $p = 29$ hat $G/C_G(P)$ einen zu $\mathrm{SL}(2,5)$ isomorphen Normalteiler. Eine zu $\mathrm{SL}(2,5)$ isomorphe Gruppe kann aber nach Bemerkung 3.14 auch auf einer zyklischen Gruppe der Ordnung 29 nur trivial operieren, also wären erneut nicht alle Elemente aus $Z(P)\setminus\{1\}$ konjugiert oder G enthielte zu viele Klassen von Involutionen.

- Schließlich besitzt $G/C_G(P)$ für $p = 59$ einen zu $\mathrm{SL}(2,5)$ isomorphen Normalteiler. Auch auf einer zyklischen Gruppe der Ordnung 59 kann $\mathrm{SL}(2,5)$ nach Bemerkung 3.14 nur trivial operieren, d. h., auch dieser Fall kann nicht eintreten.

Die Liste schließt somit aus, dass $G/C_G(P)$ wie eine der sporadischen Gruppen auf $P/Z(P)$ operiert. Daher müssen für eine ungerade Primzahl p die p-Sylowgruppen einer endlichen Gruppe, deren Charakterring endlichen Darstellungstyp hat, abelsch sein. □

Mit den Sätzen 3.2 und 3.15 folgt sofort, dass für eine ungerade Primzahl p die p-Sylowgruppen von G zyklisch der Ordnung $\leq p^2$ oder elementar-abelsch sind, wenn $R(G)$ endlichen Darstellungstyp hat.

4 Struktur von Gruppen, deren Charakterring endlichen Typ hat

Im vorigen Kapitel haben wir untersucht, welche Gestalt die Sylowgruppen von G haben müssen, damit $R(G)$ endlichen Darstellungstyp haben kann. Jetzt wollen wir auch hinreichende Bedingungen dafür, dass $R(G)$ endlichen Darstellungstyp hat, finden. Eine Reduktion diesbezüglich liefert die folgende Proposition.

Proposition 4.1. *Seien G_1 und G_2 endliche Gruppen mit $\mathrm{ggT}(|G_1|, |G_2|) = 1$. Der Darstellungstyp von $R(G_1 \times G_2)$ ist genau dann endlich, wenn $R(G_1)$ und $R(G_2)$ endlichen Darstellungstyp haben.*

Beweis. Offenbar ist der Darstellungstyp von $R(G_1 \times G_2)$ unendlich, wenn bereits $R(G_1)$ oder $R(G_2)$ unendlichen Darstellungstyp hat. Wir nehmen daher im Folgenden an, dass $R(G_1)$ und $R(G_2)$ endlichen Darstellungstyp haben mögen.

Seien $x_1 \in G_1$ und $x_2 \in G_2$. Sind $A_1, \ldots, A_m$ und $B_1, \ldots, B_n$ die Konjugationsklassen von G_1 und G_2, so sind bekanntlich A_iB_j für $i = 1, \ldots, m$ und $j = 1, \ldots, n$ die Konjugationsklassen von $G_1 \times G_2$. Für einen Primteiler p_1 von $|G_1|$ enthält die rationale p_1'-Sektion von x_1 in $G_1 \times G_2$ daher genauso viele $\mathbb{Q}$-Klassen wie die rationale p_1'-Sektion von x_1 in G_1. Ist p_2 ein Primteiler von $|G_2|$, so liegen in der rationalen p_2'-Sektion von x_1 in $G_1 \times G_2$ genauso viele $\mathbb{Q}$-Klassen wie in der rationalen p_2'-Sektion von 1_{G_2} in G_2. Analoge Aussagen gelten für x_2.

Seien $\mathcal{C}$ die $\mathbb{Q}$-Klasse von x_1x_2 in $G_1 \times G_2$, $\mathcal{C}_1$ diejenige von x_1 in G_1 und $\mathcal{C}_2$ die $\mathbb{Q}$-Klasse von x_2 in G_2. Nach Proposition 1.22 sind die irreduziblen Charaktere von $G_1 \times G_2$ genau die Charaktere der Form $\psi \times \varphi$ mit $\psi \in \mathrm{Irr}(G_1)$ und $\varphi \in \mathrm{Irr}(G_2)$. Jede Klassenfunktion von $G_1 \times G_2$ lässt sich also in Form solch eines Produkts einer Klassenfunktion von G_1 mit einer von G_2 schreiben.

Offenbar gilt $\mathbb{Q}(\mathcal{C}_1) \subseteq \mathbb{Q}(\zeta_{|G_1|})$ sowie $\mathbb{Q}(\mathcal{C}_2) \subseteq \mathbb{Q}(\zeta_{|G_2|})$. Proposition 1.14 und Lemma 1.12 implizieren deshalb

$$\mathcal{O}_{\mathbb{Q}(\mathcal{C})} = \mathcal{O}_{\mathbb{Q}(\mathcal{C}_1)}\mathcal{O}_{\mathbb{Q}(\mathcal{C}_2)}\,. \tag{4.1}$$

Sei $p \in \mathbb{P}$ mit $p \mid |G_1|$, $\mathcal{S}_1$ die rationale p'-Sektion von x_1 in G_1 und $\mathcal{S}$ die rationale p'-Sektion von x_1x_2 in $G_1 \times G_2$. Da $|G_1|$ und $|G_2|$ teilerfremd sind, liegt die Klassenfunktion ν_{x_2} von G_2 mit $\nu_{x_2}(x_2) = 1$ und $\nu_{x_2}(g) = 0$ für $g \in G_2 \setminus \mathcal{C}_2$ nach Lemma 2.11 in $R(G_2)_p$. Ist α_1 (bzw. sind α_1, α_2) Erzeuger des $R(G_1)_p$-Moduls $(R(G_1)'_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}_1))/(R(G_1)_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}_1))$, so erzeugt $\alpha_1 \times \nu_{x_2}$ (bzw. erzeugen $\alpha_1 \times \nu_{x_2}$ und $\alpha_2 \times \nu_{x_2}$) daher und wegen (4.1) den $R(G_1 \times G_2)_p$-Modul

$$(R(G_1 \times G_2)'_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}))/(R(G_1 \times G_2)_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}))\,.$$

Dieselbe Argumentation zeigt, dass der $R(G_1 \times G_2)_p$-Modul

$$\mathrm{rad}((R(G_1 \times G_2)'_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}))/(R(G_1 \times G_2)_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S})))$$

zyklisch ist, wenn der $R(G_1)_p$-Modul

$$\mathrm{rad}((R(G_1)'_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}_1))/(R(G_1)_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}_1)))$$

zyklisch ist. Da $R(G_1)_p$ nach Voraussetzung endlichen Darstellungstyp hat, folgt mit Bemerkung 2.12, dass der Darstellungstyp von $R(G_1 \times G_2)_p$ ebenfalls endlich ist.

Analog hat $R(G_1 \times G_2)_\ell$ für jeden Primteiler ℓ von $|G_2|$ endlichen Darstellungstyp und damit folgt schließlich, dass auch der Darstellungstyp von $R(G_1 \times G_2)$ endlich ist. □

Werden für endliche Gruppen G_1 und G_2 sowohl $|G_1|$ als auch $|G_2|$ von einer Primzahl $p \in \mathbb{P}$ geteilt, so gibt es in $G_1 \times G_2$ mindestens drei $\mathbb{Q}$-Klassen von Elementen der Ordnung p. Der Darstellungstyp von $R(G_1 \times G_2)_p$ und damit auch der von $R(G_1 \times G_2)$ ist in diesem Fall also unendlich.

Aus Kapitel 3 wissen wir, dass die p-Sylowgruppen von G für eine ungerade Primzahl p zyklisch der Ordnung höchstens p^2 oder elementar-abelsch sein müssen, damit $R(G)$ endlichen Darstellungstyp haben kann. Wir betrachten diese beiden Fälle jetzt getrennt.

4.1 Zyklische Sylowgruppen

Der Darstellungstyp des Gruppenrings einer zyklischen Gruppe G der Ordnung p bzw. p^2 für eine beliebige Primzahl p ist endlich. Da Gruppenring und Charakterring einer abelschen Gruppe isomorph sind, hat also auch $R(G)$ endlichen Darstellungstyp. Das legt die Vermutung nahe, dass $R(H)_p$ endlichen Darstellungstyp haben sollte, wenn H eine endliche Gruppe mit zyklischer p-Sylowgruppe der Ordnung $\leq p^2$ ist. Dass dies tatsächlich so ist, wollen wir in diesem Abschnitt beweisen.

Wir beginnen mit der möglichen Anzahl der $\mathbb{Q}$-Klassen in den einzelnen rationalen p'-Sektionen einer endlichen Gruppe mit zyklischer p-Sylowgruppe. Im Folgenden stehe dabei p stets für eine Primzahl.

Lemma 4.2. *Sei $P \in \mathrm{Syl}_p(G)$ zyklisch der Ordnung p^a für ein $a \in \mathbb{N}$. Dann besitzt jede rationale p'-Sektion von G höchstens $a+1$ verschiedene $\mathbb{Q}$-Klassen.*

Beweis. Weil P zyklisch ist, sind nach dem Satz von Sylow je zwei p-Elemente derselben Ordnung $\mathbb{Q}$-konjugiert in G. Damit genügt es zu zeigen, dass je zwei Elemente, deren p- und p'-Anteile jeweils $\mathbb{Q}$-konjugiert sind, in derselben $\mathbb{Q}$-Klasse von G liegen.

Sei $x \in P$. Wir betrachten die $\mathbb{Q}$-Klassen einer rationalen p'-Sektion in $N_G(\langle x\rangle)$, deren Elemente p-Anteile haben, die $\mathbb{Q}$-konjugiert zu x sind. Wie eben bemerkt ist dies äquivalent dazu, dass die p-Anteile dieselbe Ordnung wie x haben. Seien x_1y_1 und x_2y_2 Elemente aus solchen $\mathbb{Q}$-Klassen, d. h. $x_iy_i = y_ix_i$ für $i = 1, 2$, und y_1 und y_2 sind $\mathbb{Q}$-konjugiert in $N_G(\langle x\rangle)$. Dann gibt es ein $g \in N_G(\langle x\rangle)$ und ein $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{\exp(N_G(\langle x\rangle))})/\mathbb{Q})$ mit zu p teilerfremder Ordnung, sodass $\sigma(gy_1g^{-1}) = y_2$ ist. Damit folgt $\sigma(gx_1y_1g^{-1}) = x^by_2$ für ein $b \in \mathbb{Z}$ mit $\mathrm{ggT}(b, p) = 1$, denn jedes Element aus $N_G(\langle x\rangle)$ mit Ordnung $|\langle x\rangle|$ liegt bereits in $\langle x\rangle$. Weiter existiert ein $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_{\exp(N_G(\langle x\rangle))})/\mathbb{Q})$ mit $\tau(x^by_2) = x_2y_2$, da die Ordnungen von x und y_2 teilerfremd sind. Folglich liegen x_1y_1 und x_2y_2 in derselben $\mathbb{Q}$-Klasse von $N_G(\langle x\rangle)$ und damit besitzt jede rationale p'-Sektion von $N_G(\langle x\rangle)$ höchstens eine $\mathbb{Q}$-Klasse, die Elemente, deren p-Anteile dieselbe Ordnung wie x haben, enthält.

Jedes Element aus G, das mit x kommutiert, liegt bereits in $N_G(\langle x\rangle)$. In G gibt es daher keine $\mathbb{Q}$-Klasse, die ein Element mit p-Anteil x beinhaltet, aber keine $\mathbb{Q}$-Klasse aus $N_G(\langle x\rangle)$ enthält. Andererseits besitzt nach dem Satz von Sylow jedes Element aus G ein Konjugiertes, dessen p-Anteil in P liegt. Da alle Elemente der Ordnung $|\langle x\rangle|$ aus P bereits in $\langle x\rangle$ liegen, hat folglich jede $\mathbb{Q}$-Klasse, deren Elemente einen p-Anteil mit derselben Ordnung wie x haben, einen Repräsentanten, der in $N_G(\langle x\rangle)$ liegt. Dort besitzt nach obiger Argumentation jede rationale p'-Sektion höchstens eine $\mathbb{Q}$-Klasse mit Elementen, deren p-Anteile die Ordnung $|\langle x\rangle|$ haben, also gilt dies erst recht für G. Damit liegen zwei Elemente, deren p- und p'-Anteile jeweils $\mathbb{Q}$-konjugiert sind, tatsächlich in einer $\mathbb{Q}$-Klasse. □

Hat G eine zyklische p-Sylowgruppe der Ordnung $\leq p^2$, so bringt uns Lemma 4.2 schon ein ganzes Stück weiter. Dank dieses Lemmas müssen wir nämlich nur auf die Werte der irreduziblen Charaktere von G schauen, um zu entscheiden, ob $R(G)_p$ endlichen Darstellungstyp hat.

Lemma 4.3. *Seien $P \in \mathrm{Syl}_p(G)$ zyklisch und $g \in G$ so, dass $\langle g\rangle$ ein Normalteiler von G ist. Dann existiert zu einem in G invarianten Charakter $\vartheta \in \mathrm{Irr}(\langle g\rangle)$ ein $\chi \in \mathrm{Irr}(G)$ mit $\chi_{\langle g\rangle} = e\vartheta$, sodass e nicht von p geteilt wird.*

Beweis. Sei $Q \leq G$ so gewählt, dass $Q/\langle g\rangle \in \mathrm{Syl}_p(G/\langle g\rangle)$ gilt. Dann ist $Q/\langle g\rangle$ zyklisch und nach Proposition 1.26 gibt es daher ein $\tilde{\vartheta} \in \mathrm{Irr}(Q)$ mit $\tilde{\vartheta}_{\langle g\rangle} = \vartheta$. Für dessen nach G induzierten Charakter erhält man $\tilde{\vartheta}^G(1) = |G : Q|$, eine zu p teilerfremde Zahl. Daher besitzt $\tilde{\vartheta}^G$ eine irreduzible Konstituente $\chi \in \mathrm{Irr}(G)$ mit $p \nmid \chi(1)$. Gemäß der Frobenius-Reziprozität gilt $\langle \chi_Q, \tilde{\vartheta}\rangle = \langle \chi, \tilde{\vartheta^G}\rangle \neq 0$ und daher auch $\langle \chi_{\langle g\rangle}, \vartheta\rangle \neq 0$. Nun ist ϑ invariant in G, d. h. $\chi_{\langle g\rangle} = e\vartheta$ mit $e = \chi(1)$. □

Lemma 4.4. *Seien $\mathcal{C}$ eine $\mathbb{Q}$-Klasse, $g \in \mathcal{C}$ und $\chi_1, \ldots, \chi_n$ die irreduziblen Charaktere von G. Dann liegt jedes Element aus $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C})}$ bereits in $\mathbb{Z}_{(p)}[\chi_1(g), \ldots, \chi_n(g)]$.*

Beweis. Seien $\chi \in \mathrm{Irr}(N_G(\langle g\rangle))$ und $\psi \in \mathrm{Irr}(\langle g\rangle)$ eine Konstituente von $\chi_{\langle g\rangle}$. Nach Satz 1.21 gilt dann $\chi_{\langle g\rangle} = e_\chi \sum_{i=1}^{t} \psi_i$, wobei $\psi = \psi_1, \ldots, \psi_t$ die verschiedenen

Konjugierten von ψ in $N_G(\langle g\rangle)$ sind. Die Trägheitsgruppe von ψ in $N_G(\langle g\rangle)$ werde mit $I_{N_G(\langle g\rangle)}(\psi)$ bezeichnet. Nach Lemma 4.3 existiert ein $\tilde{\psi} \in \mathrm{Irr}(I_{N_G(\langle g\rangle)}(\psi))$ mit $\tilde{\psi}_{\langle g\rangle} = e_\psi\psi$ und $p \nmid e_\psi$. Durch erneute Anwendung von Lemma 1.21 erhalten wir damit $(\tilde{\psi}^{N_G(\langle g\rangle)})_{\langle g\rangle} = e_\psi \sum_{i=1}^t \psi_i$. Wegen $p \nmid e_\psi$ gibt es also eine Funktion in $R(N_G(\langle g\rangle))_p$, die eingeschränkt auf $\langle g\rangle$ gerade $\sum_{i=1}^t \psi_i$ ist.

Dies zeigt Folgendes: Sind $M_1, \ldots, M_k$ die Äquivalenzklassen irreduzibler Charaktere von $\langle g\rangle$ bezüglich $N_G(\langle g\rangle)$-Konjugation und gilt $S_j := \sum_{\varphi\in M_j} \varphi$ für $j = 1\ldots, k$, dann ist die Einschränkung eines Charakters von $N_G(\langle g\rangle)$ auf $\langle g\rangle$ eine $\mathbb{Z}$-Linearkombination der S_j und jedes S_j liegt in $R(N_G(\langle g\rangle))_p$. Insbesondere erhalten wir $\mathbb{Q}(\mathrm{cl}_{N_G(\langle g\rangle)}(g)) = \mathbb{Q}(S_1(g), \ldots, S_k(g))$. Dabei ist jede $|\langle g\rangle|$-te Einheitswurzel in genau einem der S_j als Summand enthalten und dort auch nur genau einmal.

Sei $j \in \{1, \ldots, k\}$. Nach Konstruktion gilt $S_j(ngn^{-1}) = S_j(g)$ für jedes $n \in N_G(\langle g\rangle)$. Außerdem liegt hgh^{-1} selbstverständlich nicht in $N_G(\langle g\rangle)$, wenn $h \in G \setminus N_G(\langle g\rangle)$ ist. Für die induzierte Funktion S_j^G erhalten wir daher

$$S_j^G(g) = \frac{1}{|N_G(\langle g\rangle)|} \sum_{h\in G} S_j(hgh^{-1})^\circ = \frac{1}{|N_G(\langle g\rangle)|} \cdot |N_G(\langle g\rangle)| S_j(g) = S_j(g)\,.$$

Da S_j^G in $R(G)_p$ liegt, folgt also $\mathbb{Z}_{(p)}[S_1(g), \ldots, S_k(g)] \subseteq \mathbb{Z}_{(p)}[\chi_1(g), \ldots, \chi_n(g)]$.

Andererseits ist für jedes $i \in \{1, \ldots, n\}$ die Einschränkung von χ_i auf $N_G(\langle g\rangle)$ eine $\mathbb{Z}$-Linearkombination irreduzibler Charaktere von $N_G(\langle g\rangle)$. Daher gilt auch $\mathbb{Z}_{(p)}[\chi_1(g), \ldots, \chi_n(g)] \subseteq \mathbb{Z}_{(p)}[S_1(g), \ldots, S_k(g)]$ und insgesamt folgt

$$\mathbb{Z}_{(p)}[S_1(g), \ldots, S_k(g)] = \mathbb{Z}_{(p)}[\chi_1(g), \ldots, \chi_n(g)]\,.$$

Das impliziert außerdem $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C})} = \mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(S_1(g),\ldots,S_k(g))}$. Weiter stimmen $\mathcal{O}_{\mathbb{Q}(S_1(g),\ldots,S_k(g))}$ und $\mathbb{Z}[S_1(g), \ldots, S_k(g)]$ wegen $\mathcal{O}_{\mathbb{Q}(\zeta_{|\langle g\rangle|})} = \mathbb{Z}[\zeta_{|\langle g\rangle|}]$ überein. Das impliziert $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C})} = \mathbb{Z}_{(p)}[S_1(g), \ldots, S_k(g)]$ und insgesamt ergibt sich schließlich $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C})} = \mathbb{Z}_{(p)}[\chi_1(g), \ldots, \chi_n(g)]$. □

An dieser Stelle wollen wir noch einmal an die in Lemma 2.11 und Definition 2.15 definierten Funktionen ν_x und μ_i erinnern. Für ein p'-Element $x \in G$ sei ν_x die Funktion aus $R(G)_p$, die auf der rationalen p'-Sektion von x den Wert 1 hat und sonst überall 0 ist. Weiter bezeichne μ_i die Funktion aus $R(G)'_p$, die auf allen Elementen von G, deren p-Anteile die Ordnung p haben, den Wert 1 annimmt und sonst 0 ist. Diese Funktionen werden wir im Folgenden verwenden, um unsere Betrachtungen lediglich auf die einzelnen $\mathbb{Q}$-Klassen von G einschränken zu können.

Satz 4.5. *Sei $P \in \mathrm{Syl}_p(G)$ zyklisch der Ordnung $\leq p^2$. Dann wird der $R(G)_p$-Modul $R(G)'_p/R(G)_p$ von μ_0 und μ_1 erzeugt.*

Beweis. Aus Bemerkung 2.12 wissen wir, dass es ausreicht zu zeigen, dass der $R(G)_p$-Modul $(R(G)'_p \cap \mathrm{Ch}_\mathbb{Q}(\mathcal{S}))/(R(G)_p \cap \mathrm{Ch}_\mathbb{Q}(\mathcal{S}))$ für jede rationale p'-Sektion $\mathcal{S}$ von den Einschränkungen der Funktionen μ_0 und μ_1 auf $\mathcal{S}$ erzeugt wird.

Sei also $\mathcal{S}$ eine beliebige rationale p'-Sektion aus G und y ein p'-Element aus $\mathcal{S}$. Nach Lemma 4.2 liegen in $\mathcal{S}$ höchstens drei $\mathbb{Q}$-Klassen. Aus dem Beweis dieses Lemmas folgt ferner, dass sich zwei Elemente derselben Ordnung aus $\mathcal{S}$ bereits in derselben $\mathbb{Q}$-Klasse befinden. Daher gibt es ein p-Element $x \in G$, sodass y, $x^p y$ und xy Repräsentanten der $\mathbb{Q}$-Klassen in $\mathcal{S}$ sind. Es ist hierbei durchaus möglich, dass $x^p y = y$ oder sogar $xy = y$ gilt, dann liegen entsprechend weniger $\mathbb{Q}$-Klassen in $\mathcal{S}$.

Unser Ziel ist es also, zu zeigen, dass die Funktionen $\mu_0\nu_y$ und $\mu_1\nu_y$ den $R(G)_p$-Modul $(R(G)'_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}))/(R(G)_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}))$ erzeugen. Da $\mu_0 + \mu_1 + \mu_2$ dem trivialen Charakter von G entspricht und ν_y nach Lemma 2.11 in $R(G)_p$ liegt, ist auch $\mu_2\nu_y = \nu_y - \mu_0\nu_y - \mu_1\nu_y$ im Erzeugnis von $\mu_0\nu_y$ und $\mu_1\nu_y$ enthalten. Für jede $\mathbb{Q}$-Klasse $\mathcal{C}$ von $\mathcal{S}$ liegt also die Funktion, die auf den Elementen von $\mathcal{C}$ gleich 1 ist und auf den anderen Elementen aus $\mathcal{S}$ den Wert 0 hat, im Erzeugnis von $\mu_0\nu_y$ und $\mu_1\nu_y$. Dieses Erzeugnis beinhaltet damit für jeden irreduziblen Charakter $\chi \in \mathrm{Irr}(G)$ auch die Funktionen $\mu_i\nu_y\chi$ für $i = 0, 1, 2$.

Wir können also schließen, dass es für den Beweis des Satzes hinreichend ist, dass für jede $\mathbb{Q}$-Klasse $\mathcal{C}$ aus $\mathcal{S}$ die Elemente aus $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C})}$ bereits in $\mathbb{Z}_{(p)}[\chi_1(g), \ldots, \chi_n(g)]$ liegen, wobei $g \in \mathcal{C}$ ist und $\chi_1, \ldots, \chi_n$ die irreduziblen Charaktere von G bezeichnen. Diese Aussage folgt direkt aus Lemma 4.4, womit der Satz bewiesen ist. □

Nachdem wir für eine Gruppe G mit einer zyklischen p-Sylowgruppe der Ordnung $\leq p^2$ ein Erzeugendensystem mit lediglich zwei Elementen für den $R(G)_p$-Modul $R(G)'_p/R(G)_p$ gefunden haben, müssen wir nun noch zeigen, dass der $R(G)_p$-Modul $\mathrm{rad}(R(G)'_p/R(G)_p)$ zyklisch ist

Wir betrachten also die maximale Ordnung $R(G)'_p \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C}_i)}$, wobei $\mathcal{C}_1, \ldots, \mathcal{C}_k$ die $\mathbb{Q}$-Klassen von G sind. Die maximalen Ideale in $R(G)'_p$ haben die Gestalt $((1), \ldots, \mathfrak{p}_i, \ldots, (1))$ mit einem maximalen Ideal $\mathfrak{p}_i$ von $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C}_i)}$, $i = 1, \ldots, k$ (siehe z. B. [44]).

Jedes Primideal von $\mathcal{O}_{\mathbb{Q}(\mathcal{C}_i)}$ enthält nach Satz 1.3 genau eine Primzahl $p \in \mathbb{Z}$. Die maximalen Ideale von $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C}_i)}$ stehen nach Proposition 1.18 also in Bijektion zu den Primidealen von $\mathcal{O}_{\mathbb{Q}(\mathcal{C}_i)}$, die p enthalten. Davon gibt es, wieder nach Satz 1.3, nur endlich viele. Lemma 1.2 liefert nun, dass $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C}_i)}$ ein Hauptidealring ist.

Wir betrachten den Kreisteilungskörper $\mathbb{Q}(\zeta_n)$ mit $n = p^a m$, $p^a > 2$ und $p \nmid m$. Seien $\mathfrak{P} \subseteq \mathcal{O}_{\mathbb{Q}(\zeta_n)}$, $\mathcal{P} \subseteq \mathcal{O}_{\mathbb{Q}(\zeta_m)}$ und $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{Q}(\zeta_{p^a})}$ Primideale, sodass $\mathfrak{P}$ sowohl über $\mathcal{P}$ als auch über $\mathfrak{p}$ liegt und alle drei Ideale über dem Ideal (p) von $\mathbb{Z}$ liegen. Da p in $\mathcal{O}_{\mathbb{Q}(\zeta_m)}$ unverzweigt ist, erhalten wir, unter Verwendung der Sätze 1.6 und 1.5, für die Verzweigungsindizes die Ungleichungskette

$$\begin{aligned}\varphi(p^a) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m)] &\geq e(\mathfrak{P}/\mathcal{P}) = e(\mathfrak{P}/\mathcal{P})e(\mathcal{P}/(p)) \\ &= e(\mathfrak{P}/(p)) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/(p)) = e(\mathfrak{P}/\mathfrak{p}) \cdot \varphi(p^a) \geq \varphi(p^a)\,.\end{aligned}$$

Es gilt also $e(\mathfrak{P}/(p)) = \varphi(p^a)$. Weiter ist $\mathfrak{p}$ nach Satz 1.16 total verzweigt über (p), insbesondere also das einzige Ideal in $\mathcal{O}_{\mathbb{Q}(\zeta_{p^a})}$, das über (p) liegt, und laut Lemma 1.17

gilt $\mathfrak{p} = (1 - \zeta_{p^a})$. Im Fall $p^a = 2$ erhalten wir natürlich ebenso $\mathfrak{p} = (2) = (1 - \zeta_2)$, wenn $\mathfrak{p}$ das Primideal von $\mathcal{O}_{\mathbb{Q}(\zeta_2)} = \mathbb{Z}$ ist, das über (2) liegt.

Das Radikal von $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\zeta_n)}$ ist der Durchschnitt aller maximalen Ideale dieses Rings. Da $(1 - \zeta_{p^a})$ das einzige maximale Ideal in $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\zeta_{p^a})}$ ist, liegt $(1 - \zeta_{p^a})$ als Ideal in $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\zeta_n)}$ betrachtet im Radikal. Angenommen, das Radikal hätte die Gestalt (α) mit $(\alpha) \subsetneq (1 - \zeta_{p^a})$. Dann wäre (α) das einzige maximale Ideal in $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\alpha)}$. Demzufolge wäre $e((\alpha)/(p)) > e((1 - \zeta_{p^a})/(p)) = \varphi(p^a)$. Nach Satz 1.6 ist dies jedoch unmöglich.

Analog erhält man für einen Teilkörper $\mathbb{L}$ von $\mathbb{Q}(\zeta_n)$ und $\mathbb{K} = \mathbb{L} \cap \mathbb{Q}(\zeta_{p^a})$, dass ein Erzeuger des Radikals von $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{K}}$ auch ein Erzeuger des Radikals von $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{L}}$ ist. Seien $g \in G$ ein Element der Ordnung n und λ ein Erzeuger von $\mathrm{Irr}(\langle g^{n/p^a} \rangle)$. Dann wird also das Radikal von $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathrm{cl}_{\langle g \rangle}(g))}$ durch $(\mathbb{1} - \lambda)(g)$ erzeugt. Somit hat das Radikal von $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathrm{cl}_G(g))}$ die Gestalt $(u((\mathbb{1} - \lambda)(g))^b)$ für eine Einheit $u \in \mathcal{O}_{\mathbb{Q}(\mathrm{cl}_{\langle g \rangle}(g))}$ und ein $b \in \mathbb{N}$.

Mithilfe dieser Vorbereitungen können wir jetzt den folgenden Satz beweisen.

Satz 4.6. *Seien die p-Sylowgruppen von G zyklisch der Ordnung $\leq p^2$. Dann ist der $R(G)_p$-Modul $\mathrm{rad}(R(G)'_p/R(G)_p)$ zyklisch.*

Beweis. Sei $g \in G$ ein Element mit zu p teilerfremder Ordnung und $\mathcal{S}$ die rationale p'-Sektion von g in G. Nach Bemerkung 2.12 genügt es zu zeigen, dass der $R(G)_p$-Modul $\mathrm{rad}(R(G)'_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}))/(R(G)_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}))$ zyklisch ist.

Das Element g habe die Ordnung m. Wir erhalten die Zerlegung $\mathcal{S} = \mathcal{C}_0 \cup \mathcal{C}_1 \cup \mathcal{C}_2$, wobei $\mathcal{C}_i$ genau die Elemente der Ordnung $p^i m$ von $\mathcal{S}$ enthält $(i = 0, 1, 2)$. Es ist durchaus möglich, dass $\mathcal{C}_2$ leer ist, bzw. dass $\mathcal{C}_1$ und $\mathcal{C}_2$ leer sind. Die nichtleeren Mengen unter den Mengen $\mathcal{C}_0$, $\mathcal{C}_1$ und $\mathcal{C}_2$ sind also genau die in $\mathcal{S}$ enthaltenden $\mathbb{Q}$-Klassen von G.

Für den Fall, dass sowohl $\mathcal{C}_1$ als auch $\mathcal{C}_2$ leer sind, ist wegen Lemma 2.10 schon alles gezeigt. Wir nehmen daher an, dass $|C_G(g)|$ durch p teilbar ist. Dann gilt zumindest $\mathcal{C}_1 \neq \emptyset$.

Nach den Bemerkungen im Vorfeld des Satzes ist (p) das Radikal von $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C}_0)}$. Demnach wird $\mathrm{rad}(R(G)'_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{C}_0))/(R(G)_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{C}_0))$ von $p\nu_g\mu_0$ erzeugt. Sicher sind auch die Funktionen $p\nu_g$, $p\nu_g\mu_1$ und $p\nu_g\mu_2$ in $\mathrm{rad}(R(G)'_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}))$ enthalten (im Fall $\mathcal{C}_2 = \emptyset$ gilt $\mu_2 = 0$). Wegen $p\nu_g\mu_0 = -p\nu_g\mu_1 - p\nu_g\mu_2 + p\nu_g$ genügt es also, einen Erzeuger von $\mathrm{rad}(R(G)'_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{C}_1 \cup \mathcal{C}_2))/(R(G)_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{C}_1 \cup \mathcal{C}_2))$ zu finden.

Sei zunächst $\mathcal{C}_2 = \emptyset$. Wir bezeichnen mit $\chi_1, \ldots, \chi_n$ die irreduziblen Charaktere von G und wählen ein Element $g_1 \in \mathcal{C}_1$. Nach Lemma 4.4 gilt $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C}_1)} = \mathbb{Z}_{(p)}[\chi_1(g_1), \ldots, \chi_n(g_1)]$. Zudem ist $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C}_1)}$ ein Hauptidealring, es existiert also ein Element π, welches das Radikal von $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C}_1)}$ erzeugt. Eine Funktion

$$\eta \in \mathrm{rad}(R(G)'_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}))/(R(G)_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}))$$

mit $\eta(g_1) = \pi$ und $\eta(h) = 0$ für $h \in G \setminus \mathcal{C}_1$ ist somit ein Erzeuger des $R(G)_p$-Moduls $\mathrm{rad}(R(G)'_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}))/(R(G)_p \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}))$, insbesondere ist dieser zyklisch.

Es verbleibt also der Fall $\mathcal{C}_2 \neq \emptyset$. Wir wählen Elemente $g_1 \in \mathcal{C}_1$ und $g_2 \in \mathcal{C}_2$ mit $g_2^p = g_1$ sowie Erzeuger π_1, π_2 der Radikale von $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C}_1)}$ und $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C}_2)}$. Wie eben existiert eine Funktion η_1 mit $\eta_1(g_1) = \pi_1$ und $\eta_1(h) = 0$ für $h \in G \setminus \mathcal{C}_1$. Wenn wir zeigen können, dass in deren Erzeugnis eine Funktion η_2 mit $\eta_2(g_2) = \pi_2$ und $\eta_2(h) = 0$ für $h \in G \setminus \mathcal{C}_2$ enthalten ist, haben wir den Satz bewiesen.

Dazu genügt es zu zeigen, dass die Funktion $\varphi \in R(G)'_p$ mit $\varphi(g_1) = \pi_1$, $\varphi(g_2) = \pi_2$ und $\varphi(x) = 0$ für $x \notin \mathcal{C}_1 \cup \mathcal{C}_2$, also $\varphi = \eta_1 + \eta_2$, bereits in $R(G)_p$ liegt. Nach Satz 1.28 ist dies genau dann der Fall, wenn φ_E für jede elementare Untergruppe $E \leq G$ in $R(E)_p$ enthalten ist. Da die p-Sylowgruppen von G zyklisch sind und φ auf allen Elementen, die nicht in $\mathcal{C}_1 \cup \mathcal{C}_2$ liegen, verschwindet, müssen wir nur die zyklischen Untergruppen von G, die g_1 enthalten, betrachten. Weiter dürfen wir annehmen, dass jede dieser zyklischen Untergruppen, deren Ordnung durch p^2 teilbar ist, g_2 ebenfalls beinhaltet.

Sei zuerst $C < G$ eine zyklische Untergruppe wie eben beschrieben, deren Ordnung nicht durch p^2 teilbar ist. Dann gilt $\langle g_1 \rangle \in \mathrm{Syl}_p(C)$. Sei λ ein Erzeuger von $\mathrm{Irr}(C)$, also $\pi = u((\mathbb{1} - \lambda^{|C|/p})(g_1))^b$ für geeignete $u \in \mathcal{O}_{\mathbb{Q}(\zeta_p)}$ und $b \in \mathbb{N}$. Da C zyklisch ist, gibt es einen virtuellen Charakter α von C, der auf g_1 den Wert u hat, denn $\{\chi(g_1) : \chi \in \mathrm{Irr}(C)\}$ enthält eine Ganzheitsbasis von $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$. Weiter hat $\mathbb{1} - \lambda^{|C|/p}$ auf allen p-regulären Elementen den Wert 0 und die einzige p-singuläre $\mathbb{Q}$-Klasse, die unter ν_{1_C} nicht verschwindet, ist die von g_1 erzeugte. Demnach gilt

$$\varphi_C = \alpha \cdot \nu_{1_C} \cdot (\mathbb{1} - \lambda^{|C|/p})^b \in R(C)_p \,.$$

Schließlich betrachten wir eine zyklische Untergruppe $C \leq G$ mit $g_2 \in C$ und setzen $M := \{i : 1 \leq i < p^2,\ g_2 \sim_G g_2^i\}$. Sind g_2 und g_2^i in G konjugiert, so gilt natürlich $\chi_C(g_2) = \chi_C(g_2^i)$ für jeden Charakter χ von G. Da das p enthaltende Primideal von $\mathcal{O}_{\mathbb{Q}(\mathrm{cl}_G(g_2))}$ nach den Sätzen 1.16 und 1.6 total verzweigt ist, muss (π_2) somit von $\big((1-\zeta_{p^2})(1-\zeta_{p^2}^i)\big)$ geteilt werden. Folglich ist $\Big(\prod_{i\in M}(1-\zeta_{p^2}^i)\Big)$ ein Teiler von (π_2). Außerdem gilt $(\pi_2)^e = (p)$, wobei e nach Satz 1.5 mit dem Grad der Körpererweiterung $\mathbb{Q}(\mathrm{cl}_G(g_2))/\mathbb{Q}$ übereinstimmt. Dieser wiederum entspricht nach Lemma 1.33 der Anzahl von Konjugationsklassen in G, die in der $\mathbb{Q}$-Klasse von g_2 liegen, d. h. $e = \frac{p^2-p}{|M|}$.

Das bedeutet, dass (π_2) bezogen auf $\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}$ ein Produkt aus $|M|$ Elementen mit der Norm p ist. Also folgt $(\pi_2) = \Big(\prod_{i\in M}\big(1-\zeta_{p^2}^i\big)\Big)$. Dieselbe Begründung liefert auch $(\pi_1) = \Big(\prod_{i\in M}\big(1-\zeta_p^i\big)\Big)$. Das Produkt läuft erneut genau über alle $i \in M$, weil $|M|$ ein Teiler von $p-1$ ist. Andernfalls läge ein Element der Ordnung p, das nicht in $\langle g_2 \rangle$ enthalten ist, in $N_G(\langle g_2 \rangle)$ und die p-Sylowgruppen von G wären daher nicht mehr zyklisch.

Sei jetzt λ ein Erzeuger von $\mathrm{Irr}(C)$, sodass $\lambda^{|C|/p^2}(g_2) = \zeta_{p^2}$ ist. Für eine beliebige ganze Zahl j ist dann $\mathbb{1} - \lambda^{j|C|/p^2} \in R(C)$ und es gilt

$$\left(\mathbb{1} - \lambda^{j|C|/p^2}\right)(g_1) = 1 - \zeta_p^j\,, \quad \left(\mathbb{1} - \lambda^{j|C|/p^2}\right)(g_2) = 1 - \zeta_{p^2}^j \quad \text{und}$$
$$\left(\mathbb{1} - \lambda^{j|C|/p^2}\right)(x) = 0 \quad \text{für jedes } p\text{-reguläre Element } x \in C\,.$$

Daher ist $\varphi_C = \nu_{1_C} \cdot \prod_{i \in M} \left(\mathbb{1} - \lambda^{i|C|/p^2}\right)$ eine Funktion aus $R(C)_p$ und insgesamt folgt, dass φ in $R(G)_p$ liegt. □

Aus den Sätzen 4.5 und 4.6 folgt jetzt sofort das gewünschte Resultat:

Folgerung 4.7. *Hat G eine zyklische p-Sylowgruppe der Ordnung $\leq p^2$, so ist der Darstellungstyp von $R(G)_p$ endlich.*

Insbesondere hat der Charakterring einer kubikfreien Gruppe, die nur zyklische Sylowgruppen besitzt, endlichen Darstellungstyp.

4.2 Elementar-abelsche Sylowgruppen

Wir haben eben gesehen, dass der Darstellungstyp von $R(G)_p$ ausschließlich von der Ordnung von P abhängt, wenn $P \in \mathrm{Syl}_p(G)$ zyklisch ist. Besitzt G dagegen eine elementar-abelsche p-Sylowgruppe, so benötigt man mehr Informationen über die Struktur von G, um entscheiden zu können, ob $R(G)_p$ endlichen oder unendlichen Darstellungstyp hat.

So hat beispielsweise der Charakterring jeder elementar-abelschen p-Gruppe vom Rang > 1 unendlichen Darstellungstyp, weil jede dieser Gruppen mindestens drei $\mathbb{Q}$-Klassen von Elementen der Ordnung p besitzt. Insbesondere ist der Darstellungstyp von $R(C_2 \times C_2)_2$ unendlich. Dagegen hat $R(A_4)_2$ ebenfalls eine zu $C_2 \times C_2$ isomorphe 2-Sylowgruppe, aber endlichen Darstellungstyp, weil in A_4 alle Involutionen konjugiert sind.

In diesem Abschnitt wollen wir nun untersuchen, welche Eigenschaften eine Gruppe G mit einer elementar-abelschen p-Sylowgruppe P besitzen muss bzw. welche sie nicht besitzen darf, damit $R(G)$ endlichen Darstellungstyp hat. Nach Folgerung 2.14 besitzt G entweder genau eine oder genau zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung p. Wir betrachten diese beiden Fälle getrennt.

In den Beweisen werden wir zumeist annehmen, dass P ein Normalteiler von G ist. Aufgrund der Resistenz abelscher Gruppen folgen die Aussagen dann auch allgemeiner, wenn P nicht normal in G ist.

4.2.1 Gruppen mit genau einer $\mathbb{Q}$-Klasse von Elementen der Ordnung p

Sei wieder p eine Primzahl und $\mathfrak{p}$ ein maximales Ideal von $\mathcal{O}_{\mathbb{Q}(\zeta_{|G|})}$, das p enthält. Nach Lemma 1.30 gilt für Elemente $x, y \in G$ mit $x_{p'} = y_{p'}$ die Kongruenz $\chi(x) \equiv \chi(y) \pmod{\mathfrak{p}}$ für jeden Charakter $\chi \in \mathrm{Irr}(G)$. Besitzt G eine elementar-abelsche p-Sylowgruppe und sind alle zyklischen Untergruppen der Ordnung p in G konjugiert, so lässt sich dieses Resultat noch verschärfen. Wir zeigen dies zunächst für einen Spezialfall, der Beweis dafür stammt von Haberland. Die allgemeine Aussage wird aus diesem Spezialfall schnell folgen.

Lemma 4.8 (Haberland)**.** *Seien $p > 2$, $k \geq 2$, P die additive Gruppe von $\mathbb{F}_{p^k}$ und C eine Untergruppe der multiplikativen Gruppe von $\mathbb{F}_{p^k}^\times$. Weiter sei*

$$G := \left\{ \begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} : a \in C,\, x \in P \right\},$$

$u \in G$ ein Element der Ordnung p und $\mathfrak{p}$ das p enthaltende maximale Ideal von $\mathcal{O}_{\mathbb{Q}(\mathrm{cl}_G(u))}$. Gibt es in G nur eine Konjugationsklasse von Untergruppen der Ordnung p, so gilt $\chi(1) \equiv \chi(u) \pmod{\mathfrak{p}^k}$ für jedes $\chi \in \mathrm{Irr}(G)$.

Beweis. Wir setzen

$$V := \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in P \right\} \cong P \quad \text{und} \quad H := \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in C \right\} \cong C\,.$$

Offenbar ist G das semidirekte Produkt $V \rtimes H$, wobei H transitiv auf den zyklischen Untergruppen von V operiert.

Die Anzahl der zyklischen Untergruppen von V ist $\frac{p^k-1}{p-1}$, da P als $\mathbb{F}_p$-Vektorraum der Dimension k aufgefasst werden kann. Der Stabilisator von $\mathbb{F}_p$ in der multiplikativen Gruppe $\mathbb{F}_{p^k}^\times$ ist $C \cap \mathbb{F}_p^\times$. Ist $|C| = n$, so hat dieser Stabilisator also $d := \mathrm{ggT}(n, p-1)$ Elemente und die Bahn von $\mathbb{F}_p$ die Länge $\frac{n}{d}$. Damit H transitiv auf V operiert, muss $\frac{n}{d}$ ein Vielfaches von $\frac{p^k-1}{p-1}$ sein, d. h. $n = \frac{p^k-1}{p-1} \cdot t$ mit $d \mid t \leq p-1$.

Man kann sehr leicht nachrechnen, dass G eine Frobeniusgruppe mit Kern V und Komplement H ist. Die Konjugationsklassen von G haben folgende Repräsentanten:

1. 1_G,
2. $P_1, \ldots, P_{\frac{p-1}{t}}$, wobei jedes P_i die Gestalt $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ mit $x \in \mathbb{F}_p$ hat,
3. $C_1, \ldots, C_{\frac{p^k-1}{p-1} \cdot t}$, wobei jedes C_j die Gestalt $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ mit $a \in C$ hat.

Die linearen Charaktere von G entstehen wegen $G' = V$ allesamt durch Fortsetzung der linearen Charaktere von H: Ist $\lambda \in \mathrm{Irr}(C)$, so kann man λ natürlich auch als linearen Charakter von H auffassen und man erhält einen linearen Charakter $\chi \in \mathrm{Irr}(G)$ durch $\chi(g) := \lambda(h)$, wobei $g = vh$ mit $v \in V$ und $h \in H$ ist. Für einen linearen Charakter $\chi \in \mathrm{Irr}(G)$ ist die Behauptung des Satzes damit gezeigt.

Die verbleibenden $\frac{p-1}{t}$ irreduziblen Charaktere von G entstehen, da G eine Frobeniusgruppe mit Kern V ist, durch Induktion irreduzibler Charaktere von V. Wir betrachten zunächst die irreduziblen Charaktere von P. Seien μ_p die (komplexen) p-ten Einheitswurzeln. Bekanntlich ist die Spurform

$$P \times P \to \mathbb{F}_p \to \mu_p\,, \quad (x,y) \mapsto \mathrm{Tr}_{\mathbb{F}_{p^k}/\mathbb{F}_p}(xy) \mapsto \zeta_p^{\mathrm{Tr}(xy)}$$

nicht ausgeartet, jeder irreduzible Charakter von P lässt sich also mithilfe dieser Form darstellen. Genauer ist $\mathrm{Irr}(P) = \{\lambda_x : x \in P\}$, wobei λ_x durch

$$\lambda_x : P \to \mu_p\,, \quad y \mapsto \zeta_p^{\mathrm{Tr}(xy)}$$

gegeben wird. Wir schreiben $\tilde{\lambda}_x$ für den entsprechenden Charakter von V, der zum Element $X := \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ gehört, d. h. $\tilde{\lambda}_x(Y) := \lambda_x(y)$ für $Y := \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$. Da die Konjugationsklassen von Elementen der Ordnung p in G von Matrizen repräsentiert werden, deren Eintrag rechts oben in $\mathbb{F}_p^\times$ liegt, genügt es, nur die induzierten Charaktere $\tilde{\lambda}_x^G$ mit $X \in \{P_1, \ldots, P_{\frac{p-1}{t}}\}$, also $x \in \mathbb{F}_p^\times$, und nur deren Werte auf Elementen $Y := \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$ mit $Y \in \{P_1, \ldots, P_{\frac{p-1}{t}}\}$, also $y \in \mathbb{F}_p^\times$, zu betrachten. Für den entsprechenden irreduziblen Charakter $\chi_x \in \mathrm{Irr}(G)$ erhalten wir (neben $\chi_x(1) = \frac{p^k-1}{p-1} \cdot t$ und $\chi_x(g) = 0$, $g \notin V$) die Werte

$$\begin{aligned}\chi_x(Y) = \tilde{\lambda}_x^G(Y) &= \frac{1}{|V|} \sum_{g \in G} \tilde{\lambda}_x^\circ(gYg^{-1}) = \sum_{g \in H} \tilde{\lambda}_x(gYg^{-1}) \\ &= \sum_{a \in C} \lambda_x(ay) = \sum_{a \in C} \zeta_p^{\mathrm{Tr}(xay)} = \sum_{a \in C} \zeta_p^{xy\mathrm{Tr}(a)} = \sum_{a \in C} \left(\zeta_p^{xy}\right)^{\mathrm{Tr}(a)}\,.\end{aligned}$$

Unser Ziel ist es, $\chi_x(1_G) \equiv \chi_x(Y) \pmod{\mathfrak{p}^k}$ zu zeigen. Da $\mathbb{Q}(\mathrm{cl}_G(Y))/\mathbb{Q}$ eine Körpererweiterung vom Grad $\frac{p-1}{t}$ ist, gilt $\mathfrak{p} = (1-\zeta_p)^t \cap \mathcal{O}_{\mathbb{Q}(\mathrm{cl}_G(Y))}$ (wir sehen $(1-\zeta_p)$ als Ideal in $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ an). Demzufolge müssen wir

$$\frac{p^k-1}{p-1} \cdot t \equiv \sum_{a \in C} \left(\zeta_p^{xy}\right)^{\mathrm{Tr}(a)} \quad \left(\mathrm{mod}\ (1-\zeta_p)^{tk}\right)$$

zeigen. Da die P_i für $i = 1, \ldots, \frac{p-1}{t}$ alle in derselben zyklischen Gruppe liegen, lassen sich $\chi_x(P_1), \ldots, \chi_x(P_{\frac{p-1}{t}})$ durch Galois-Automorphismen von $\mathbb{Q}(\mathrm{cl}_G(Y))/\mathbb{Q}$ ineinander überführen, es genügt also $\frac{p^k-1}{p-1} \cdot t \equiv s_1 \pmod{\mathfrak{p}^k}$ für $s_1 = \sum_{a \in C} \zeta_p^{\mathrm{Tr}(a)}$ zu beweisen.

Sei $M \leq \mathbb{F}_p^\times$ die Untergruppe, für die $\mathbb{F}_{p^k}^\times = \biguplus_{m\in M} mC$ gilt. Für $m \in M$ setzen wir dann

$$s(m) := \sum_{a\in m^{-1}C} \zeta_p^{\mathrm{Tr}(a)} = \sum_{a\in C} \zeta_p^{m\mathrm{Tr}(a)}\,.$$

Sei weiter $N \leq \mathrm{Irr}(\mathbb{F}_{p^k}^\times)$ die Untergruppe der irreduziblen Charaktere der multiplikativen Gruppe $\mathbb{F}_{p^k}$, die auf C trivial sind. Davon gibt es $\frac{p-1}{t}$ viele. Für $\psi \in N$ haben wir dann die Gaußsche Summe

$$\Gamma(\psi) := \sum_{\alpha\in\mathbb{F}_{p^k}^\times} \psi(\alpha)\zeta_p^{\mathrm{Tr}(\alpha)} = \sum_{m\in M}\sum_{a\in C} \psi(ma)\zeta_p^{m\mathrm{Tr}(a)} = \sum_{m\in M} \psi(m)s(m)\,.$$

Wir können die durch $\widetilde{\Gamma}(\psi) := \Gamma(\bar{\psi})$ definierte Funktion $\widetilde{\Gamma}$ also als Fourier-Transformierte von s ansehen und erhalten demzufolge

$$s_1 = s(1_G) = \frac{1}{\frac{p-1}{t}} \sum_{\psi\in N} \overline{\psi(1_G)}\Gamma(\psi) = \frac{t}{p-1}\sum_{\psi\in N}\Gamma(\psi)\,.$$

Da wir nur die Charaktere ψ betrachten, die auf C trivial sind, folgt $\psi(\alpha) = \alpha^{-\ell}$ für $\alpha \in \mathbb{F}_{p^k}^\times$ und ein $\ell \in \left\{\frac{p^k-1}{p-1}\cdot t\cdot r : r \in \left\{0,1,\ldots,\frac{p-1}{t}-1\right\}\right\}$.

Für den trivialen Charakter gilt, da die Spur ein surjektiver Gruppenhomomorphismus ist,

$$\Gamma(\mathbb{1}) = \sum_{a\in\mathbb{F}_{p^k}^\times} \zeta_p^{\mathrm{Tr}(a)} = -1 + \sum_{a\in\mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}(a)} = -1\,.$$

Sei $\psi \in N$ jetzt ein nichttrivialer Charakter, also

$$\Gamma(\psi) = \Gamma_\ell = \sum_{\alpha\in\mu_{p^k-1}} \alpha^{-\ell}\zeta_p^{\mathrm{Tr}(\alpha)}$$

für ein $\ell \in \left\{\frac{p^k-1}{p-1}\cdot t\cdot r : r \in \left\{1,2,\ldots,\frac{p-1}{t}-1\right\}\right\}$. Dann hat ℓ die Darstellung

$$\ell = \frac{p^k-1}{p-1}\cdot t\cdot r = tr(1+\ldots+p^{k-1})$$

für ein $r \in \left\{1,2,\ldots,\frac{p-1}{t}-1\right\}$. Nach Satz 1.20 gilt somit

$$\Gamma_\ell \equiv -\frac{(1-\zeta_p)^{ktr}}{((tr)!)^k} \pmod{(1-\zeta_p)^{ktr+1}}\,,$$

wobei dies eine Kongruenz in $\mathcal{O}_{\mathbb{Q}_p(\zeta_p)}$ ist. Demnach ist $\Gamma_\ell \equiv 0 \pmod{(1-\zeta_p)^{kt+1}}$ für $\ell \in \left\{\frac{p^k-1}{p-1}\cdot t\cdot r : r \in \left\{2,3,\ldots,\frac{p-1}{t}-1\right\}\right\}$. Das führt zu

$$s_1 - \frac{p^k-1}{p-1}\cdot t = \frac{t}{p-1}\sum_{\psi\in N}\Gamma(\psi) - \frac{p^k-1}{p-1}\cdot t \equiv \frac{t}{p-1}\left(-1 - \frac{(1-\zeta_p)^{kt}}{(t!)^k} - p^k + 1\right)$$
$$\equiv -\frac{t}{p-1}\cdot\left(\frac{(1-\zeta_p)^{tk}}{(t!)^k} + p^k\right) \pmod{(1-\zeta_p)^{kt+1}}.$$

Folglich ist $s_1 - \frac{p^k-1}{p-1}\cdot t$ durch $(1-\zeta_p)^{tk}$ teilbar. Da $\mathfrak{p} = ((1-\zeta_p)^t) \cap \mathcal{O}_{\mathbb{Q}(\mathrm{cl}_G(g))}$ ist, erhalten wir $\frac{p^k-1}{p-1}\cdot t \equiv s_1 \pmod{\mathfrak{p}}$ bzw. $\chi_x(1_G) \equiv \chi_x(Y) \pmod{\mathfrak{p}^k}$. □

Satz 4.9. *Sei $P \in \mathrm{Syl}_p(G)$ elementar-abelsch mit Ordnung $p^k \geq p^3$. Beinhaltet G nur eine $\mathbb{Q}$-Klasse von Elementen der Ordnung p und sind die Elemente der Ordnung p nichtrational, so hat $R(G)$ unendlichen Darstellungstyp.*

Beweis. Aus den Voraussetzungen folgt sofort, dass p ungerade ist. Sei x ein Element der Ordnung p. Nach der Klassifikation der endlichen transitiven linearen Gruppen muss G eine Untergruppe H enthalten, die zu einer Untergruppe von $\Gamma\mathrm{L}(p^k)$ isomorph ist, in der x liegt und in der es genauso viele Konjugationsklassen der Ordnung p gibt wie in G. Wir setzen zudem voraus, dass H eine minimale Untergruppe von G mit dieser Eigenschaft sei.

Wir nehmen zunächst an, dass H zu einer Gruppe wie in Lemma 4.8 isomorph ist. Für jeden irreduziblen Charakter $\chi \in \mathrm{Irr}(H)$ gilt $\chi(1) \equiv \chi(x) \pmod{\mathfrak{p}^k}$ nach Lemma 4.8, wobei $\mathfrak{p}$ das p enthaltende maximale Ideal von $\mathcal{O}_{\mathbb{Q}(\mathrm{cl}_H(x))} = \mathcal{O}_{\mathbb{Q}(\mathrm{cl}_G(x))}$ ist. Daher muss auch $\eta(1) \equiv \eta(x) \pmod{\mathfrak{P}^k}$ für jede Funktion $\eta \in R(H)_p$ gelten, wobei $\mathfrak{P}$ das maximale Ideal in $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathrm{cl}_H(x))}$ bezeichnet. Die Einschränkung einer Klassenfunktion aus G auf H ist natürlich eine Klassenfunktion auf H, weswegen sogar $\eta(1) \equiv \eta(x) \pmod{\mathfrak{P}^k}$ für $\eta \in R(G)_p$ folgt.

In $R(G)'_p$ existieren offenbar Funktionen ψ_1, ψ_2 mit $\psi_1(x) \in \mathfrak{P}\setminus\mathfrak{P}^2$, $\psi_2(x) \in \mathfrak{P}^2\setminus\mathfrak{P}^3$ sowie $\psi_1(g) = 0 = \psi_2(g)$ für jedes $g \in G$, dessen Ordnung verschieden von p ist. Angenommen, es gibt ein $\alpha \in \mathrm{rad}(R(G)'_p)$, das den $R(G)_p$-Modul $\mathrm{rad}(R(G)'_p/R(G)_p)$ erzeugt. Dann existieren $\eta_1, \eta_2, \varphi_1, \varphi_2 \in R(G)_p$ mit $\eta_1\alpha+\eta_2 = \psi_1$ und $\varphi_1\alpha+\varphi_2 = \psi_2$. Die Werte $\eta_1(1)$, $\eta_2(1)$, $\varphi_1(1)$ und $\varphi_2(1)$ liegen, da sie rational sind, jeweils entweder in $\mathfrak{P}^k$ oder nicht in $\mathfrak{P}$. Nach Lemma 4.8 liegen also auch $\eta_1(x)$, $\eta_2(x)$, $\varphi_1(x)$ und $\varphi_2(x)$ jeweils entweder in $\mathfrak{P}^k$ oder nicht in $\mathfrak{P}$.

Nun gilt $\eta_1(x)\alpha(x)+\eta_2(x) = \psi_1(x) \in \mathfrak{P}\setminus\mathfrak{P}^2$. Weil $\alpha(x)$ in $\mathfrak{P}$ liegt, muss auch $\eta_2(x)$ in $\mathfrak{P}$ enthalten sein und damit sogar $\eta_2(x) \in \mathfrak{P}^k$. Das impliziert $\alpha(x) \in \mathfrak{P}\setminus\mathfrak{P}^2$. Weiter gilt $\varphi_1(x)\alpha(x)+\varphi_2(x) = \psi_2(x) \in \mathfrak{P}^2\setminus\mathfrak{P}^3$. Weil $\alpha(x)$ in $\mathfrak{P}$ liegt, muss zunächst $\varphi_2(x)$ in $\mathfrak{P}$ und damit sogar in $\mathfrak{P}^k$ sein. Nun liegt aber $\alpha(x)$ nicht in $\mathfrak{P}^2$, d. h. $\varphi_1(x)$ müsste ein Element aus $\mathfrak{P}\setminus\mathfrak{P}^2$ sein. Dies ist jedoch unmöglich, also kann der $R(G)_p$-Modul $\mathrm{rad}(R(G)'_p/R(G)_p)$ nicht zyklisch sein. Damit hat $R(G)_p$ und folglich auch $R(G)$ unendlichen Darstellungstyp.

Es verbleibt der Fall, dass H nicht zu einer Gruppe wie in Lemma 4.8 isomorph ist. Sei also H isomorph zu $K := C_p^k \rtimes \left(C_{\frac{p^k-1}{p-1}\cdot\frac{t}{m}} \rtimes C_m\right)$ für geeignete natürliche

Zahlen t und k ($\mathrm{ggT}(k, p-1) \mid t \mid p-1$ und $m \mid k$). Wir zeigen, dass dann ebenfalls $\chi(1) \equiv \chi(x) \pmod{\mathfrak{p}^k}$ für $\chi \in \mathrm{Irr}(G)$ gilt.

Sei dazu L die zu $C_p^k \rtimes C_{\frac{p^k-1}{p-1}t}$ isomorphe Untergruppe von $\mathbb{F}_p^k \rtimes \Gamma\mathrm{L}(p^k)$. Die Konjugationsklassen von Elementen der Ordnung p in L stimmen mit den Konjugationsklassen von Elementen der Ordnung p in $M := C_p^k \rtimes \left(C_{\frac{p^k-1}{p-1}t} \rtimes C_m\right) \leq \mathbb{F}_p^k \rtimes \Gamma\mathrm{L}(p^k)$ überein, weil Galois-Automorphismen von $\mathbb{F}_{p^k}$ den Teilkörper $\mathbb{F}_p$ fest lassen. Da H nur eine $\mathbb{Q}$-Klasse von Elementen der Ordnung p besitzt, stimmen ebenso die Konjugationsklassen von Elementen der Ordnung p in M und K überein.

Sei $\lambda \in \mathrm{Irr}(C_p^k)$. Wegen $|K| = |L|$ und weil Elemente $y, z \in C_p^k$ genau dann in K konjugiert sind, wenn sie in L konjugiert sind, folgt $\lambda^K(y) = \lambda^L(y)$. Damit folgt aber auch $\lambda^K(1) \equiv \lambda^K(y) \pmod{\mathfrak{p}^k}$. Für jedes $\psi \in \mathrm{Irr}(H)$ gilt dementsprechend $\psi(1) \equiv \psi(x) \pmod{\mathfrak{p}^k}$ und somit $\chi(1) \equiv \chi(x) \pmod{\mathfrak{p}^k}$ für jedes $\chi \in \mathrm{Irr}(G)$. Mit derselben Argumentation wie im Fall, dass H zu einer Gruppe wie in Lemma 4.8 isomorph ist, kann man jetzt zeigen, dass der $R(G)_p$-Modul $\mathrm{rad}(R(G)'_p/R(G)_p)$ nicht zyklisch ist. Der Darstellungstyp von $R(G)$ muss daher unendlich sein. □

Folgerung 4.10. *Sei $P \in \mathrm{Syl}_p(G)$ elementar-abelsch mit Ordnung $p^k \geq p^3$. Ist der Darstellungstyp von $R(G)$ endlich und beinhaltet G nur eine $\mathbb{Q}$-Klasse von Elementen der Ordnung p, so ist $p^k - 1$ kubikfrei und alle nichttrivialen Elemente von P sind in G konjugiert.*

Beweis. Nach der Klassifikation der endlichen transitiven linearen Gruppen tritt einer der beiden folgenden Fälle ein:

1. Die Operation von $N_G(P)/C_G(P)$ auf P entspricht der von $\Gamma\mathrm{L}(p^k)$ auf $\mathbb{F}_p^k$. Nach Bemerkung 3.9 ist der Exponent von G ein Teiler von $p^k - 1$. Folglich muss $p^k - 1$ kubikfrei sein, damit $R(G)$ endlichen Darstellungstyp haben kann.

2. $P \cong C_3^4$ und $N_G(P)/C_G(P)$ operiert wie eine der sporadischen transitiven linearen Gruppen auf P. Dann enthält G eine extraspezielle 2-Gruppe H der Ordnung 2^5. In dieser gibt es Involutionen, die nicht miteinander kommutieren, also kann H keine Untergruppe einer Suzuki 2-Gruppe sein. Damit sind die 2-Sylowgruppen von G aber zu keiner Gruppe aus der Liste in Satz 3.12 isomorph, also hat $R(G)$ unendlichen Darstellungstyp. □

Umgekehrt gibt es zu jeder elementar-abelschen Gruppe P der Ordnung p^k ($k \geq 1$), wobei $p^k - 1$ kubikfrei ist, eine Gruppe G, sodass $P \in \mathrm{Syl}_p(G)$ und der Darstellungstyp von $R(G)$ endlich ist: Die zyklische Gruppe C_{p^k-1} operiert regulär auf den nichttrivialen Elementen von P, wobei die Operation der von $\Gamma\mathrm{L}_0(p^k)$ auf $\mathbb{F}_p^k$ entspricht. Folglich erfüllt $G := P \rtimes C_{p^k-1}$ die Bedingungen.

Weil $p^{2k} - 1$ für jede positive ganze Zahl k durch 8 teilbar ist, impliziert Folgerung 4.10, dass G keine elementar-abelsche p-Gruppe von geradem Rang > 2 als p-Sylowgruppe haben kann, wenn es in G nur eine $\mathbb{Q}$-Klasse von Elementen der

Ordnung p gibt und $R(G)$ endlichen Darstellungstyp hat. Den Fall, dass G eine elementar-abelsche p-Gruppe der Ordnung p^2 als 2-Sylowgruppe hat, betrachten wir gesondert.

Proposition 4.11. *Seien $P \in \mathrm{Syl}_p(G)$ eine elementar-abelsche Gruppe der Ordnung p^2 und der Darstellungstyp von $R(G)$ endlich. Sind alle Untergruppen der Ordnung p in G konjugiert, so sind auch alle Elemente der Ordnung p in G konjugiert und es gilt $p \in \{2, 5, 11, 29, 59\}$.*

Beweis. Im Fall $p = 2$ sind die Behauptungen automatisch erfüllt, wir nehmen also an, dass p ungerade ist. Da $p^2 - 1$ durch 8 teilbar ist, müsste G ein Element der Ordnung 8 besitzen, wenn $N_G(P)/C_G(P)$ auf P wie eine Untergruppe von $\Gamma\mathrm{L}(p^2)$ auf $\mathbb{F}_p^2$ operiert. Dann hätte $R(G)$ aber unendlichen Darstellungstyp.

Folglich besitzt G eine Untergruppe, die zu einer Untergruppe einer der sporadischen 2-transitiven Gruppen isomorph ist, und wir erhalten $p \in \{5, 7, 11, 19, 23, 29, 59\}$. Mit GAP lässt sich schnell nachrechnen, dass für $p \in \{7, 23\}$ jede Gruppe, in der alle Untergruppen der Ordnung p konjugiert sind, ein Element der Ordnung 8 enthält.

Als nächstes untersuchen wir den Fall $p = 19$. Die Gruppe $C_{19}^2 \rtimes (C_9 \times \mathrm{SL}(2,5))$ enthält zu $C_9 \times C_3$ isomorphe 3-Sylowgruppen. Enthält G eine solche Untergruppe, ist der Darstellungstyp von $R(G)$ folglich unendlich.

In den Gruppen $H_1 := C_{19}^2 \rtimes (C_3 \times \mathrm{SL}(2,5))$ und $H_2 := C_{19}^2 \rtimes \mathrm{SL}(2,5)$ gibt es jeweils drei Konjugationsklassen von Elementen der Ordnung 19. Sei $\mathcal{C}$ eine dieser Klassen, $x \in \mathcal{C}$ und $\mathfrak{p}$ das 19 enthaltende maximale Ideal von $\mathcal{O}_{\mathbb{Q}(\mathcal{C})}$. Mit GAP lässt sich überprüfen, dass dann $\chi(1) \equiv \chi(x) \pmod{\mathfrak{p}^2}$ für jeden irreduziblen Charakter χ von H_1 bzw. H_2 gilt. Außerdem gibt es einen irreduziblen Charakter ψ von H_1 bzw. H_2 und ein $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mathcal{C})/\mathbb{Q})$, sodass jeder irreduzible Charakter auf x entweder rational ist oder einen der Werte $\psi(x)$, $\sigma(\psi(x))$, $\sigma^2(\psi(x))$ annimmt.

Damit können wir nun zeigen, dass der $R(H_i)_{19}$-Modul $\mathrm{rad}(R(H_i)'_{19})/R(H_i)_{19})$, $i \in \{1, 2\}$, nicht zyklisch ist. Wäre α ein Erzeuger dieses Moduls, so wäre $\alpha(x) \in \mathfrak{P} \setminus \mathfrak{P}^2$, wobei $\mathfrak{P}$ das maximale Ideal in $\mathbb{Z}_{(19)} \otimes \mathcal{O}_{\mathbb{Q}(\mathcal{C})}$ ist. Für jede Funktion η aus dem Erzeugnis von α gilt dann aber $\eta(x) \in \mathfrak{P}^2$ oder $\eta(x) = r \cdot \alpha(x)$ für eine rationale Zahl r mit zu 19 teilerfremdem Nenner. Demnach gibt es kein η mit $\eta(x) = \sigma(\alpha(x))$, obwohl die Funktion φ mit $\varphi(x) = \sigma(\alpha(x))$ und $\varphi(h) = 0$ für $h \in H_i$ in $\mathrm{rad}(R(H_i)'_{19}) \setminus R(H_i)_{19}$ liegt. Damit ist auch der $R(G)_{19}$-Modul $\mathrm{rad}(R(G)'_{19})/R(G)_{19})$ nicht zyklisch, was der Voraussetzung, dass $R(G)$ endlichen Darstellungstyp hat, widerspricht.

In den weiteren Untergruppen von $C_{19}^2 \rtimes (C_9 \times \mathrm{SL}(2,5))$ sind nicht alle Untergruppen der Ordnung 19 konjugiert, weswegen G keine zu C_{19}^2 isomorphe 19-Sylowgruppe besitzen kann.

Es verbleibt zu zeigen, dass für $p \in \{5, 11, 29, 59\}$ alle Elemente der Ordnung p in G konjugiert sind. Die Gruppe $C_5^2 \rtimes \mathrm{SL}(2,3)$ besitzt keine echte Untergruppe, in der alle Untergruppen der Ordnung 5 konjugiert sind. Ebenso gibt es in $C_{11}^2 \rtimes \mathrm{SL}(2,5)$

keine echte Untergruppe mit nur einer Konjugationsklasse von Untergruppen der Ordnung 11. In diesen Fällen ist daher nichts zu zeigen.

Die Gruppe $C_{11}^2 \rtimes (C_5 \times \mathrm{SL}(2,3))$ enthält genau eine echte Untergruppe H, deren Ordnung von 11^2 geteilt wird und in der alle Untergruppen der Ordnung 11 konjugiert sind. Diese ist zu $C_{11}^2 \rtimes \mathrm{SL}(2,3)$ isomorph. Ist $\mathfrak{p}$ das 11 enthaltende maximale Ideal von $\mathcal{O}_{\mathbb{Q}(\mathrm{cl}_H(x))}$, so gilt für jedes Element $x \in H$ der Ordnung 11 und jedes $\chi \in \mathrm{Irr}(H)$ die Kongruenz $\chi(1) \equiv \chi(x) \pmod{\mathfrak{p}^3}$. Analog zum Beweis von Satz 4.9 kann man jetzt schließen, dass der $R(H)_{11}$-Modul $\mathrm{rad}(R(H)'_{11}/R(H)_{11})$ nicht zyklisch ist. Der $R(G)_{11}$-Modul $\mathrm{rad}(R(G)'_{11}/R(G)_{11})$ kann also nur dann zyklisch sein, wenn G neben H auch eine zu $C_{11}^2 \rtimes (C_5 \times \mathrm{SL}(2,3))$ isomorphe Untergruppe enthält.

Analog lassen sich die Fälle $p = 29$ bzw. $p = 59$ behandeln. Die einzige echte Untergruppe H von $C_{29}^2 \rtimes (C_7 \times \mathrm{SL}(2,5))$, deren Ordnung von 29^2 geteilt wird und in der alle Untergruppen der Ordnung 29 konjugiert sind, ist zu $C_{29}^2 \rtimes \mathrm{SL}(2,5)$ isomorph. Für $x \in H$ der Ordnung 29, $\chi \in \mathrm{Irr}(H)$ und das maximale Ideal $\mathfrak{p}$ von $\mathcal{O}_{\mathbb{Q}(\mathrm{cl}_H(x))}$, das 29 enthält, gilt hier sogar $\chi(1) \equiv \chi(x) \pmod{\mathfrak{p}^6}$.

Schließlich hat $C_{59}^2 \rtimes (C_{29} \times \mathrm{SL}(2,5))$ nur eine einzige echte Untergruppe H, deren Ordnung ein Vielfaches von 59^2 ist und die nur eine Konjugationsklasse von Untergruppen der Ordnung 59 enthält. Diese ist zu $C_{59}^2 \rtimes \mathrm{SL}(2,5)$ isomorph und für $x \in H$ mit Ordnung 59, $\chi \in \mathrm{Irr}(H)$ und das maximale Ideal $\mathfrak{p}$ von $\mathcal{O}_{\mathbb{Q}(\mathrm{cl}_H(x))}$, in dem die 59 liegt, erhalten wir $\chi(1) \equiv \chi(x) \pmod{\mathfrak{p}^6}$. □

Auch hier gibt es zu jeder elementar-abelschen p-Gruppe P der Ordnung p^2 mit $p \in \{2, 5, 11, 29, 59\}$ eine Gruppe G, sodass $R(G)$ endlichen Darstellungstyp hat und $P \in \mathrm{Syl}_p(G)$ gilt. Natürlich ist der Darstellungstyp von $R(A_4)$ endlich. Weiter lässt sich leicht nachprüfen, dass die Charakterringe der sporadischen 2-transitiven Gruppen

$$C_5^2 \rtimes \mathrm{SL}(2,3), \quad C_{11}^2 \rtimes (C_5 \times \mathrm{SL}(2,3)), \quad C_{11}^2 \rtimes \mathrm{SL}(2,5),$$
$$C_{29}^2 \rtimes (C_7 \times \mathrm{SL}(2,5)) \quad \text{und} \quad C_{59}^2 \rtimes (C_{29} \times \mathrm{SL}(2,5))$$

allesamt endlichen Darstellungstyp haben, denn die nichttrivialen Elemente des jeweiligen elementar-abelschen Normalteilers sind in diesen Gruppen alle konjugiert.

Mit den Argumenten aus dem Beweis von Proposition 4.11 folgt sogar noch, dass jede Gruppe G eine dieser 2-transitiven Gruppen enthalten muss, wenn $P \in \mathrm{Syl}_p(G)$ die Ordnung p^2 hat, alle Untergruppen der Ordnung p in G konjugiert sind und der Darstellungstyp von $R(G)$ endlich ist.

Bisher haben wir uns nur angeschaut, welche Bedingungen die Elemente der Ordnung p einer Gruppe G mit elementar-abelscher p-Sylowgruppe erfüllen müssen, damit $R(G)_p$ endlichen Darstellungstyp hat. Im Allgemeinen ist es allerdings nicht ausreichend, sich lediglich auf die Betrachtung der p-Elemente zu beschränken. Die folgenden Beispiele illustrieren dies.

Beispiel 4.12.

1. Sei $G = (C_5^2 \times C_{11}^2) \rtimes C_{12}$, wobei C_{12} auf C_5^2 wie die Untergruppe vom Index 2 in $\Gamma\mathrm{L}_0(5^2)$ auf $\mathbb{F}_5^2$ operiert und auf C_{11}^2 wie die Untergruppe vom Index 10 in $\Gamma\mathrm{L}_0(11^2)$ auf $\mathbb{F}_{11}^2$. Dann gibt es für jeden Primteiler p von $|G|$ höchstens zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung p. Da G jedoch 240 Konjugationsklassen von Elementen der Ordnung 55 beinhaltet, muss es zu einem $x \in G$ der Ordnung 5 mindestens drei $\mathbb{Q}$-Klassen von Elementen der Ordnung 55 geben. Folglich besitzt jedes Erzeugendensystem von $R(G)'_{11}/R(G)_{11}$ mindestens drei Erzeuger, was sich durch alleinige Betrachtung der Elemente der Ordnung 11 nicht zeigen ließe.
2. Sei $G = (C_3^3 \times C_5) \rtimes C_{52}$, wobei die zyklische Gruppe der Ordnung 52 jeweils transitiv auf den nichttrivialen Elementen von C_3^3 und C_5 operiert. Dann gibt es jeweils nur eine Konjugationsklasse von Elementen der Ordnung 3 bzw. 5, aber zwei Klassen von Elementen der Ordnung 15. Die einzigen nichtreellen Werte irreduzibler Charaktere von G auf diesen sind $\frac{1\pm3\sqrt{-15}}{2}$. Folglich kann $\mathrm{rad}(R(G)'_3/R(G)_3)$ nicht zyklisch sein, d. h., der Darstellungstyp von $R(G)_3$ und somit auch der von $R(G)$ ist unendlich.

Das zweite Beispiel zeigt, dass der Darstellungstyp von $R(G)$ selbst dann nicht endlich sein muss, wenn es einen Normalteiler $N \trianglelefteq G$ mit $\mathrm{ggT}(|N|, |G : N|) = 1$ gibt, sodass sowohl $R(N)$ als auch $R(G/N)$ endlichen Darstellungstyp haben (man kann im obigen Beispiel $N = C_5$ wählen).

Umgekehrt lässt sich daraus, dass $R(G)$ endlichen Darstellungstyp hat, natürlich nicht schließen, dass auch $R(N)$ für einen Normalteiler $N \trianglelefteq G$ endlichen Darstellungstyp hat, was schon durch die Wahl $G = A_4$, $N = C_2^2$ deutlich wird. Folglich kann es keine Reduktionssätze geben, die den Darstellungstyp von $R(G)$ mit dem des Charakterrings eines Normalteilers von G in Verbindung bringen.

Das zweite Beispiel mag außerdem suggerieren, dass, wenn G eine (nichtzyklische) elementar-abelsche p-Sylowgruppe P besitzt, alle Untergruppen der Ordnung p in G konjugiert sind und $R(G)$ endlichen Darstellungstyp hat, alle Elemente in einer beliebigen rationalen p'-Sektion von G konjugiert sein müssen. Dem ist natürlich nicht so, wie man leicht mithilfe von Proposition 4.1 sieht. Hat $R(G)$ endlichen Darstellungstyp und ist ℓ eine Primzahl, die $|G|$ nicht teilt, so hat auch $R(G \times C_\ell)$ endlichen Darstellungstyp. Für einen Primteiler p von $|G|$ und ein nichttriviales Element $x \in C_\ell$ sind jedoch nicht alle Elemente der rationalen p'-Sektion von $G \times C_\ell$, die x enthält, konjugiert.

4.2.2 Gruppen mit genau zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung p

Der Fall, dass es in G genau zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung p gibt, ist deutlich komplizierter als der vorige, weil es hier kein zu Satz 1.52 analoges

Klassifikationsresultat gibt. Nichtsdestotrotz lassen sich auch hier einige allgemeine Aussagen treffen. Da eine Gruppe mit elementar-abelscher 2-Sylowgruppe nie genau zwei Klassen von Involutionen besitzen kann, setzen wir in diesem Abschnitt stets voraus, dass p eine ungerade Primzahl ist.

Lemma 4.13. *Seien G eine endliche Gruppe und $P \in \mathrm{Syl}_p(G)$ elementar-abelsch mit Ordnung $p^k \geq p^3$. Beinhaltet G zwei rationale Konjugationsklassen von Elementen der Ordnung p, so hat $R(G)$ unendlichen Darstellungstyp.*

Beweis. Zunächst ist klar, dass $R(G)$ unendlichen Darstellungstyp hat, falls G mehr als zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung p hat. Wir nehmen daher im Folgenden an, dass G genau zwei $\mathbb{Q}$-Klassen $\mathcal{C}_1$, $\mathcal{C}_2$ von Elementen der Ordnung p besitzt und dass beide rational sind.

Wir zeigen nun, dass der $R(G)_p$-Modul $\mathrm{rad}(R(G)'_p/R(G)_p)$ mindestens zwei Erzeuger benötigt. Auf jeden Fall liegt die Funktion ψ_1 mit $\psi_1(1) = p$ und $\psi_1(g) = 0$ für $g \in G \setminus \{1\}$ in $R(G)'_p \setminus R(G)_p$. Ist ϱ der Charakter der regulären Darstellung von G, so gilt $\psi_1 = \frac{p}{|G|}\varrho$, also ist sogar $p^{k-2}\psi_1 \in R(G)'_p \setminus R(G)_p$ und es gilt $\langle \psi_1, \mathbb{1} \rangle = \frac{p}{|G|}$.

Sei $x \in P$ ein Element aus $\mathcal{C}_1$. Nach Lemma 2.17 existiert ein Charakter ψ von G mit

$$\begin{aligned}
\psi(g) &= \begin{cases} \frac{|C_G(g)|}{|\langle x \rangle|} \cdot \sum\limits_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{|\langle g \rangle|})/\mathbb{Q}(\mathrm{cl}_G(g)))} 1, & g \sim_G x^k \text{ für ein } k \in \mathbb{Z} \\ 0, & \text{sonst} \end{cases} \\
&= \begin{cases} \frac{|C_G(g)|}{|\langle x \rangle|} \cdot \frac{|N_G(\langle g \rangle)|}{|C_G(g)|}, & g \sim_G x^k \text{ für ein } k \in \mathbb{Z} \\ 0, & \text{sonst} \end{cases} \\
&= \begin{cases} \frac{|N_G(\langle g \rangle)|}{|\langle x \rangle|}, & g \sim_G x^k \text{ für ein } k \in \mathbb{Z} \\ 0, & \text{sonst} \end{cases}.
\end{aligned}$$

Ebenfalls nach Lemma 2.17 gilt $\langle \psi, \mathbb{1} \rangle = 1$. Deshalb liegt auch die Funktion

$$\psi_2 := \frac{p^2}{|N_G(\langle x \rangle)|} \left(\psi - \frac{|G|}{p^2} \psi_1 \right),$$

d. h. $\psi_2(g) = p$ für $g \sim_G x$ und $\psi_2(g) = 0$ für alle anderen $g \in G$, in $R(G)'_p \setminus R(G)_p$ und es gilt

$$\langle \psi_2, \mathbb{1} \rangle = \frac{p^2}{|N_G(\langle x \rangle)|} - \frac{|G|}{|N_G(\langle x \rangle)|} \cdot \frac{p}{|G|} = \frac{p^2}{|N_G(\langle x \rangle)|} - \frac{p}{|N_G(\langle x \rangle)|} = \frac{p}{|C_G(x)|}.$$

Analog ist für $y \in P \cap \mathcal{C}_2$ die Funktion ψ_3 mit $\psi_3(g) = p$ für $g \sim_G y$ und $\psi_3(g) = 0$ für jedes andere $g \in G$ ein Element aus $R(G)'_p \setminus R(G)_p$.

Sei $\chi \in \mathrm{Irr}(G)$. Dann ist $\chi(x) - \chi(1)$ durch p teilbar, da $\mathrm{cl}_G(x)$ rational ist. Angenommen

$$\chi(x) - \chi(1) \equiv rp \pmod{p^k} \tag{4.2}$$

für ein $r \in \mathbb{Z}$ mit $\mathrm{ggT}(r,p) = 1$. Dann gibt es ein $\varphi \in R(G)_p$, sodass $0 \leq (\chi-\varphi)(1) < p^k$, $(\chi-\varphi)(x) - (\chi-\varphi)(1) \equiv rp \pmod{p^k}$ und $(\chi-\varphi)(y) = 0$ ist, denn $\mathbb{1}$, $p^{k-1}\psi_1$ und $p^{k-1}\psi_2$ liegen in $R(G)$. Gleiches gilt dann auch für die Funktion $\eta := \nu_1(\chi-\varphi)$, die in $R(G)_p$ liegt. Wir haben jetzt also eine Funktion $\eta \in R(G)_p$ erhalten mit

$$\eta(g) = \begin{cases} ap, & g = 1 \\ bp, & g \sim_G x \\ 0, & \text{sonst} \end{cases},$$

wobei $a, b \in [0, p^{k-1}-1]$ ganze Zahlen sind und $bp - ap \equiv rp \pmod{p^k}$ gilt. Daher lässt sich η darstellen als $\eta = a\psi_1 + b\psi_2$ und wir erhalten

$$\langle \eta, \mathbb{1} \rangle = a\langle \psi_1, \mathbb{1} \rangle + b\langle \psi_2, \mathbb{1} \rangle = \frac{ap}{|G|} + \frac{bp}{|C_G(x)|} = \frac{p(a + b \cdot |\mathrm{cl}_G(x)|)}{|G|}.$$

Da $\eta \in R(G)_p$ ist, muss der Zähler durch p^k teilbar sein, also folgt

$$a + b \cdot |\mathrm{cl}_G(x)| \equiv 0 \pmod{p^{k-1}}. \tag{4.3}$$

Weiter gilt

$$\langle \eta, \chi \rangle = \frac{1}{|G|} \cdot (\eta(1)\chi(1) + |\mathrm{cl}_G(x)|\eta(x)\chi(x)) = \frac{ap\chi(1) + |\mathrm{cl}_G(x)| \cdot bp\chi(x)}{|G|}.$$

Auch hier muss der Zähler wieder durch p^{k-1} teilbar sein, also folgt

$$a\chi(1) + |\mathrm{cl}_G(x)|b\chi(x) \equiv 0 \pmod{p^{k-1}}.$$

Ersetzen wir in dieser Kongruenz $\chi(1)$ nach (4.2) durch $\chi(x) - rp$ und a gemäß (4.3) durch $-b|\mathrm{cl}_G(x)|$, so ergibt sich

$$0 \equiv -b|\mathrm{cl}_G(x)| \cdot (\chi(x) - rp) + b|\mathrm{cl}_G(x)|\chi(x) \equiv pbr|\mathrm{cl}_G(x)| \pmod{p^{k-1}}.$$

Nun ist $|\mathrm{cl}_G(x)| = |G : C_G(x)|$ teilerfremd zu p, weil P abelsch ist, und r wird entsprechend unserer Annahme nicht von p geteilt. Also ist $b \equiv 0 \pmod{p^{k-2}}$. Nach (4.3) folgt daher auch $a \equiv 0 \pmod{p^{k-2}}$. Wir hatten aber $bp - ap \equiv rp \pmod{p^k}$ bei der Definition von η vorausgesetzt, was $a \equiv b \equiv 0 \pmod{p^{k-2}}$ widerspricht.

Für jeden irreduziblen Charakter $\chi \in \mathrm{Irr}(G)$ gilt also $\chi(1) \equiv \chi(x) \pmod{p^2}$. Dieselbe Argumentation wie oben liefert auch $\chi(1) \equiv \chi(y) \pmod{p^2}$ für $\chi \in \mathrm{Irr}(G)$. Demzufolge gilt für jede Funktion $\eta \in R(G)_p$ ebenfalls $\eta(1) \equiv \eta(x) \equiv \eta(y) \pmod{p^2}$.

Angenommen, der $R(G)_p$-Modul $\mathrm{rad}(R(G)'_p/R(G)_p)$ wäre zyklisch und würde von $\alpha \in \mathrm{rad}(R(G)'_p) \setminus R(G)_p$ erzeugt. Dann gäbe es $\eta_1, \eta_2, \varphi_1, \varphi_2, \xi_1, \xi_2 \in R(G)_p$ mit $\eta_1\alpha + \eta_2 = \psi_1$, $\varphi_1\alpha + \varphi_2 = \psi_2$ und $\xi_1\alpha + \xi_2 = \psi_3$. Wir betrachten den Ringhomomorphismus

$$F : R(G)'_p \to (\mathbb{Z}/p^2\mathbb{Z})^3, \quad \vartheta \mapsto (\vartheta(1), \vartheta(x), \vartheta(y)) \pmod{p^2}.$$

Dann existieren $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathbb{Z}/p^2\mathbb{Z}$, sodass $F(\eta_i) = (a_i, a_i, a_i)$, $F(\varphi_i) = (b_i, b_i, b_i)$ und $F(\xi_i) = (c_i, c_i, c_i)$ für $i = 1, 2$ ist. Sei $F(\alpha) = (x, y, z)$ mit $x, y, z \in \mathbb{Z}/p^2\mathbb{Z}$. Dann haben wir also die Gleichungen

$$(a_1x + a_2, a_1y + a_2, a_1z + a_2) \equiv (p, 0, 0) \pmod{p^2}, \tag{4.4}$$
$$(b_1x + b_2, b_1y + b_2, b_1z + b_2) \equiv (0, p, 0) \pmod{p^2}, \tag{4.5}$$
$$(c_1x + c_2, c_1y + c_2, c_1z + c_2) \equiv (0, 0, p) \pmod{p^2}. \tag{4.6}$$

Aus (4.4) folgt $a_1y+a_2 \equiv a_1z+a_2$, d. h. $a_1(y-z) \equiv 0 \pmod{p^2}$. Nun kann $y-z$ nicht durch p^2 teilbar sein, weil sonst b_2 nach (4.5) sowohl zu 0 als auch zu $p \pmod{p^2}$ kongruent sein müsste. Also gilt $a_1 = p\tilde{a}_1$ und damit auch $a_2 = p\tilde{a}_2$ mit $\tilde{a}_1, \tilde{a}_2 \in \mathbb{Z}/p^2\mathbb{Z}$.

Auf dieselbe Weise kann man die Kongruenzen (4.5) und (4.6) auswerten und erhält $b_1 = p\tilde{b}_1$, $b_2 = p\tilde{b}_2$, $c_1 = p\tilde{c}_1$ und $c_2 = p\tilde{c}_2$ mit $\tilde{b}_1, \tilde{b}_2, \tilde{c}_1, \tilde{c}_2 \in \mathbb{Z}/p^2\mathbb{Z}$. Das bedeutet aber, dass die folgenden Kongruenzen erfüllt sein müssen:

$$(\tilde{a}_1x + \tilde{a}_2, \tilde{a}_1y + \tilde{a}_2, \tilde{a}_1z + \tilde{a}_2) \equiv (1, 0, 0) \pmod{p},$$
$$(\tilde{b}_1x + \tilde{b}_2, \tilde{b}_1y + \tilde{b}_2, \tilde{b}_1z + \tilde{b}_2) \equiv (0, 1, 0) \pmod{p},$$
$$(\tilde{c}_1x + \tilde{c}_2, \tilde{c}_1y + \tilde{c}_2, \tilde{c}_1z + \tilde{c}_2) \equiv (0, 0, 1) \pmod{p}.$$

Diese können jedoch nicht gleichzeitig erfüllt sein, weil (x, y, z) und $(1, 1, 1)$ sonst den $\mathbb{Z}/p\mathbb{Z}$-Vektorraum $(\mathbb{Z}/p\mathbb{Z})^3$ erzeugen würden. □

Die Voraussetzung $|P| \geq p^3$ in der obigen Proposition ist tatsächlich notwendig. Man kann sich leicht davon überzeugen, dass der Charakterring von $G = C_3^2 \rtimes C_4$ endlichen Darstellungstyp hat (C_4 möge auf C_3^2 wie eine Untergruppe von $\Gamma\mathrm{L}_0(3^2)$ auf $\mathbb{F}_3^2$ operieren). Ein weiteres Beispiel dieser Art erhält man durch die zu $C_7^2 \rtimes \mathrm{SL}(2, 3)$ isomorphe Untergruppe der scharf 2-transitiven Permutationsgruppe vom Grad 49, die nicht zu $C_7^2 \rtimes \Gamma\mathrm{L}(7^2)$ isomorph ist.

Als nächstes wollen wir ein zu Lemma 4.8 analoges Lemma beweisen. Wir beschränken uns daher auf solche Gruppen G, in denen $N_G(P)/C_G(P)$ wie eine Untergruppe von $\Gamma\mathrm{L}_0(P)$ auf einer elementar-abelschen p-Sylowgruppe von G operiert. Hat P die Ordnung p^k, so lässt sich schnell einsehen, dass k dann gerade sein muss, wenn es in G genau zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung p gibt.

Lemma 4.14. *Seien $k \geq 2$ gerade, P die additive Gruppe von $\mathbb{F}_{p^k}$ und C eine Untergruppe der multiplikativen Gruppe von $\mathbb{F}_{p^k}^\times$. Weiter gebe es in*

$$G := \left\{ \begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix} : a \in C,\, x \in P \right\},$$

genau zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung p. Sei $u \in G$ ein Element der Ordnung p und $\mathfrak{p}$ das p enthaltende maximale Ideal von $\mathcal{O}_{\mathbb{Q}(\mathrm{cl}_G(u))}$. Ist u nicht zu u^{-1} konjugiert, so gilt $\chi(1) \equiv \chi(u) \pmod{\mathfrak{p}^k}$ für jedes $\chi \in \mathrm{Irr}(G)$. Sind u und u^{-1} dagegen in G konjugiert, so gilt $\chi(1) \equiv \chi(u) \pmod{\mathfrak{p}^{k/2}}$ für jedes $\chi \in \mathrm{Irr}(G)$.

Beweis. Wir betrachten zunächst den Fall, dass u und u^{-1} nicht in G konjugiert sind und setzen wieder

$$V := \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in P \right\} \cong P \quad \text{und} \quad H := \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in C \right\} \cong C\,,$$

womit $G = V \rtimes H$ gilt. Analog zum Beweis von Lemma 4.8 erhalten wir $|C| = \frac{1}{2} \cdot \frac{p^k-1}{p-1} \cdot t$ mit $\mathrm{ggT}(n, p-1) \mid t \leq p-1$. Der Faktor $\frac{1}{2}$ rührt daher, dass es in G nicht eine, sondern zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung p gibt.

Da die Elemente der Ordnung p in G nicht zu ihren Inversen konjugiert sind, enthält H keine Matrix, deren Eintrag links oben -1 ist. Folglich hat H ungerade Ordnung. Für $p \equiv 3 \pmod 4$ ist aber $\frac{p^k-1}{2(p-1)}$ gerade, also muss $p \equiv 1 \pmod 4$ gelten.

Wie in Lemma 4.8 ist G auch hier eine Frobeniusgruppe mit Kern V und Komplement H. Die Konjugationsklassen von G haben folgende Repräsentanten:

1. 1_G,
2. $P_1, \ldots, P_{\frac{(p-1)}{t}}$, wobei jedes P_i die Gestalt $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ mit einem $x \in \mathbb{F}_p$ hat,
3. $P_{\frac{p-1}{t}+1}, \ldots, P_{\frac{2(p-1)}{t}}$, wobei jedes P_i die Gestalt $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ mit einem $x \notin \mathbb{F}_p$ hat,
4. $C_1, \ldots, C_{\frac{p^k-1}{2(p-1)} \cdot t}$, wobei jedes C_j die Gestalt $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ mit $a \in C$ hat.

Die linearen Charaktere von G sind wieder Erweiterungen der linearen Charaktere von H. Zu einem linearen Charakter $\chi \in \mathrm{Irr}(G)$ existiert also ein linearer Charakter $\lambda \in \mathrm{Irr}(H)$, sodass $\chi(g) = \lambda(h)$ ist, wenn $g = vh$ mit $v \in V$ und $h \in H$ gilt. Die Behauptung des Satzes ist für einen linearen Charakter $\chi \in \mathrm{Irr}(G)$ somit trivialerweise erfüllt.

Die weiteren irreduziblen Charaktere von G entstehen wieder durch Induktion der irreduziblen Charaktere von V. Jeder irreduzible Charakter von V hat die Gestalt $\tilde{\lambda}_x$, wobei $X := \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ ein Element der Menge $\{P_1, \ldots, P_{\frac{2(p-1)}{t}}\}$ ist und $\tilde{\lambda}_x(Y) = \zeta_p^{\mathrm{Tr}(xy)}$ für $Y \in V$ mit $Y = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$ gilt. Sicher gilt $\tilde{\lambda}_x^G(1) = \frac{p^k-1}{2(p-1)} \cdot t$ und $\tilde{\lambda}_x^G(g) = 0$, wenn $g \notin V$ ist. Für $Y \in \{P_1, \ldots, P_{\frac{2(p-1)}{t}}\}$ mit Eintrag y oben rechts erhalten wir ferner

$$\tilde{\lambda}_x^G(Y) = \frac{1}{|V|} \sum_{g \in G} \tilde{\lambda}_x^\circ(gYg^{-1}) = \sum_{g \in H} \tilde{\lambda}_x(gYg^{-1}) = \sum_{a \in C} \lambda_x(ay) = \sum_{a \in C} \zeta_p^{\mathrm{Tr}(xay)}\,.$$

Wir fassen $(1-\zeta_p)$ wieder als maximales Ideal von $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ auf. Dann müssen wir

$$\frac{p^k-1}{2(p-1)} \cdot t \equiv \sum_{a \in C} \zeta_p^{\mathrm{Tr}(axy)} \pmod{(1-\zeta_p)^{tk}}$$

zeigen.

Für $i = 1, \ldots, \frac{p-1}{t}$ liegen die P_i alle in derselben zyklischen Gruppe. Daher lassen sich die Werte $\tilde{\lambda}_x^G(P_1), \ldots, \tilde{\lambda}_x^G(P_{\frac{p-1}{t}})$ durch Galois-Automorphismen von $\mathbb{Q}(\mathrm{cl}_G(P_1))/\mathbb{Q}$ ineinander überführen und wir müssen für diese P_i nur $\frac{p^k-1}{2(p-1)} \cdot t \equiv s_x \pmod{(1-\zeta_p)^{kt}}$ mit $s_x = \sum_{a \in C} \zeta_p^{\mathrm{Tr}(ax)}$ zeigen. Analog kann man $P_{\frac{p-1}{t}+1}, \ldots, P_{\frac{2(p-1)}{t}}$ so wählen, dass für $i = \frac{p-1}{t} + 1, \ldots, \frac{2(p-1)}{t}$ die P_i in einer zyklischen Gruppe liegen. Ist z der Eintrag rechts oben von $P_{\frac{2(p-1)}{t}}$, so genügt es für diese P_i also, $\frac{p^k-1}{2(p-1)} \cdot t \equiv s_{xz} \pmod{(1-\zeta_p)^{kt}}$ mit $s_{xz} = \sum_{a \in C} \zeta_p^{\mathrm{Tr}(axz)}$ zu beweisen.

Sei $M \subseteq \mathbb{F}_{p^k}^\times$ ein Repräsentantensystem für die Nebenklassen $\mathbb{F}_{p^k}^\times / C$. Wir können M also sowohl als Teilmenge von $\mathbb{F}_{p^k}^\times$ als auch als Gruppe auffassen. Für $m \in M$ setzen wir dann

$$s(m) := \sum_{a \in m^{-1}C} \zeta_p^{\mathrm{Tr}(a)} = \sum_{a \in C} \zeta_p^{\mathrm{Tr}(ma)} .$$

Weiter sei $N \leq \mathrm{Irr}(\mathbb{F}_{p^k}^\times)$ die Untergruppe der irreduziblen Charaktere von $\mathbb{F}_{p^k}^\times$, die auf C trivial sind, also $|N| = \frac{2(p-1)}{t}$. Für $\psi \in N$ haben wir die Gaußsche Summe

$$\Gamma(\psi) := \sum_{\alpha \in \mathbb{F}_{p^k}^\times} \psi(\alpha) \zeta_p^{\mathrm{Tr}(\alpha)} = \sum_{m \in M} \sum_{a \in C} \psi(ma) \zeta_p^{\mathrm{Tr}(ma)} = \sum_{m \in M} \psi(m) s(m) .$$

Da N aus genau den Charakteren von $\mathbb{F}_{p^k}^\times$ besteht, die kanonisch zu den irreduziblen Charakteren von $\mathbb{F}_{p^k}^\times / C$ korrespondieren, lässt sich N als Menge der irreduziblen Charaktere von M ansehen. Mit dieser Sichtweise ist die durch $\widetilde{\Gamma}(\psi) := \Gamma(\bar{\psi})$ definierte Funktion $\widetilde{\Gamma}$ die Fourier-Transformierte von s und somit erhalten wir

$$s_x = s(x) = \frac{t}{2(p-1)} \sum_{\psi \in N} \overline{\psi(x)} \Gamma(\psi) \quad \text{sowie} \quad s_{xz} = s(xz) = \frac{t}{2(p-1)} \sum_{\psi \in N} \overline{\psi(xz)} \Gamma(\psi) .$$

Da wir nur die Charaktere ψ betrachten, die auf C trivial sind, folgt $\psi(\alpha) = \alpha^{-\ell}$ für $\alpha \in \mathbb{F}_{p^k}^\times$ und ein $\ell \in \left\{ \frac{p^k-1}{2(p-1)} \cdot t \cdot r : r \in \left\{0, 1, \ldots, \frac{2(p-1)}{t} - 1\right\} \right\}$. Für den trivialen Charakter gilt natürlich

$$\overline{\mathbb{1}(x)} \Gamma(\mathbb{1}) = \overline{\mathbb{1}(xz)} \Gamma(\mathbb{1}) = \sum_{a \in \mathbb{F}_{p^k}^\times} \zeta_p^{\mathrm{Tr}(a)} = -1 + \sum_{a \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}(a)} = -1 .$$

Ist $\psi \in N$ ein nichttrivialer Charakter, so erhalten wir

$$\Gamma(\psi) = \Gamma_\ell = \sum_{\alpha \in \mu_{p^k-1}} \alpha^{-\ell} \zeta_p^{\mathrm{Tr}(\alpha)}$$

für ein $\ell \in \left\{ \frac{p^k-1}{2(p-1)} \cdot t \cdot r : r \in \left\{1, 2, \ldots, \frac{2(p-1)}{t} - 1\right\} \right\}$.

Ist r gerade, so hat ℓ die Darstellung $\ell = \frac{p^k-1}{p-1} \cdot t \cdot b = tb(1 + \ldots + p^{k-1})$ für ein $b \in \left\{1, 2, \ldots, \frac{p-1}{t} - 1\right\}$. Für jedes dieser b ist $tb < p$, also lassen sich die Koeffizienten

der p-adischen Darstellung von ℓ aus dieser Zerlegung direkt ablesen. Die Summe der Koeffizienten ist folglich ktb und wird für $b = 1$ minimal.

Ist r ungerade, so gilt $\ell = \frac{p^k-1}{2(p-1)} \cdot t \cdot (2b+1)$ für ein $b \in \left\{0, 1, \ldots, \frac{p-1}{t} - 1\right\}$. Weil zudem t ungerade ist, d. h. $t = 2w + 1$ für eine ganze Zahl $w \geq 0$, liefert uns das

$$\begin{aligned}
\ell &= \frac{p^k-1}{2(p-1)} \cdot (2w+1) \cdot (2b+1) = (2w+1)(2b+1) \cdot \frac{1 + \ldots + p^{k-1}}{2} \\
&= (4bw + 2(b+w) + 1) \cdot \frac{p+1}{2} \cdot \left(1 + p^2 + \ldots + p^{k-2}\right) \\
&= \left((2bw + b + w)(p+1) + \frac{p+1}{2}\right) \cdot \left(1 + p^2 + \ldots + p^{k-2}\right) \\
&= \left(2bw + b + w + \frac{p+1}{2} + (2bw + b + w)p\right) \cdot \left(1 + p^2 + \ldots + p^{k-2}\right).
\end{aligned}$$

Wegen $(2w+1)(2b+1) = tr \leq 2(p-1) - t < 2(p-1)$ folgt

$$\begin{aligned}
2bw + b + w &= \frac{4bw + 2(b+w)}{2} \\
&< \frac{4bw + 2(b+w) + 1}{2} = \frac{(2w+1)(2b+1)}{2} = \frac{tr}{2} < p - 1\,,
\end{aligned}$$

weswegen $2bw + b + w + \frac{p+1}{2} < 2p$ ist. Entweder ist also $2bw + b + w + \frac{p+1}{2} < p$ und die Koeffizienten in der p-adischen Darstellung von ℓ lassen sich aus der obigen Zerlegung von ℓ direkt ablesen. Oder es gilt $2bw + b + w + \frac{p+1}{2} > p$, womit

$$\ell = (c + (2bw + b + w + 1)p) \cdot \left(1 + p^2 + \ldots + p^{k-2}\right)$$

für ein $c < p$ ist. Dann lassen sich die Koeffizienten der p-adischen Darstellung von ℓ aus dieser Gleichung ablesen. Im ersten Fall sind die Koeffizienten vor den ungeraden Potenzen von p größer oder gleich $\frac{p+1}{2}$, im zweiten Fall trifft dies auf die Koeffizienten der geraden Potenzen von p zu. Die Summe der Koeffizienten ist also in beiden Fällen mindestens $\frac{k}{2} \cdot \frac{p+1}{2} = \frac{k(p+1)}{4}$.

Da $p \equiv 1 \pmod 4$ gilt und t ein ungerader Teiler von $p-1$ ist, teilt t auch $\frac{p-1}{4}$. Das impliziert $\frac{k(p+1)}{4} > kt$. Nach Satz 1.20 ist demnach $\Gamma_\ell \equiv 0 \pmod{(1-\zeta_p)^{kt+1}}$ für $\ell \in \left\{\frac{p^k-1}{p-1} \cdot t \cdot r : r \in \{1, 3, 4, \ldots, \frac{2(p-1)}{t} - 1\}\right\}$ und weiterhin haben wir für $r = 2$ die Kongruenz $\Gamma_\ell \equiv -\frac{(1-\zeta_p)^{kt}}{(t!)^k} \pmod{(1-\zeta_p)^{kt+1}}$ in $\mathcal{O}_{\mathbb{Q}_p(\zeta_p)}$. Das führt zu

$$\begin{aligned}
s_x - \frac{p^k-1}{2(p-1)} \cdot t &= \frac{t}{2(p-1)} \sum_{\psi \in N} \overline{\psi(x)}\Gamma(\psi) - \frac{p^k-1}{2(p-1)} \cdot t \\
&\equiv \frac{t}{2(p-1)} \left(-1 - \zeta_{2(p-1)/t}^d \cdot \frac{(1-\zeta_p)^{kt}}{(t!)^k} - p^k + 1\right) \\
&\equiv -\frac{t}{2(p-1)} \cdot \left(\zeta_{2(p-1)/t}^d \cdot \frac{(1-\zeta_p)^{tk}}{(t!)^k} + p^k\right) \pmod{(1-\zeta_p)^{kt+1}}
\end{aligned}$$

für ein $d \in \mathbb{Z}$, sodass $\overline{\psi(x)} = \zeta_{2(p-1)/2}^d$ gilt. Völlig analog erhält man

$$s_{xz} - \frac{p^k-1}{2(p-1)} \cdot t \equiv -\frac{t}{2(p-1)} \cdot \left(\zeta_{2(p-1)/t}^d \cdot \frac{(1-\zeta_p)^{tk}}{(t!)^k} + p^k \right) \pmod{(1-\zeta_p)^{kt+1}},$$

wenn $d \in \mathbb{Z}$ so gewählt wird, dass $\overline{\psi(xz)} = \zeta_{2(p-1)/2}^d$ gilt. Folglich sind sowohl

$$s_x - \frac{p^k-1}{2(p-1)} \cdot t \qquad \text{als auch} \qquad s_{xz} - \frac{p^k-1}{2(p-1)} \cdot t$$

durch $(1-\zeta_p)^{tk}$ teilbar und die erste Aussage des Lemmas ist bewiesen.

Im Fall, dass u und u^{-1} in G konjugiert sind, geht man völlig analog vor. Der einzige Unterschied ist, dass t in diesem Fall gerade ist, d. h. $t = 2w$ für ein $w \in \mathbb{N}$. Mit denselben Bezeichnungen wie oben gelangt man schließlich zu

$$\Gamma(\psi) = \Gamma_\ell = \sum_{\alpha \in \mu_{p^k-1}} \alpha^{-\ell} \zeta_p^{\mathrm{Tr}(\alpha)}$$

für ein $\ell \in \left\{ \frac{p^k-1}{2(p-1)} \cdot t \cdot r : r \in \left\{1, 2, \ldots, \frac{2(p-1)}{t} - 1\right\} \right\}$.

Wegen $t = 2w$ folgt also $\ell = wr(1 + \ldots + p^{k-1})$ für ein $r \in \left\{1, 2, \ldots, \frac{p-1}{w} - 1\right\}$. Damit lässt sich $\Gamma_\ell \equiv 0 \pmod{(1-\zeta_p)^{1+kt/2}}$ für $\ell \in \left\{ \frac{p^k-1}{p-1} \cdot t \cdot r : r \in \{2, 3, \ldots, \frac{2(p-1)}{t} - 1\} \right\}$ sowie $\Gamma_\ell \equiv -\frac{(1-\zeta_p)^{kt/2}}{(w!)^k} \pmod{(1-\zeta_p)^{1+kt/2}}$ für $r = 1$ schließen. Der restliche Beweis verläuft wieder analog zu dem des ersten Falls. □

Proposition 4.15. *Sei $P \in \mathrm{Syl}_p(G)$ elementar-abelsch mit Ordnung $p^k \geq p^2$, G beinhalte genau zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung p und $G/C_G(P)$ operiere auf P wie eine Untergruppe von $\Gamma\mathrm{L}(p^k)$ auf $\mathbb{F}_p^k$.*

(i) Ist $k > 2$, so ist der Darstellungstyp von $R(G)$ unendlich.

(ii) Ist $k = 2$ und $|G/C_G(P)|$ ungerade, so hat $R(G)$ unendlichen Darstellungstyp.

Beweis. Der Beweis erfolgt unter Verwendung von Lemma 4.14 analog zum Beweis von Satz 4.9. Es sei lediglich bemerkt, dass $\mathrm{rad}(R(G)'_p/R(G)_p)$ hier auch für $k = 2$ und $|G/C_G(P)|$ ungerade nicht zyklisch sein kann. Seien x, y Repräsentanten der beiden $\mathbb{Q}$-Klassen von G, die Elemente der Ordnung p enthalten. Das maximale Ideal $\mathfrak{P}$ von $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathrm{cl}_G(x))}$ stimmt mit dem von $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{\mathbb{Q}(\mathrm{cl}_G(y))}$ überein. Nach Lemma 4.14 kann es keine Funktion $\alpha \in \mathrm{rad}(R(G)'_p)$ geben, zu der $\eta_1, \eta_2, \varphi_1, \varphi_2 \in R(G)_p$ existieren, sodass $\eta_1(x)\alpha(x) + \eta_2(x) \in \mathfrak{P} \setminus \mathfrak{P}^2$, $\eta_1(y)\alpha(y) + \eta_2(y) = 0$, $\varphi_1(x)\alpha(x) + \varphi_2(x) = 0$ und $\varphi_1(y)\alpha(y) + \varphi_2(y) \in \mathfrak{P} \setminus \mathfrak{P}^2$ gilt. Folglich ist der $R(G)_p$-Modul $\mathrm{rad}(R(G)'_p/R(G)_p)$ nicht zyklisch. □

Die Voraussetzung in Proposition 4.15, dass $|G/C_G(P)|$ für $k = 2$ ungerade ist, kann man nicht weglassen. In diesem Fall gibt es nämlich Gruppen, deren Charakterring endlichen Darstellungstyp hat.

Beispiel 4.16. Seien $P \cong C_5^2$, $C \cong C_6$ und $G = P \rtimes C$, wobei C auf P wie eine Untergruppe von $\Gamma\mathrm{L}_0(5^2)$ auf $\mathbb{F}_5^2$ operiert. Für ein Element x der Ordnung 5 von G lässt sich schnell einsehen, dass $\frac{1+\sqrt{5}}{2}$ in $\mathbb{Z}[\chi(x) : \chi \in \mathrm{Irr}(G)]$ liegt und dieser Ring demzufolge mit $\mathcal{O}_{\mathbb{Q}(\mathrm{cl}_G(x))} = \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ übereinstimmt. Da G genau zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung 5 besitzt, erzeugen α_1, α_2 mit $\alpha_1(1) = 1$, $\alpha_1(g) = 0$ für $1 \neq g \in G$ und $\alpha_2(x) = 1$, $\alpha_2(g) = 0$ für $g \in G \setminus \mathrm{cl}_G(x)$ den $R(G)_5$-Modul $R(G)_5'/R(G)_5$. Des Weiteren gibt es ein $y \in G \setminus \mathrm{cl}_G(x)$ der Ordnung 5, für das die Funktion φ mit $\varphi(x) = 2\sqrt{5}$, $\varphi(y) = \sqrt{5}$ und $\varphi(g) = 0$ für $g \in G \setminus P$ in $R(G)$ liegt. Da $\mathrm{rad}\big(\mathbb{Z}_{(5)} \otimes \mathcal{O}_{\mathbb{Q}(\sqrt{5})}\big) = (\sqrt{5})$ ist, erzeugt die Funktion β mit $\beta(x) = \sqrt{5}$ und $\beta(g) = 0$ für $g \in G \setminus \mathrm{cl}_G(x)$ den $R(G)_5$-Modul $\mathrm{rad}(R(G)_5'/R(G)_5)$. Außerdem sind die 2- und 3-Sylowgruppen von G zyklisch der Ordnung 2 bzw. 3, also hat $R(G)$ endlichen Darstellungstyp.

Sei jetzt $P \in \mathrm{Syl}_p(G)$ eine elementar-abelsche Gruppe der Ordnung $p^k \geq p^2$, $N_G(P)/C_G(P)$ operiere nicht auf P wie eine Untergruppe von $\Gamma\mathrm{L}(p^k)$ auf $\mathbb{F}_p^k$ und G besitze genau zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung p. Dann sieht die Lage wieder etwas anders als zuvor aus. Möglicherweise muss in diesem Fall $k = 2$ gelten und in beiden $\mathbb{Q}$-Klassen von Elementen der Ordnung p in G müssen alle Elemente konjugiert sein, damit der Darstellungstyp von $R(G)_p$ endlich ist. Das ist jedoch lediglich eine Vermutung.

Als Beispiel für diesen Fall schauen wir uns die Gruppe $G = C_{11}^2 \rtimes Q_{12}$ an (Q_{12} sei die nichtabelsche Gruppe der Ordnung 12 mit normaler 3-Sylowgruppe und das semidirekte Produkt sei so, dass G genau zwei Konjugationsklassen zyklischer Untergruppen der Ordnung 11 besitzt). Dann gilt für jedes $x \in G$ der Ordnung 11 und jeden Charakter $\chi \in \mathrm{Irr}(G)$ die Kongruenz $\chi(1) \equiv \chi(x) \pmod{\mathfrak{p}^2}$, wobei $\mathfrak{p}$ das maximale Ideal in $\mathcal{O}_{\mathbb{Q}(\mathrm{cl}_G(x))}$ ist. Der Darstellungstyp von $R(G)_{11}$, und damit auch der von $R(G)$, ist demzufolge unendlich. Wir merken an, dass die Elemente der Ordnung 11 in G jeweils zu ihren Inversen konjugiert sind.

Der Charakterring der Gruppe $G = C_{11}^2 \rtimes (C_5 \times Q_{12})$ (wobei C_5 nichttrivial und Q_{12} auf C_{11}^2 wie eben operiert) hat dagegen endlichen Darstellungstyp, wie man der Charaktertafel schnell entnehmen kann.

Ein weiteres Beispiel liefert die Gruppe $G = C_7^2 \rtimes \mathrm{SL}(2,3)$, die keine Untergruppe einer 2-transitiven Gruppe ist, aber trotzdem nur zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung 7 besitzt. Für ein Element $x \in G$ der Ordnung 7, das sich nicht in der rationalen Konjugationsklasse von Elementen der Ordnung 7 in G befindet, gilt stets $\chi(1) \equiv \chi(x) \pmod{\mathfrak{p}}$, wenn $\chi \in \mathrm{Irr}(G)$ und $\mathfrak{p}$ das maximale Ideal in $\mathcal{O}_{\mathbb{Q}(\mathrm{cl}_G(x))}$, in dem die 7 liegt, ist. Daher hat $R(G)_7$ unendlichen Darstellungstyp.

Es gibt eine Reihe weiterer Beispiele für Gruppen G mit einer elementar-abelschen p-Sylowgruppe P der Ordnung p^2 und genau zwei $\mathbb{Q}$-Klassen der Ordnung p, sodass nicht alle Elemente einer $\mathbb{Q}$-Klasse konjugiert sind. Die Operation von $N_G(P)/C_G(P)$ auf P verläuft dabei auf unterschiedliche Arten, der Darstellungstyp von $R(G)$ ist jedoch in allen von mir betrachteten Beispielen unendlich.

4.3 Zusammenfassung

In diesem Kapitel haben wir untersucht, welche Bedingungen eine Gruppe G mit einer abelschen p-Sylowgruppe P erfüllen muss, damit der Darstellungstyp von $R(G)_p$ endlich ist. Der Darstellungstyp von $R(G)$ kann aber nach Satz 3.12 auch dann endlich sein, wenn G gewisse nichtabelsche 2-Sylowgruppen besitzt. Auch hier kann man nach Bedingungen an G fragen, sodass $R(G)_2$ endlichen Darstellungstyp hat. Bezüglich der Operation von G auf einer 2-Sylowgruppe ist die Antwort darauf relativ leicht, weil die $\mathbb{Q}$-Klassen der 2-Elemente in G, außer wenn G zu C_4 isomorphe 2-Sylowgruppen hat, rationale Konjugationsklassen sein müssen. Die Beispiele im Anschluss an Satz 3.12 liefern daher minimale Gruppen G, sodass G eine 2-Sylowgruppe aus der Liste dieses Satzes und $R(G)$ endlichen Darstellungstyp hat.

Eine Gruppe H, die eine der Gruppen $\neq D_8$ aus Satz 3.12 als 2-Sylowgruppe hat, muss also eine dieser minimalen Gruppen enthalten, wenn der Darstellungstyp von $R(H)$ endlich ist. Hat H zu D_8 isomorphe 2-Sylowgruppen, so enthält H eine zu $\mathrm{PSL}(2,p)$ mit $p \equiv \pm 7 \pmod{16}$ isomorphe Untergruppe, wobei $p \pm 1$ durch keine dritte Potenz einer ungeraden Primzahl teilbar ist.

Die Frage, was auf den rationalen $2'$-Sektionen von H, die nicht 1_H enthalten, passiert, scheint wieder schwer zu beantworten zu sein. Der Charakterring der Gruppe $G = (C_2^2 \times C_7) \rtimes C_3$, wobei C_3 mit keinem Element der Ordnung 2 bzw. 7 kommutiert, hat beispielsweise unendlichen Darstellungstyp. Ist $\mathcal{S}$ die $\mathbb{Q}$-Klasse der Elemente der Ordnung 14 in G, so hat jedes Erzeugendensystem des $R(G)_2$-Moduls $(R(G)_2' \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}))/(R(G) \cap \mathrm{Ch}_{\mathbb{Q}}(\mathcal{S}))$ nämlich mindestens vier Erzeuger, wie man sich durch eine etwas längere Rechnung klarmachen kann. Interessanterweise ist der $R(G)_2$-Modul $\mathrm{rad}(R(G)_2'/R(G)_2)$ zyklisch. Der Grund dafür, dass $R(G)$ unendlichen Darstellungstyp hat, ist also ein anderer als der in Beispiel 4.12 dafür, dass $R((C_3^3 \times C_5) \rtimes C_{52})$ unendlichen Darstellungstyp hat. Für $G = (Q_8 \times C_7) \rtimes C_3$ erhält man übrigens ebenso, dass $R(G)$ unendlichen Darstellungstyp hat (C_3 operiere auf Q_8 und C_7 wieder nichttrivial). Die Vorgehensweise ist völlig analog zum obigen Beispiel mit $G = (C_2^2 \times C_7) \rtimes C_3$, hier ist die $\mathbb{Q}$-Klasse der Elemente der Ordnung 28 ausschlaggebend.

Es gibt eine Gemeinsamkeit zwischen den beiden Gruppen aus Beispiel 4.12 sowie den Gruppen $(C_2^2 \times C_7) \rtimes C_3$ und $(Q_8 \times C_7) \rtimes C_3$. Ist G eine dieser vier Gruppen, so gibt es ein $p \in \mathbb{P}$, sodass G eine nichtzyklische p-Sylowgruppe P besitzt, für die $C_G(N_G(P)) < C_G(P)$ gilt. Möglicherweise lässt sich das wie folgt verallgemeinern: Hat G eine nichtzyklische p-Sylowgruppe $P \neq D_8$ und gibt es eine Untergruppe $H \leq N_G(P)$, sodass $H/P \cong N_G(P)/C_G(P)$ und $C_G(H) < C_G(P)$ gilt, dann hat $R(G)$ unendlichen Darstellungstyp. Diese Vermutung stützt sich allerdings nur auf wenige Beispiele und wäre, sollte sie stimmen, wohl schwer zu beweisen, wie die obigen Beispiele nahelegen. Gruppen mit zu D_8 isomorphen 2-Sylowgruppen muss man natürlich extra betrachten, da D_8 nicht resistent ist.

Zusammen mit den Ergebnissen aus den vorigen Abschnitten und Kapiteln erhalten wir also Folgendes:

Satz 4.17. *Der Darstellungstyp von $R(G)$ ist genau dann endlich, wenn $\exp(G)$ von keiner dritten Potenz einer Primzahl geteilt wird und für jedes $p \in \mathbb{P}$, für das G eine nichtzyklische p-Sylowgruppe P besitzt, $R(G)_p$ endlichen Darstellungstyp hat. Gegebenenfalls tritt einer der folgenden Fälle ein:*

1. *$P \cong C_p^k$ für ein ungerades $k \geq 3$, wobei $p^k - 1$ von keiner dritten Potenz einer Primzahl geteilt wird, alle Elemente der Ordnung p sind in G konjugiert und $N_G(P)/C_G(P)$ enthält eine zyklische Gruppe der Ordnung $p^k - 1$.*
2. *$P \cong C_p^2$, in G liegen genau zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung p und*
   - *beide $\mathbb{Q}$-Klassen sind bereits Konjugationsklassen oder*
   - *die Elemente der Ordnung p sind zu ihren Inversen konjugiert, $p+1$ ist nicht durch 16 teilbar und $N_G(P)/C_G(P)$ enthält eine zyklische Untergruppe der Ordnung $\frac{p+1}{2}$.*
3. *$P \cong C_p^2$, $p \in \{2, 5, 11, 29, 59\}$, alle Elemente der Ordnung p in G sind konjugiert und $N_G(P)/C_G(P)$ enthält einen zu C_3 ($p = 2$), $\mathrm{SL}(2,3)$ ($p = 5$), $C_5 \times \mathrm{SL}(2,3)$ ($p = 11$), $\mathrm{SL}(2,5)$ ($p = 11$), $C_7 \times \mathrm{SL}(2,5)$ ($p = 29$) oder $C_{29} \times \mathrm{SL}(2,5)$ ($p = 59$) isomorphen Normalteiler.*
4. *P ist isomorph zu einer 2-Sylowgruppe von $\mathrm{PSU}(3, 2^n)$ für ein $n \in \mathbb{N}$, sodass $2^{2n} - 1$ von keiner dritten Potenz einer Primzahl geteilt wird, alle Elemente der Ordnung 2 bzw. 4 sind in G konjugiert und $N_G(P)/C_G(P)$ enthält eine zyklische Untergruppe der Ordnung $2^{2n} - 1$.*
5. *P ist isomorph zur Suzuki 2-Gruppe S aus Satz 3.12 mit $|S| = 2^9$, alle Elemente der Ordnung 2 bzw. 4 sind in G konjugiert und $N_G(P)/C_G(P)$ enthält eine metazyklische nichtabelsche Untergruppe der Ordnung 63.*
6. *$P \cong D_8$ und G enthält für ein $q \equiv \pm 7 \pmod{16}$ eine zu $\mathrm{PSL}(2,q)$ isomorphe Untergruppe, wobei $q \pm 1$ nicht von der dritten Potenz einer ungeraden Primzahl geteilt wird.*
7. *$P \cong C_p^k$ für ein $k \geq 2$, in G gibt es genau zwei $\mathbb{Q}$-Klassen von Elementen der Ordnung p, mindestens eine dieser beiden $\mathbb{Q}$-Klassen enthält mehr als eine Konjugationsklasse von G und $N_G(P)/C_G(P)$ operiert nicht auf P wie eine Untergruppe von $\Gamma\mathrm{L}(p^k)$ auf $\mathbb{F}_p^k$.*

Zu jedem der Punkte 1 bis 6 des obigen Satzes gibt es eine Gruppe G mit einer p-Sylowgruppe P, sodass alle Bedingungen dieses Punktes erfüllt sind und $R(G)$ endlichen Darstellungstyp hat. Meine Vermutung ist, dass das auf Punkt 7 nicht zutrifft, dass also der Charakterring jeder Gruppe G, die eine p-Sylowgruppe P besitzt, für die alle Bedingungen aus Punkt 7 erfüllt sind, unendlichen Darstellungstyp hat.

Anhang – Charaktertafeln

Die folgenden Charaktertafeln lassen sich alle mithilfe von GAP bestimmen, lediglich für $\mathrm{PSL}(2,q)$ und $\mathrm{SL}(2,q)$ verweisen wir auf [17] bzw [35]. Die Zahlen in der ersten Zeile einer Tafel geben die Ordnung eines Repräsentanten der entsprechenden Konjugationsklasse an, einzig bei $\mathrm{PSL}(2,q)$ und $\mathrm{SL}(2,q)$ sind einige Spalten durch Elemente indiziert.

Quasieinfache Gruppen

• $\mathrm{PSL}(2,q)$ mit $q \equiv 0 \pmod 2$

	1	2	A^j	B^k
χ_1	1	1	1	1
$\chi_{2,\ell}$	$q-1$	-1	0	$-\zeta_{q+1}^{k\ell} - \zeta_{q+1}^{-k\ell}$
χ_3	q	0	1	-1
$\chi_{4,m}$	$q+1$	1	$\zeta_{q-1}^{jm} + \zeta_{q-1}^{-jm}$	0

$|\langle A\rangle| = q-1, \quad |\langle B\rangle| = q+1,$
$j = 1,\dots,\frac{q-2}{2}, \quad k = 1,\dots,\frac{q}{2},$
$\ell = 1,\dots,\frac{q}{2}, \quad m = 1,\dots,\frac{q-2}{2}$

• $\mathrm{PSL}(2,q)$ mit $q \equiv 1 \pmod 4$

	1	$p_\pm$	2	A^j	B^k
χ_1	1	1	1	1	1
$\chi_{2,+}$	$\frac{q+1}{2}$	$\frac{1\pm\sqrt{q}}{2}$	$(-1)^{(q-1)/4}$	$(-1)^j$	0
$\chi_{2,-}$	$\frac{q+1}{2}$	$\frac{1\mp\sqrt{q}}{2}$	$(-1)^{(q-1)/4}$	$(-1)^j$	0
$\chi_{3,\ell}$	$q-1$	-1	0	0	$-\zeta_{(q+1)/2}^{k\ell} - \zeta_{(q+1)/2}^{-k\ell}$
χ_4	q	0	1	1	-1
$\chi_{5,m}$	$q+1$	1	$2\cdot(-1)^m$	$\zeta_{(q-1)/2}^{jm} + \zeta_{(q-1)/2}^{-jm}$	0

$|\langle A\rangle| = \frac{q-1}{2}, \quad |\langle B\rangle| = \frac{q+1}{2},$
$j = 1,\dots,\frac{q-5}{4}, \quad k = 1,\dots,\frac{q-1}{4}, \quad \ell = 1,\dots,\frac{q-1}{4}, \quad m = 1,\dots,\frac{q-5}{4}$

• $\mathrm{PSL}(2,q)$ mit $q \equiv 3 \pmod 4$

	1	$p_\pm$	2	A^j	B^k
χ_1	1	1	1	1	1
$\chi_{2,+}$	$\frac{q-1}{2}$	$\frac{-1\pm\sqrt{-q}}{2}$	$(-1)^{(q-3)/4}$	0	$(-1)^{k+1}$
$\chi_{2,-}$	$\frac{q-1}{2}$	$\frac{-1\mp\sqrt{-q}}{2}$	$(-1)^{(q-3)/4}$	0	$(-1)^{k+1}$
$\chi_{3,\ell}$	$q-1$	-1	$2\cdot(-1)^{\ell+1}$	0	$-\zeta_{(q+1)/2}^{k\ell} - \zeta_{(q+1)/2}^{-k\ell}$
χ_4	q	0	-1	1	-1
$\chi_{5,m}$	$q+1$	1	0	$\zeta_{(q-1)/2}^{jm} + \zeta_{(q-1)/2}^{-jm}$	0

$|\langle A\rangle| = \frac{q-1}{2}, \quad |\langle B\rangle| = \frac{q+1}{2},$
$j = 1,\dots,\frac{q-3}{4}, \quad k = 1,\dots,\frac{q-3}{4}, \quad \ell = 1,\dots,\frac{q-3}{4}, \quad m = 1,\dots,\frac{q-3}{4}$

• $\mathrm{SL}(2,q)$

	1	2	$p_\pm$	$2p_\pm$	A^j	B^k
χ_1	1	1	1	1	1	1
$\chi_{2,+}$	$\frac{q-\varepsilon}{2}$	$-\frac{(q-\varepsilon)}{2}$	$\frac{-\varepsilon\pm\sqrt{\varepsilon q}}{2}$	$\frac{\varepsilon\mp\sqrt{\varepsilon q}}{2}$	$\frac{(1-\varepsilon)(-1)^j}{2}$	$\frac{(1+\varepsilon)(-1)^{k+1}}{2}$
$\chi_{2,-}$	$\frac{q-\varepsilon}{2}$	$-\frac{(q-\varepsilon)}{2}$	$\frac{-\varepsilon\mp\sqrt{\varepsilon q}}{2}$	$\frac{\varepsilon\pm\sqrt{\varepsilon q}}{2}$	$\frac{(1-\varepsilon)(-1)^j}{2}$	$\frac{(1+\varepsilon)(-1)^{k+1}}{2}$
$\chi_{3,+}$	$\frac{q+\varepsilon}{2}$	$\frac{(q+\varepsilon)}{2}$	$\frac{\varepsilon\pm\sqrt{\varepsilon q}}{2}$	$\frac{\varepsilon\pm\sqrt{\varepsilon q}}{2}$	$\frac{(1+\varepsilon)(-1)^j}{2}$	$\frac{(1-\varepsilon)(-1)^{k+1}}{2}$
$\chi_{3,-}$	$\frac{q+\varepsilon}{2}$	$\frac{(q+\varepsilon)}{2}$	$\frac{\varepsilon\mp\sqrt{\varepsilon q}}{2}$	$\frac{\varepsilon\mp\sqrt{\varepsilon q}}{2}$	$\frac{(1+\varepsilon)(-1)^j}{2}$	$\frac{(1-\varepsilon)(-1)^{k+1}}{2}$
$\chi_{4,\ell}$	$q-1$	$(-1)^\ell(q-1)$	-1	$(-1)^{\ell+1}$	0	$-\zeta_{q+1}^{k\ell}-\zeta_{q+1}^{-k\ell}$
χ_5	q	q	0	0	1	-1
$\chi_{6,m}$	$q+1$	$(-1)^m(q+1)$	1	$(-1)^m$	$\zeta_{q-1}^{jm}+\zeta_{q-1}^{-jm}$	0

$|\langle A\rangle| = q-1, \quad |\langle B\rangle| = q+1, \quad \varepsilon = (-1)^{(q-1)/2}$
$j = 1,\dots,\frac{q-3}{2}, \quad k = 1,\dots,\frac{q-1}{2}, \quad \ell = 1,\dots,\frac{q-1}{2}, \quad m = 1,\dots,\frac{q-3}{2}$

• $\mathrm{PSU}(3,4)$

	1	2	4	3	13_k
χ_1	1	1	1	1	1
χ_2	12	-4	0	4	-1
$\chi_{3,\ell}$	13	-3	1	1	0
$\chi_{4,+}$	39	7	-1	0	0
$\chi_{4,-}$	39	7	-1	0	0
$\chi_{5,\ell}$	52	4	0	1	0
χ_6	64	0	0	1	-1
$\chi_{7,m}$	65	1	1	-1	0
$\chi_{8,n}$	75	-5	-1	0	$-\zeta_{13}^{2\cdot 2^{k+n}}-\zeta_{13}^{5\cdot 2^{k+n}}-\zeta_{13}^{6\cdot 2^{k+n}}$

	$5_{1,j}$	$5_{2,\pm}$	10_j	15_j
χ_1	1	1	1	1
χ_2	-3	2	1	0
$\chi_{3,\ell}$	$-3\zeta_5^{j\ell}+\zeta_5^{3j\ell}$	$\sigma_\ell\left(\frac{1\pm\sqrt{5}}{2}\right)$	$\zeta_5^{3j\ell}+\zeta_5^{4j\ell}$	$\zeta_5^{3j\ell}$
$\chi_{4,+}$	$-3\zeta_5^{j}-3\zeta_5^{4j}$	$\frac{3\mp\sqrt{5}}{2}$	$\zeta_5^{2j}+\zeta_5^{3j}$	0
$\chi_{4,-}$	$-3\zeta_5^{2j}-3\zeta_5^{3j}$	$\frac{3\pm\sqrt{5}}{2}$	$\zeta_5^{j}+\zeta_5^{4j}$	0
$\chi_{5,\ell}$	$3\zeta_5^{3j\ell}+4\zeta_5^{4j\ell}$	$\sigma_\ell\left(\frac{-1\pm\sqrt{5}}{2}\right)$	$-\zeta_5^{4j\ell}$	$\zeta_5^{4j\ell}$
χ_6	4	-1	0	1
$\chi_{7,m}$	$5\zeta_5^{4jm}$	0	ζ_5^{2jm}	$-\zeta_5^{4jm}$
$\chi_{8,n}$	0	0	0	0

$j = 1,\dots,4, \quad k = 1,\dots,4, \quad \ell = 1,\dots,4, \quad m = 0,\dots,4, \quad n = 1,\dots,4,$
$\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$, $\sigma_\ell(\zeta_5) = \zeta_5^\ell$

• A_7

	1	2	3_1	3_2	4	5	6	$7_\pm$
χ_1	1	1	1	1	1	1	1	1
χ_2	6	2	0	3	0	1	-1	-1
$\chi_{3,+}$	10	-2	1	1	0	0	1	$\frac{-1\pm\sqrt{-7}}{2}$
$\chi_{3,-}$	10	-2	1	1	0	0	1	$\frac{-1\mp\sqrt{-7}}{2}$
χ_4	14	2	2	-1	0	-1	2	0
χ_5	14	2	-1	2	0	-1	-1	0
χ_6	15	-1	3	0	-1	0	-1	1
χ_7	21	1	-3	0	-1	1	1	0
χ_8	35	-1	-1	-1	1	0	-1	0

Untergruppen 2-transitiver Gruppen

• $C_3^2 \rtimes C_4$

	1	2	$4_\pm$	3_1	3_2
$\chi_{1,k}$	1	$(-1)^k$	$(\pm i)^k$	1	1
$\chi_{2,1}$	4	0	0	1	-2
$\chi_{2,2}$	4	0	0	-2	1

$k = 1, \ldots, 4$

• $C_5^2 \rtimes C_6$

	1	2	3_j	6_j	$5_{1,\pm}$	$5_{2,\pm}$
$\chi_{1,k}$	1	$(-1)^k$	ζ_3^{jk}	$(-\zeta_3^j)^k$	1	1
$\chi_{2,+}$	6	0	0	0	$1 \pm \sqrt{5}$	$\frac{-3\pm\sqrt{5}}{2}$
$\chi_{2,-}$	6	0	0	0	$1 \mp \sqrt{5}$	$\frac{-3\mp\sqrt{5}}{2}$
$\chi_{3,+}$	6	0	0	0	$\frac{-3\pm\sqrt{5}}{2}$	$1 \mp \sqrt{5}$
$\chi_{3,-}$	6	0	0	0	$\frac{-3\mp\sqrt{5}}{2}$	$1 \pm \sqrt{5}$

$j = 1, 2, \quad k = 1, \ldots, 6$

• $C_7^2 \rtimes \mathrm{SL}(2,3)$

	1	7_1	7_2	2	4	3_j	6_j
$\chi_{1,k}$	1	1	1	1	1	ζ_3^{jk}	ζ_3^{jk}
$\chi_{2,k}$	2	2	2	-2	0	$-\zeta_3^{jk}$	ζ_3^{jk}
χ_3	3	3	3	3	-1	0	0
$\chi_{4,1}$	24	3	-4	0	0	0	0
$\chi_{4,1}$	24	-4	3	0	0	0	0

$j = 1, 2, \quad k = 1, 2, 3$

• $C_{19}^2 \rtimes \mathrm{SL}(2,5)$

	1	19_j	2	4	3	6	$5_\pm$	$10_\pm$
χ_1	1	1	1	1	1	1	1	1
$\chi_{2,+}$	2	2	−2	0	−1	1	$\frac{-1\pm\sqrt{5}}{2}$	$\frac{1\mp\sqrt{5}}{2}$
$\chi_{2,-}$	2	2	−2	0	−1	1	$\frac{-1\mp\sqrt{5}}{2}$	$\frac{1\pm\sqrt{5}}{2}$
$\chi_{3,+}$	3	3	3	−1	0	0	$\frac{1\pm\sqrt{5}}{2}$	$\frac{1\pm\sqrt{5}}{2}$
$\chi_{3,-}$	3	3	3	−1	0	0	$\frac{1\mp\sqrt{5}}{2}$	$\frac{1\mp\sqrt{5}}{2}$
$\chi_{4,\pm}$	4	4	± 4	0	1	± 1	−1	∓ 1
χ_5	5	5	5	1	−1	−1	0	0
χ_6	6	6	−6	0	0	0	1	−1
$\chi_{7,k}$	120	$\sigma_{j+k}(\alpha)$	0	0	0	0	0	0

$j = 0, 1, 2, \quad k = 0, 1, 2, \quad \sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta_{19})/\mathbb{Q})$, $\sigma_i(\zeta_{19}) = \zeta_{19}^{2^i}$,

$\alpha = 3\zeta_{19} - 2\zeta_{19}^4 - 2\zeta_{19}^6 + 3\zeta_{19}^7 + 3\zeta_{19}^8 - 2\zeta_{19}^9 - 2\zeta_{19}^{10} + 3\zeta_{19}^{11} + 3\zeta_{19}^{12} - 2\zeta_{19}^{13} - 2\zeta_{19}^{15} + 3\zeta_{19}^{18}$

• $C_{59}^2 \rtimes \mathrm{SL}(2,5)$

	1	59_j	2	4	3	6	$5_\pm$	$10_\pm$
χ_1	1	1	1	1	1	1	1	1
$\chi_{2,+}$	2	2	−2	0	−1	1	$\frac{-1\pm\sqrt{5}}{2}$	$\frac{1\mp\sqrt{5}}{2}$
$\chi_{2,-}$	2	2	−2	0	−1	1	$\frac{-1\mp\sqrt{5}}{2}$	$\frac{1\pm\sqrt{5}}{2}$
$\chi_{3,+}$	3	3	3	−1	0	0	$\frac{1\pm\sqrt{5}}{2}$	$\frac{1\pm\sqrt{5}}{2}$
$\chi_{3,-}$	3	3	3	−1	0	0	$\frac{1\mp\sqrt{5}}{2}$	$\frac{1\mp\sqrt{5}}{2}$
$\chi_{4,\pm}$	4	4	± 4	0	1	± 1	−1	∓ 1
χ_5	5	5	5	1	−1	−1	0	0
χ_6	6	6	−6	0	0	0	1	−1
$\chi_{7,k}$	120	$\sigma_{j+k}(\alpha)$	0	0	0	0	0	0

$j = 0, \ldots, 28, \quad k = 0, \ldots, 28, \quad \sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta_{59})/\mathbb{Q})$, $\sigma_i(\zeta_{59}) = \zeta_{59}^{2^i}$,

$$\begin{aligned}\alpha = {} & \zeta_{59} - 2\zeta_{59}^2 - \zeta_{59}^3 + \zeta_{59}^4 + \zeta_{59}^5 - \zeta_{59}^6 - \zeta_{59}^7 - 2\zeta_{59}^8 + 3\zeta_{59}^{10} + 2\zeta_{59}^{11} - 2\zeta_{59}^{12} + \zeta_{59}^{14} - \zeta_{59}^{16} - \zeta_{59}^{17} \\ & + \zeta_{59}^{19} + 2\zeta_{59}^{21} - 2\zeta_{59}^{22} - \zeta_{59}^{23} + 2\zeta_{59}^{25} - 2\zeta_{59}^{26} + 2\zeta_{59}^{28} + \zeta_{59}^{29} + \zeta_{59}^{30} + 2\zeta_{59}^{31} - 2\zeta_{59}^{33} + 2\zeta_{59}^{34} - \zeta_{59}^{36} \\ & - 2\zeta_{59}^{37} + 2\zeta_{59}^{38} + \zeta_{59}^{40} - \zeta_{59}^{42} - \zeta_{59}^{43} + \zeta_{59}^{45} - 2\zeta_{59}^{47} + 2\zeta_{59}^{48} + 3\zeta_{59}^{49} - 2\zeta_{59}^{51} - \zeta_{59}^{52} - \zeta_{59}^{53} + \zeta_{59}^{54} \\ & + \zeta_{59}^{55} - \zeta_{59}^{56} - 2\zeta_{59}^{57} + \zeta_{59}^{58}\end{aligned}$$

Weitere Gruppen

• $C_7^2 \rtimes \mathrm{SL}(2,3)$ (`SmallGroup(1176,214)` in GAP)

	1	7_1	$7_{2,i}$	2	4	3_j	6_j	$21_{i,j}$
$\chi_{1,k}$	1	1	1	1	1	ζ_3^{jk}	ζ_3^{jk}	ζ_3^{jk}
$\chi_{2,k}$	2	2	2	-2	0	$-\zeta_3^{jk}$	ζ_3^{jk}	$-\zeta_3^{jk}$
χ_3	3	3	3	3	-1	0	0	0
$\chi_{4,k,\ell}$	8	1	$\sigma_{i+\ell}(\alpha)$	0	0	$2\zeta_3^{jk}$	0	$(\zeta_7^{2^{i+\ell}} + \zeta_7^{6\cdot 2^{i+\ell}}) \cdot \zeta_3^{jk}$
χ_5	24	-4	3	0	0	0	0	0

$i = 0,1,2, \quad j = 1,2, \quad k = 0,1,2, \quad \ell = 0,1,2,$
$\alpha = \zeta_7 + 3\zeta_7^3 + 3\zeta_7^4 + \zeta_7^6, \quad \sigma_m \in \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}),\ \sigma_m(\zeta_7) = \zeta_7^{2^m}$

• $(C_3^3 \times C_5) \rtimes C_{52}$ (C_{52} operiert sowohl auf C_3^3 als auch auf C_5 transitiv)

	1	3	5	$15_\pm$	2	$4_\pm$	6	13_j	26_j	$52_{j,\pm}$	65_j
$\chi_{1,k}$	1	1	1	1	$(-1)^k$	$(\pm i)^k$	1	ζ_{13}^{jk}	$(-\zeta_{13}^{j})^k$	$(\pm i\zeta_{13}^{j})^k$	ζ_{13}^{jk}
$\chi_{2,\ell}$	4	4	-1	-1	0	0	0	$4\zeta_{13}^{j\ell}$	0	0	$-\zeta_{13}^{b\ell}$
$\chi_{3,\pm}$	26	-1	26	-1	± 26	0	∓ 1	0	0	0	0
$\chi_{4,+}$	52	-2	-13	α_+	0	0	0	0	0	0	0
$\chi_{4,-}$	52	-2	-13	α_-	0	0	0	0	0	0	0

$j = 1,\dots,12, \quad k = 0,\dots,51, \quad \ell = 0,\dots,12, \quad \alpha_+ = \frac{1\pm 3\sqrt{-15}}{2}, \quad \alpha_- = \frac{1\mp 3\sqrt{-15}}{2}$

• $C_{11}^2 \rtimes Q_{12}$

	1	$11_{1,j}$	$11_{2,j}$	2	$4_\pm$	3	6
$\chi_{1,k}$	1	1	1	$(-1)^k$	$(\pm i)^k$	1	$(-1)^k$
$\chi_{2,\pm}$	2	2	2	± 2	0	-1	∓ 1
$\chi_{3,1,\ell}$	12	$\sigma_{j+\ell}(\alpha)$	$\sigma_{j+\ell}(\beta)$	0	0	0	0
$\chi_{3,2,\ell}$	12	$\sigma_{j+\ell}(\beta)$	$\sigma_{j+\ell}(\alpha)$	0	0	0	0

$j = 0,\dots,4, \quad k = 0,\dots,3, \quad \ell = 0,\dots,4, \quad \sigma_m \in \mathrm{Gal}(\mathbb{Q}(\zeta_{11})/\mathbb{Q}),\ \sigma_m(\zeta_{11}) = \zeta_{11}^{2^m}$
$\alpha = \zeta_{11} + \zeta_{11}^2 + 2\zeta_{11}^3 + 2\zeta_{11}^4 + 2\zeta_{11}^7 + 2\zeta_{11}^8 + \zeta_{11}^9 + \zeta_{11}^{10}$
$\beta = 1 + 2\zeta_{11} - \zeta_{11}^2 - \zeta_{11}^3 - \zeta_{11}^8 - \zeta_{11}^9 + 2\zeta_{11}^{10}$

• $(C_2^2 \times C_7) \rtimes C_3$ (C_3 operiert sowohl auf C_2^2 als auch auf C_7 nichttrivial)

	1	2	3_i	$7_\pm$	$14_{+,j}$	$14_{-,j}$
$\chi_{1,k}$	1	1	ζ_3^{ik}	1	1	1
χ_2	3	-1	0	3	-1	-1
$\chi_{3,+}$	3	3	0	$\frac{-1\pm\sqrt{-7}}{2}$	$\zeta_7 + \zeta_7^2 + \zeta_7^4$	$\zeta_7^3 + \zeta_7^5 + \zeta_7^6$
$\chi_{3,-}$	3	3	0	$\frac{-1\mp\sqrt{-7}}{2}$	$\zeta_7^3 + \zeta_7^5 + \zeta_7^6$	$\zeta_7 + \zeta_7^2 + \zeta_7^4$
$\chi_{4,\ell,+}$	3	-1	0	$\frac{-1\pm\sqrt{-7}}{2}$	$\zeta_7^{3\cdot 2^{j+\ell}} - \zeta_7^{5\cdot 2^{j+\ell}} - \zeta_7^{6\cdot 2^{j+\ell}}$	$\zeta_7^{2^{j+\ell}} - \zeta_7^{2\cdot 2^{j+\ell}} - \zeta_7^{4\cdot 2^{j+\ell}}$
$\chi_{4,\ell,-}$	3	-1	0	$\frac{-1\mp\sqrt{-7}}{2}$	$\zeta_7^{2^{j+\ell}} - \zeta_7^{2\cdot 2^{j+\ell}} - \zeta_7^{4\cdot 2^{j+\ell}}$	$\zeta_7^{3\cdot 2^{j+\ell}} - \zeta_7^{5\cdot 2^{j+\ell}} - \zeta_7^{6\cdot 2^{j+\ell}}$

$i = 1,2, \quad j = 0,1,2, \quad k = 1,2, \quad \ell = 0,1,2$

• $C_{11}^2 \rtimes (C_5 \times Q_{12})$

	1	11_1	11_2	2	$4_\pm$	3	6
$\chi_{1,k}$	1	1	1	$(-1)^k$	$(\pm i)^k$	1	$(-1)^k$
$\chi_{2,\ell}$	2	2	2	$2(-1)^\ell$	0	-1	$(-1)^{\ell+1}$
$\chi_{3,1}$	60	5	-6	0	0	0	0
$\chi_{3,2}$	60	-6	5	0	0	0	0

	5_j	10_j	15_j	$20_{\pm,j}$	30_j
$\chi_{1,k}$	ζ_5^{jk}	$(-\zeta_5^j)^k$	ζ_5^{jk}	$(\pm i\zeta_5^j)^k$	$(-\zeta_5^j)^k$
$\chi_{2,\ell}$	$2\zeta_5^{j\ell}$	$2(-\zeta_5^j)^\ell$	$-\zeta_5^{j\ell}$	0	$-\zeta_5^{j\ell}$
$\chi_{3,1}$	0	0	0	0	0
$\chi_{3,2}$	0	0	0	0	0

$j = 1, \ldots, 4, \quad k = 0, \ldots, 19, \quad \ell = 0, \ldots, 9$

• $(Q_8 \times C_7) \rtimes C_3$ (C_3 operiert sowohl auf Q_8 als auch auf C_7 nichttrivial)

	1	2	3_i	4	6_i	$7_\pm$	$14_\pm$
$\chi_{1,k}$	1	1	ζ_3^{ik}	1	ζ_3^{ik}	1	1
$\chi_{2,k}$	2	-2	$-\zeta_3^{ik}$	0	ζ_3^{ik}	2	-2
χ_3	3	3	0	-1	0	3	3
$\chi_{4,+}$	3	3	0	3	0	$\frac{-1\pm\sqrt{-7}}{2}$	$\frac{-1\pm\sqrt{-7}}{2}$
$\chi_{4,-}$	3	3	0	3	0	$\frac{-1\mp\sqrt{-7}}{2}$	$\frac{-1\pm\sqrt{-7}}{2}$
$\chi_{5,\ell,+}$	3	3	0	-1	0	$\frac{-1\pm\sqrt{-7}}{2}$	$\frac{-1\pm\sqrt{-7}}{2}$
$\chi_{5,\ell,-}$	3	3	0	-1	0	$\frac{-1\mp\sqrt{-7}}{2}$	$\frac{-1\mp\sqrt{-7}}{2}$
$\chi_{6,+}$	6	-6	0	0	0	$-1 \pm \sqrt{-7}$	$1 \mp \sqrt{-7}$

	$28_{+,j}$	$28_{-,j}$
$\chi_{1,k}$	1	1
$\chi_{2,k}$	0	0
χ_3	-1	-1
$\chi_{4,+}$	$\zeta_7 + \zeta_7^2 + \zeta_7^4$	$\zeta_7^3 + \zeta_7^5 + \zeta_7^6$
$\chi_{4,-}$	$\zeta_7^3 + \zeta_7^5 + \zeta_7^6$	$\zeta_7 + \zeta_7^2 + \zeta_7^4$
$\chi_{5,\ell,+}$	$\zeta_7^{2^{j+\ell}} - \zeta_7^{2\cdot 2^{j+\ell}} - \zeta_7^{4\cdot 2^{j+\ell}}$	$\zeta_7^{3\cdot 2^{j+\ell}} - \zeta_7^{5\cdot 2^{j+\ell}} - \zeta_7^{6\cdot 2^{j+\ell}}$
$\chi_{5,\ell,-}$	$\zeta_7^{3\cdot 2^{j+\ell}} - \zeta_7^{5\cdot 2^{j+\ell}} - \zeta_7^{6\cdot 2^{j+\ell}}$	$\zeta_7^{2^{j+\ell}} - \zeta_7^{2\cdot 2^{j+\ell}} - \zeta_7^{4\cdot 2^{j+\ell}}$
$\chi_{6,+}$	0	0

$i = 1, 2, \quad j = 0, 1, 2, \quad k = 1, 2, \quad \ell = 0, 1, 2$

Literaturverzeichnis

[1] S. D. Berman: *On the theory of representations of finite groups.* Dokl. Akad. Nauk SSSR 86 (1952) 885–888 (Russisch).

[2] S. D. Berman: *Characters of linear representations of finite groups over an arbitrary field.* Mat. Sb. 44 (1958) 409–456 (Russisch).

[3] S. D. Berman, P. M. Gudivok: *Indecomposable representations of finite groups over the ring of p-adic integers.* Izv. Akad. Nauk SSSR Ser. Mat. 28 (1964) 875–910 (Russisch).

[4] Z. I. Borevich, I. R. Shafarevich: *Number theory.* Academic Press, New York-London, 1966.

[5] R. Brauer: *A characterization of the characters of groups of finite order.* Ann. of Math. 57 (1953) 357–377.

[6] J. Coates: *p-adic L-functions and Iwasawa's theory.* In: A. Fröhlich (Ed.), Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, 1975). Academic Press, London, 269–353, 1977.

[7] H. Cohen: *Number theory I.* GTM 239. Springer, New York, 2007.

[8] H. Cohen: *Number theory II.* GTM 240. Springer, New York, 2007.

[9] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson: *Atlas of finite groups.* Oxford University Press, Eynsham, 1985.

[10] B. N. Cooperstein: *Maximal subgroups of* $G_2(2^n)$. J. Algebra 70 (1981) 23–36.

[11] M. Costantini, E. Jabara: *On finite groups in which cyclic subgroups of the same order are conjugate.* Comm. Algebra 37 (2009) 3966–3990.

[12] D. Craven: *The theory of fusion systems: an algebraic approach.* CSAM 131. Cambridge University Press, Cambridge, 2011.

[13] C. W. Curtis, W. M. Kantor, G. M. Seitz: *The* 2*-transitive permutation representations of the finite Chevalley groups.* Trans. Amer. Math. Soc. 218 (1976) 1–59.

[14] C. W. Curtis, I. Reiner: *Methods of representation theory. Vol. I.* Wiley-Interscience, New York, 1981.

[15] M. Deiml: *Zur Darstellungstheorie von Darstellungsringen.* Dissertation, Friedrich-Schiller-Universität Jena, 1997.

[16] D. I. Deriziotis, G. O. Michler: *Character table and blocks of finite simple triality groups* ${}^3D_4(q)$. Trans. Amer. Math. Soc. 303 (1987) 39–70.

[17] L. Dornhoff: *Group Representation Theory. Part A: Ordinary representation theory.* Marcel Dekker, New York, 1971.

[18] J. A. Drozd, A. V. Roĭter: *Commutative rings with a finite number of indecomposable integral representations.* Izv. Akad. Nauk SSSR Ser. Mat. 31 (1967) 783–798 (Russisch).

[19] R. H. Dye: *On the involution classes of the linear groups* $\mathrm{GL}_n(K)$, $\mathrm{SL}_n(K)$, $\mathrm{PGL}_n(K)$, $\mathrm{PSL}_n(K)$ *over fields of characteristic two.* Proc. Cambridge Philos. Soc. 72 (1972) 1–6.

[20] R. H. Dye: *On the conjugacy classes of involutions of the unitary groups* $\mathrm{U}_m(K)$, $\mathrm{SU}_m(K)$, $\mathrm{PU}_m(K)$, $\mathrm{PSU}_m(K)$, *over perfect fields of characteristic* 2. J. Algebra 24 (1973) 453–459.

[21] V. Ennola: *On the conjugacy classes of the finite unitary groups.* Ann. Acad. Sci. Fenn. Ser. A I 3 (1962) 3–13.

[22] T. Fritzsche: *The Brauer group of character rings.* J. Algebra 361 (2012) 37–40.

[23] GAP – *Groups, algorithms and programming.* Version 4.4.12, 2008.

[24] E. L. Green, I. Reiner: *Integral representations and diagrams.* Michigan Math. J. 25 (1978) 53–84.

[25] A. Heller, I. Reiner: *Representations of cyclic groups in rings of integers, I.* Ann. of Math. 76 (1962) 73–92.

[26] A. Heller, I. Reiner: *Representations of cyclic groups in rings of integers, II.* Ann. of Math. 77 (1963) 318–328.

[27] C. Hering: *Transitive linear groups and linear groups which contain irreducible subgroups of prime order.* Geom. Dedic. 2 (1974) 425–460.

[28] G. Higman: *Suzuki* 2*-groups.* Illinois J. Math. 7 (1963) 79–96.

[29] B. Huppert: *Endliche Gruppen I.* GMW 134. Springer, Berlin, 1967.

[30] B. Huppert, N. Blackburn: *Finite Groups II.* GMW 242. Springer, Berlin, 1982.

[31] B. Huppert, N. Blackburn: *Finite Groups III.* GMW 243. Springer, Berlin, 1982.

[32] I. M. Isaacs: *Character theory of finite groups.* Dover, New York, 1994.

[33] H. Jacobinski: *Sur les ordres commutatifs avec un nombre fini de réseaux indécomposables.* Acta Math. 118 (1967) 1–31.

[34] A. Jones: *Groups with a finite number of indecomposable integral representations.* Michigan Math. J. 10 (1963) 257–261.

[35] H. E. Jordan: *Group-characters of various types of linear groups.* Amer. J. Math. 29 (1907) 387–405.

[36] G. Karpilovsky: *Group representations. Vol. 1. Part B. Introduction to group representations and characters.* North-Holland Mathematics Studies 175. North-Holland, Amsterdam, 1992.

[37] P. B. Kleidman: *The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$, and their automorphism groups.* J. Algebra 117 (1988) 30–71.

[38] G. Navarro, J. Tent: *Rationality and Sylow 2-subgroups.* Proc. Edinb. Math. Soc. 53 (2010) 787–798.

[39] J. Neukirch: *Algebraische Zahlentheorie.* Springer, Berlin, 1992.

[40] A. Raggi-Cárdenas: *Burnside rings of finite representation type.* Bull. Austral. Math. Soc. 42 (1990) 247–251.

[41] U. Reichenbach: *Modultheorie von Burnsideringen endlicher Gruppen.* Mathematica Gottingensis 12, 1997.

[42] J. Rosenberg: *Algebraic K-theory and its applications.* GTM 147. Springer, New York, 1994.

[43] A. I. Saksonov: *The integral ring of characters of a finite group.* Vesci Akad. Navuk BSSR Ser. Fiz.-Mat. Navuk 1966 (1966) 69–76 (Russisch.

[44] J.-P. Serre: *Lineare Darstellungen endlicher Gruppen.* Akademie-Verlag, Berlin, 1972.

[45] E. E. Shult: *On finite automorphic algebras.* Illinois J. Math. 13 (1969) 625–653.

[46] W. A. Simpson, J. S. Frame: *The character tables for* $\mathrm{SL}(3,q)$, $\mathrm{SU}(3,q^2)$, $\mathrm{PSL}(3,q)$, $\mathrm{PSU}(3,q^2)$. Canad. J. Math. 25 (1973) 486–494.

[47] R. Steinberg: *The representations of* $\mathrm{GL}(3,q)$, $\mathrm{GL}(4,q)$, $\mathrm{PGL}(3,q)$, *and* $\mathrm{PGL}(4,q)$. Canadian J. Math. 3 (1951) 225–235.

[48] M. Suzuki: *Applications of group characters.* In: Proc. Sympos. Pure Math., vol. 1. Amer. Math. Soc., Providence, 88–99, 1959.

[49] M. Suzuki: *On a class of doubly transitive groups.* Ann. of Math. 75 (1962) 105–145.

[50] M. Szymik: *The Brauer group of Burnside rings.* J. Algebra 324 (2010) 2589–2593.

[51] A. Terras: *Fourier analysis on finite groups and applications*. LMSST 43. Cambridge University Press, Cambridge, 1999.

[52] H. N. Ward: *On Ree's series of simple groups*. Trans. Amer. Math. Soc. 121 (1966) 62–89.

[53] L. C. Washington: *Introduction to cyclotomic fields*. GTM 83. Springer, New York, 1997.

[54] B. Wilkens: 2-*automorphic* 2-*groups and some applications*. Dissertation, Martin-Luther-Universität Halle-Wittenberg, 2001.

[55] R. A. Wilson: *The finite simple groups*. GTM 251. Springer, London, 2009.

[56] H. Yamaki: *The order of a group of even order*. Proc. Amer. Math. Soc. 136 (2008) 397–402.

[57] K. Yamauchi: *A unit group of the character ring in an alternating group*. Hokkaido Math. J. 20 (1991) 549–558.

[58] K. Yamauchi: *A unit group of the character ring in an alternating group, II*. Hokkaido Math. J. 22 (1993) 13–23.

[59] K. Yamauchi: *The construction of units of infinite order in the character ring of a finite group*. Yokohama Math. J. 51 (2005) 89–97.

Stichwortverzeichnis

Lebenslauf

Zur Person

Name	Tim Fritzsche
Geboren	28. August 1985 in Leipzig
E-Mail-Adresse	`tim.fritzsche@uni-jena.de`

Ausbildung

08/1992 – 07/1998	Grundschule „Am Beetzsee“ in Radewege
08/1998 – 06/2005	Bertolt-Brecht-Gymnasium Brandenburg/Havel
06/2005	Abitur mit Note 1,0, Auszeichnung als bester Abiturient der Stadt Brandenburg 2005
07/2005 – 03/2006	Zivildienst in den Wohn- und Werkstätten „Theodor Fliedner“ in Brandenburg/Havel
04/2006 – 10/2010	Mathematikstudium mit Nebenfach Physik an der Friedrich-Schiller-Universität Jena
10/2010	Diplom Mathematik mit Prädikat „Sehr gut“
seit 04/2011	Wissenschaftlicher Mitarbeiter am Mathematischen Institut der Friedrich-Schiller-Universität Jena

Veröffentlichungen und Vorträge

- *The depth of subgroups of* $\mathrm{PSL}(2,q)$, J. Algebra 349 (2012), 217–233.
- *The Brauer group of character rings*, J. Algebra 361 (2012), 37–40.
- *The Brauer group of character rings*, Young Algebraists' Conference 2012, Lausanne.
- *The depth of subgroups of* $\mathrm{PSL}(2,q)$ *II*, J. Algebra 381 (2013), 37–53.
- (gemeinsam mit B. Külshammer und C. Reiche) *The depth of Young subgroups of symmetric groups*, J. Algebra 381 (2013), 96–109.
- *CSC-groups and the representation type of the character ring*, Algebra-Seminar Halle-Jena, Halle 2013.

Sonstiges

- Organisation des Junior Mathematical Congress 2008 in Jena (als einer von drei Hauptorganisatoren).
- Leitung der Redaktion der Zeitschrift „Die Wurzel“ seit November 2008.

Ehrenwörtliche Erklärung

Hiermit erkläre ich,

- dass mir die geltende Promotionsordnung der Fakultät bekannt ist,
- dass ich die Dissertation selbst angefertigt, keine Textabschnitte oder Ergebnisse eines Dritten oder eigener Prüfungsarbeiten ohne Kennzeichnung übernommen und alle von mir benutzten Hilfsmittel, persönlichen Mitteilungen und Quellen in meiner Arbeit angegeben habe,
- dass ich die Hilfe eines Promotionsberaters nicht in Anspruch genommen habe und dass Dritte weder unmittelbar noch mittelbar geldwerte Leistungen von mir für Arbeiten erhalten haben, die im Zusammenhang mit dem Inhalt der vorgelegten Dissertation stehen,
- dass ich die Dissertation noch nicht als Prüfungsarbeit für eine staatliche oder andere wissenschaftliche Prüfung eingereicht habe.

Bei der Auswahl und Auswertung des Materials sowie bei der Herstellung des Manuskripts haben mich folgende Personen unterstützt: Prof. Dr. Burkhard Külshammer.

Ich habe die gleiche, eine in wesentlichen Teilen ähnliche bzw. eine andere Abhandlung bereits bei einer anderen Hochschule als Dissertation eingereicht: Nein.

Jena, den 20. Februar 2014