Perfekte Komplemente in endlichen Frobeniusgruppen

Martin Brüning

27. Dezember 2017

Diese Arbeit behandelt die Klassifikation perfekter Frobeniuskomplemente und die Bemühungen, diese mit "gefesselten Händen" ohne Charaktertheorie zu bestimmen. Der Text basiert auf meiner Diplomarbeit, die ich 2010 als Student bei Herrn Prof. Dr. Grundhöfer an der Universität Würzburg angefertigt habe. Ich habe hierfür einen Beweis von Ulrich Meierfrankenfeld von der Michigan State University reproduziert. Die Lösung des Problems besagt folgendes: Wenn in einer endlichen Frobeniusgruppe das Komplement des Frobeniuskerns eine perfekte Gruppe ist, so ist diese isomorph zur speziellen linearen Gruppe $\mathrm{SL}_2(5) = \left\{X \in \mathbb{Z}_5^{2\times 2} \mid \det X = 1\right\}$.

Inhaltsverzeichnis

1 Einleitung

Darstellungs- und Charaktertheorie sind mitunter die wichtigsten Hilfsdisziplinen, um Sätze über endliche Gruppen zu beweisen. Insbesondere bei der Beschreibung endlicher Frobeniusgruppen, mit der sich diese Diplomarbeit beschäftigt, sind die größten Durchbrüche erstmals mittels Methoden linearer Darstellungen und deren Gruppencharakteren gelungen. In der modernen Gruppentheorie ist man nun interessiert, alternative Beweismethoden zu entwickeln, welche zumindest ohne den Einsatz von Gruppencharakteren auskommen. Während derartige Bemühungen in diversen Fällen erfolgreich waren, entziehen sich zwei bedeutende Resultate bis heute noch der Möglichkeit eines vollständig charakterfreien Beweises:

- der Satz von Frobenius über die Untergruppeneigenschaft der fixpunktfreien Elemente und des Neutralen in einer Frobeniusgruppe
- die Bestimmung des (einzigen) Isomorphietyps perfekter Komplemente endlicher Frobeniusgruppen.

Ferdinand Georg Frobenius (1849-1917), der die klassische Gruppentheorie wie kaum ein anderer geprägt hat, ließ seinen Satz 1901 im Sitzungsbericht der Königlich-Preußischen Akademie der Wissenschaften [1] publizieren und zeigte darin, dass die später nach ihm benannten Frobeniusgruppen stets isomorph zu einem semidirekten Produkt $G = KH \approx K \rtimes H$ sind mit dem Frobeniuskern K als Normalteiler und einem Frobeniuskomplement H. Der Frobeniuskern wird durch die fixpunktfreien Elemente von G bezüglich der Operation auf dem Nebenklassenraum G/H eindeutig festgelegt, wogegen H nur bis auf Konjugation bestimmt ist.

Mit dem Satz von Frobenius lässt sich zeigen, dass in jeder Frobeniusgruppe ein zugehöriges Komplement H stets isomorph zu einer fixpunktfreien Automorphismengruppe eines geeigneten Vektorraums V ist. Der Vektorraum V wird dabei aus einer elementar abelschen p-Untergruppe des Frobeniuskerns K über dem endlichen Restklassenkörper $\mathbb{F}_p$ der Charakteristik p konstruiert. Umgekehrt ist eine fixpunktfreie Automorphismengruppe H eines Vektorraums V über einem Körper $\mathbb{K}$ stets isomorph zu einem Komplement in einer geeigneten Frobeniusgruppe, die wir als $V \rtimes H$ angeben können. Damit erweist sich die Klassifikation perfekter Frobeniuskomplemente als äquivalent zur Bestimmung perfekter Gruppen fixpunktfreier Vektorraumautomorphismen. Letztere Aufgabe wurde 1934 von Hans Zassenhaus (1912-1991) bewältigt.

In seiner Arbeit über endliche Fastkörper in den Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg [2] konnte Zassenhaus zeigen, dass perfekte Gruppen

fixpunktfreier Vektorraumautomorphismen stets isomorph zur speziellen Linearen Gruppe

$$\mathrm{S}L_2(5) = \left\{X \in \mathbb{Z}_5^{2\times 2} \mid \det X = 1\right\}$$

sind. Dieses Ergebnis werden wir im Folgenden auch als "$\mathrm{S}L_2(5)$-Theorem" bezeichnen. Die Arbeit von Zassenhaus war innovativ, aber in ihrer Durchführung nicht in allen Details vollständig. Einer Empfehlung von Daniel Gorenstein (1923-1992) folgend hat Zassenhaus den Beweis 1985 in [3] nocheinmal sorgfältig dargelegt.

Nach dem zuvor gesagten ist damit der einzige Isomorphietyp perfekter Frobeniuskomplemente als $\mathrm{S}L_2(5)$ ausgemacht. Es sei daran erinnert, dass die Äquivalenz des $\mathrm{S}L_2(5)$-Theorems zur Klassifikation perfekter Frobeniuskomplemente auf dem Satz von Frobenius basiert und damit indirekt von charaktertheoretischen Hilfsmitteln abhängt. Ebenso ist der Beweis des $\mathrm{S}L_2(5)$-Theorems von Zassenhaus ein charaktertheoretischer.

Nach 1998 gaben Ulrich Meierfrankenfeld in [4] und Victor Mazurov in [5] zwei neue Beweise des $\mathrm{S}L_2(5)$-Theorems, welche ohne den Einsatz von Gruppencharakteren auskommen. Auf der Suche nach neuen Beweismöglichkeiten der beiden genannten Hauptresultate über Frobeniusgruppen ist das ein entscheidender Teilerfolg, denn er führt einen charakterfreien Beweis des Klassifikationssatzes auf den Satz von Frobenius zurück, dessen Beweis ist allerdings bis heute nicht ohne Charaktertheorie gelungen. Der bislang übliche Beweis dieses Satzes ist im wesentlichen der selbe, den Frobenius in [1] gab. Eine leicht veränderte Variante hat Helmut Wielandt 1958 in [6] gegeben. Ein komplett neuer Beweis wurde erst 2009 von Wolfgang Knapp und Peter Schmid in [7] publiziert. Der Beweis von Knapp und Schmid ist wesentlich kürzer, als der alte Beweis nach Frobenius und Wielandt. Er verwendet jedoch nach wie vor Charaktertheorie.

Im Folgenden soll zunächst der Zusammenhang des $\mathrm{S}L_2(5)$-Theorems zur Bestimmung der perfekten Frobeniuskomplemente aufgezeigt werden. Anschließend den Beweis von Meierfrankenfeld in einem sinnvollen Kontext darzustellen, ist das Hauptziel dieser Arbeit und nimmt den meisten Raum ein. Mit dem Beweis des Satzes von Frobenius nach Knapp und Schmid wird diese Diplomarbeit abgeschlossen. Dabei folgen wir einer leicht geänderten Fassung nach einer Mitteilung von Prof. Peter Müller.

Alle benötigten Notationskonventionen, Begriffe und Sätze werden im Text genannt, wenn sie erstmals verwendet werden, oder zuvor, falls es in den lokalen thematischen Kontext passt. Es können aber im hiesigen Rahmen selbstverständlich nicht alle benötigten Sätze bewiesen werden, so dass mitunter der Beweis nur angedeutet oder auf entsprechende Literatur verwiesen wird. Insgesamt wurde versucht, einen Stil zu finden, der mit dem Pensum der üblichen Einführungsvorlesungen in Algebra nachvollzogen werden kann. Im

Mittelpunkt dieser Arbeit stehen ausschließlich endliche Gruppen. Hier und im Folgenden sind daher auch ohne explizite Erwähnung alle Gruppen in allen Zusammenhängen stets als endlich vorausgesetzt.

2 Frobeniusgruppen

2.1 Definition von Frobeniusgruppen

Eine Darstellung oder Operation einer Gruppe G auf einer Menge Ω ist ein Homomorphismus $G \to S_\Omega$ in die symmetrische Gruppe von Ω. Ist $\Omega = V$ ein Vektorraum über einem Körper $\mathbb{K}$ und das Bild von G eine Automorphismengruppe von V, so sprechen wir auch von einer linearen Darstellung und nennen V einen G-Modul. Identifiziert man die mit den Elementen aus G assoziierten Automorphismen mit ihren Darstellungsmatrizen bezüglich einer Basis, so sprechen wir von einer Matrizendarstellung.

Die Menge aller Endomorphismen auf V bildet den Endomorphismenring End$V$. Identifiziert man die Elemente von G mit den ihnen zugeordneten Automorphismen, so lässt sich auch der von G erzeugte Unterring von End$V$ betrachten. Er besteht aus allen Linearkombinationen der von G induzierten Automorphismen. Ohne auf den Vektorraum und die spezielle Darstellung Bezug zu nehmen, lässt er sich präzise als Menge der finiten Abbildungen $a : G \mapsto \mathbb{K}$ verallgemeinern. Man schreibt sie als Linearkombinationen $a = \sum_{x \in G} a_x x$ und definiert eine polynomiale Multiplikation

$$\left(\sum_{g \in G} a_g g\right)\left(\sum_{g \in G} b_g g\right) = \sum_{x \in G}\left(\sum_{\substack{g,h \in G \\ gh = x}} a_g b_h\right) x.$$

Den so konstruierten Ring bezeichnen wir als den Gruppenring $\mathbb{K}G$. Jeder von G induzierte Automorphismenring von $\mathbb{K}$-Vektorräumen ist ein Faktorring von $\mathbb{K}G$. Ein Vektorraum über $\mathbb{K}$ ist genau dann ein G-Modul, wenn er ein Modul über $\mathbb{K}G$ im Sinne der Ringtheorie ist.

Für Gruppenoperationen verwenden wir die Linksnotation. Dabei ist die linksseitige Kürzungsregel

$$gx = gy \quad \Longrightarrow \quad x = y \qquad \forall x, y \in \Omega, g \in G$$

eine direkte Folgerung aus der Injektivität der assoziierten Elemente in S_Ω und somit trivialerweise erfüllt. Eine rechtsseitige Kürzungsregel

$$gx = hx \quad \Longrightarrow \quad g = h \qquad \forall x \in \Omega, g, h \in G$$

ist hingegen nur genau dann erfüllt, wenn alle nicht trivialen Elemente fixpunktfrei operieren. In diesem Fall sagen wir, G operiert scharf auf Ω. Zu $\omega \in \Omega$ bezeichnen wir den

Stabilisator mit $G_\omega = \{g \in G \mid g\omega = \omega\}$. Eine Darstellung ist genau dann scharf, wenn alle Stabilisatoren G_ω trivial sind.

Der Kern der Darstellung $G \to S_\Omega$ ist der Durchschnitt aller Stabilisatoren $\bigcap_\omega G_\omega$. Wir haben also eine injektive Darstellung der Faktorgruppe $\frac{G}{\bigcap_\omega G_\omega} \hookrightarrow S_\Omega$. Ist eine Darstellung injektiv, so nennen wir sie treu und die Gruppe eine Permutationsgruppe. Insbesondere ist das der Fall, wenn die Operation scharf und damit insbesondere $\bigcap_\omega G_\omega$ trivial ist. In der disjunkte Bahnenzerlegung $\Omega = \biguplus_\omega G\omega$ gilt für die Ordnung der einzelne Bahnen $|G\omega| = [G : G_\omega]$ und die Linkstranslation auf der Menge der Linksnebenklassen G/G_ω ist äquivalent zur Operation auf der Bahn $G\omega$ vermöge der äquivarianten Zuordnung $g\omega \longleftrightarrow gG_\omega$ bezüglich des Aufpunktes ω. Anstelle von ω lässt sich genauso gut ein beliebiges anderes Bahnelement $\tilde{\omega} = g\omega \in G\omega$ zur Konstruktion einer äquivarianten Abbildung verwenden. Für die Stabilisatoren gilt dann $G_{g\omega} = gG_\omega g^{-1} = G_\omega^{\left(g^{-1}\right)}$ respektive $G_{g\omega}^g = G_\omega$. Wir verwenden die Exponentialschreibweise wie üblich nur für rechts notierte Operationen, bei denen die Komposition in der Reihenfolge von links nach rechts erfolgt. Dementsprechend ist x^g als $g^{-1}xg$ zu lesen.

Bei transitiven Operationen besteht Ω nur aus einer einzigen Bahn. Solche Darstellungen sind folglich äquivalent zur Linkstranslation auf einem Nebenklassenraum $G/H \approx \Omega$. Dabei gilt $H = G_\omega$ für einen zuvor beliebig gewählten Aufpunkt $\omega \in \Omega$. Ist eine Operation treu und transitiv, so ist $\bigcap H^g = e$. Ist sie sogar scharf transitiv, so ist $H = e$ und $\Omega \approx G/H \approx G$. Scharf transitive Linksoperationen entsprechen also der Operation einer Gruppe auf sich selbst durch Linksmultiplikation. Eine Operation ist genau dann scharf transitiv, wenn die Gleichung

$$gx = y \qquad \text{mit} \qquad x, y \in \Omega$$

stets eine eindeutige Lösung in $g \in G$ besitzt. Die Transitivität verbürgt sich hierbei für die Existenz einer Lösung, während die Schärfe ihre Eindeutigkeit gewährleistet.

Frobeniusgruppen sind nun dadurch charakterisiert, dass H nicht trivial ist, sich bei der Bildung des Durchschnitts $\bigcap_g H^g$ jedoch paarweise verschiedene Konjugierte trivial scheiden und darüber hinaus mit $\mathrm{N}_G H = H$ der Normalisator der kleinste überhaupt mögliche ist. Äquivalent hierzu ist $H \cap H^g = e$ für alle $g \in G \setminus H$, was wir zur Definition verwenden.

Definition 2.1. (Frobeniusgruppe) Eine Gruppe G mit einer nicht trivialen, echten Untergruppe H und

$$H \cap H^g = e \qquad \forall g \in G \setminus H$$

nennen wir eine Frobeniusgruppe. H nennen wir ein Frobeniuskomplement von G.

Die Bedingung $H \cap H^g = e$ für alle $g \in G \setminus H$ bedeutet, dass kein nicht triviales Element mehr als zwei Nebenklassen stabilisiert. Da jede transitive Operation einer Operation auf einem Nebenklassenraum entspricht, sind Frobeniusgruppen gerade diejenigen transitiven Permutationsgruppen $G \hookrightarrow S_\Omega$ mit $\Omega \approx G/H$, in denen jeder Zweipunktstabilisator trivial ist. Ein Frobeniuskomplement H wird mit der Auswahl eines Aufpunkts $\omega \in \Omega$ durch dessen Stabilisator $H = G_\omega$ bestimmt und ist bis auf Konjugation eindeutig. Es ist wegen $\mathrm{N}_G H = H$ niemals ein Normalteiler.

Eine Darstellung auf Ω induziert komponentenweise eine Darstellung auf $\Omega \times \Omega$. Hierbei kann Ω selbst mit der Diagonalen D identifiziert werden. Die Trivialität der Zweipunktstabilisatoren, welche Frobeniusgruppen charakterisiert, ist dann äquivalent zur rechtsseitigen Kürzungsregel

$$gx = hx \quad \Longrightarrow \quad g = h \qquad \forall g \in G, x \in \Omega^2 \setminus D.$$

Jedes $g \in G^\#$ operiert also fixpunktfrei auf $\Omega^2 \setminus D$, da jeder Fixpunkt von g in $\Omega^2 \setminus D$ zwei Fixpunkten in Ω entspräche.

Frobeniusgruppen lassen sich in naheliegender Weise verallgemeinern. Fordert man bei einer transitiven Permutationsgruppe, dass jeder n-Punktstabilisator trivial ist, so lässt sich dies durch eine Kürzungsregel auf Ω^n charakterisieren. Dazu wählt man eine verallgemeinerte Diagonale $D^n := \{\omega \in \Omega^n \mid \omega \text{ nicht injektiv}\}$ und betrachtet die komponentenweise Operation $G \hookrightarrow \mathcal{S}_{\Omega^n \setminus D^n}$. Die Gültigkeit einer rechtsseitigen Kürzungsregel der Operation auf $\Omega^n \setminus D^n$ vererbt sich auf die Operation auf $\Omega^{n+1} \setminus D^{n+1}$. Bei der Transitivität verhält es sich genau umgekehrt. Operiert G (scharf) transitiv auf $\Omega^n \setminus D^n$, so nennen wir die ursprüngliche Operation $G \hookrightarrow S_\Omega$ auch n-fach (scharf) transitiv. Ist eine Operation n-fach scharf transitiv auf Ω, so ist das gleichbedeutend mit der eindeutigen Lösbarkeit der Gleichung

$$gx = y \qquad \text{mit} \qquad x, y \in \Omega^n \setminus D^n.$$

Frobeniusgruppen operieren demnach einfach transitiv und zweifach scharf auf Ω respektive scharf auf $\Omega^2 \setminus D$.

2.2 Grundlegende Eigenschaften von Frobeniusgruppen

Während viele Ergebnisse über Frobeniusgruppen die Anwendung starker Hilfsmittel erfordern, lassen sich mit den definierenden Eigenschaften auch ohne weiteren Aufwand bereits hilfreiche Aussagen machen. Fassen wir G als Permutationsgruppe von $G/H \approx \Omega$ auf, so zeigt sich, dass in der disjunkten Zykelzerlegung eines Elementes $g = z_1 \cdots z_m$ alle Zykel die selbe Länge haben. Ausgenommen hiervon ist der triviale Zykel eines Fixpunktes, den wir nicht mitschreiben. Zwei Zykel $z_i \neq z_j$ unterschiedlicher Längen hätten nämlich auch unterschiedliche Ordnungen. Bildet man sukzessive Potenzen g^n mit $n = 1, 2 \ldots$, so wären die Zykel z_i und z_j bei unterschiedlichen Exponenten annulliert. Diese Potenzen von g hätten dann eine der Zykellänge entsprechende Anzahl von Fixpunkten, was in Frobeniusgruppen per Definition nicht vorkommt. Also sind alle Zykel gleich lang.

Aus den gleichen Zykellängen lässt sich folgern, dass die fixpunktfreien Elemente jeweils Ordnungen haben, die $|\Omega|$ teilen, während die Ordnungen aller übrigen Elemente Teiler von $|\Omega| - 1$ sind. Wir schließen daraus, dass $|H|$ eine Potenz von $|\Omega| - 1$ teilt. Da $|\Omega|$ und $|\Omega| - 1$ teilerfremd sind, folgt daraus, dass fixpunktfreie und fixpunktbehaftete Elemente jeweils teilerfremde Ordnungen besitzen. Diese Beobachtung wird im Folgenden noch weiter präzisiert. Zuvor benötigen wir aber noch den Begriff des Frobeniuskerns und seine Ordnung.

Der eingangs erwähnte Satz von Frobenius besagt, dass die disjunkte Vereinigung $\biguplus (H^g)^\#$ aller "gelochten" Konjugierten von H das mengentheoretische Komplement eines Normalteilers $K \lhd G$ bildet, der anders als ein Frobeniuskomplement eindeutig bestimmt ist und dessen Ordnung gerade $|K| = |G/H|$ ist. Er besteht neben dem Neutralen aus allen fixpunktfreien Elementen, während die Elemente aus $G \setminus K = \biguplus (H^g)^\#$ je genau einen Fixpunkt besitzen.

Satz 2.1. (Frobenius) *Sei G eine Frobeniusgruppe mit Komplement H. Dann ist die Menge*

$$K := G \setminus \biguplus (H^g)^\# = \{e\} \cup \left(G \setminus H^G\right)$$

ein Normalteiler mit $|K| = |G/H|$. Wir nennen ihn den Frobeniuskern von G.

Beweis. Der bislang übliche Beweis nach Frobenius und Wielandt basiert auf Abzählargumenten unter Verwendung von Gruppencharakteren. Eine moderne Darstellung findet man etwa bei Gorenstein [8]. Den sehr eleganten, neuen Beweis nach Knapp und Schmid verschieben wir an das Ende der Arbeit, um die Argumentation hier nicht unnötig zu

unterbrechen. An dieser Stelle wollen wir den Satz daher als gegeben hinnehmen. Es sei aber noch erwähnt, dass abgesehen von der Abgeschlossenheit alle Untergruppeneigenschaften unmittelbar einsichtig sind, so dass die Problematik der Situation nicht auf den ersten Blick erkennbar ist.

Die zuvor gemachten Beobachtungen über die Zykellängen zeigen nämlich, dass K auf jeden Fall stabil gegenüber Inversenbildung ist, und dass mit $k \in K$ auch alle Potenzen von k in K liegen, also $\langle k \rangle \subseteq K$. Da Konjugation die Zykelstruktur eines Elementes nicht verändert, folgt auch sofort die Normalteilereigenschaft von K. Die Aussage über die Ordnung von K lässt sich ebenfalls leicht einsehen. Wegen $\mathrm{N}_G H = H$ hat die Operation von G auf den Konjugierten von H gerade $[G : \mathrm{N}_G H] = [G : H]$ Elemente. Es gilt daher

$$|K| = |G| - \left| \biguplus (H^g)^{\#} \right| = |G| - \frac{|G|}{|H|} (|H| - 1) = \frac{|G|}{|H|}.$$

□

Als direkte Folgerung aus dem Satz von Frobenius operiert H durch Konjugation als Automorphismengruppe auf K und für die Ordnung von G gilt überdies

$$|G| = |G/H| \cdot |H| = |K| \cdot |H| = |KH| \,.$$

Damit ist G ein semidirektes Produkt $G = KH \approx K \rtimes H$. Die Verknüpfung im semidirekten Produkt $K \rtimes H$ schreiben wir extern als

$$(x, g)\,(y, h) = (x \cdot gy, gh) \qquad \forall x, y \in K, g, h \in H$$

und intern dementsprechend als $xgyh = xgyg^{-1}gh$. Wir wollen die Operation von H auf K näher untersuchen.

Einen Endomorphismus nennen wir bereits fixpunktfrei wenn er außer dem neutralen Element keine weiteren Fixpunkte besitzt. Eine Darstellung als Automorphismengruppe nennen wir fixpunktfrei, wenn alle nicht trivialen Elemente im genannten Sinne fixpunktfrei operieren. Die Operation von H auf K durch Konjugation ist auf eben diese Weise fixpunktfrei, denn wegen

$$hkh^{-1} = k \Leftrightarrow h = khk^{-1} \qquad \forall h \in H, k \in K$$

widerspricht das Auftreten eines nicht trivialen Fixpunktes $k \in K$ dem trivialen Durchschnitt $H^k \cap H = e$.

Wir können nun die zuvor gemachte Bemerkung über die Teilerfremdheit der Ordnungen jeweiliger Elemente aus K und $G \setminus K$ präzisieren. Es folgt sofort, dass die Ordnungen von H und K teilerfremd sind. Außerdem gilt für den Index $[G : K] = |H|$ und $[G : H] = |K|$. Somit sind die Ordnungen von K und H jeweils teilerfremd zu ihren Indices. Untergruppen mit dieser Eigenschaft werden auch als Hallsche Untergruppen bezeichnet. Aus der Fixpunktfreiheit der Operation von H auf K folgt, dass die disjunkte Bahnenzerlegung von K neben der einelementigen Bahn e nur aus Bahnen der Länge $|H|$ besteht. Insbesondere ist $\left|K^{\#}\right| = |K| - 1$ ein Vielfaches von $|H|$ und es gilt daher

Korollar 2.1. *Sei $G = KH$ eine Frobeniusgruppe mit Kern K, Komplement H und $\Omega = G/H$. Dann ist $|H|$ ein Teiler von $\left|K^{\#}\right| = |K| - 1 = |\Omega| - 1$ und $|K| = |\Omega|$.*

Es zeigt sich sogar, dass auch umgekehrt durch die Fixpunktfreiheit einer Automorphismengruppe H einer beliebigen Gruppe K das entsprechende semidirekte Produkt zu einer Frobeniusgruppen wird. Frobeniusgruppen lassen sich daher auch äquivalent als semidirektes Produkt einer Gruppe mit einer fixpunktfreien Automorphismengruppen definieren.

Satz 2.2. *Sei K eine Gruppen und H eine Gruppe fixpunktfreier Automorphismen von K, beide nicht trivial. Dann ist das semidirekte Produkt $G = K \rtimes H$ eine Frobeniusgruppe mit Kern $K \rtimes e$ und Komplement $e \rtimes H$.*

Beweis. Sei $(e, h) \in e \rtimes H$ und $(v, k) \in G \setminus (e \rtimes H)$, d.h. mit $v \neq e$. Dann ist

$$\begin{aligned}(v,k)\,(e,h)\,(v,k)^{-1} &= (v,k)\,(e,h)\left(k^{-1}v^{-1}, k^{-1}\right)\\ &= (v,kh)\left(k^{-1}v^{-1}, k^{-1}\right)\\ &= \left(vkhk^{-1}v^{-1}, khk^{-1}\right)\end{aligned}$$

genau dann in $e \rtimes H$ enthalten, wenn $h = e$ und damit $(v, k)\,(e, h)\,(v, k)^{-1} = (e, e)$ ist. Somit ist $e \rtimes H$ ein Frobeniuskomplement und $K \rtimes H$ eine Frobeniusgruppe. □

Man mag nun annehmen, dass man eine beliebige Gruppe zu einem Frobeniuskomplement machen kann. Sofern man eine fixpunktfreie Automorphismengruppe findet, trifft dies zu. Tatsächlich stellt sich jedoch heraus, dass die Existenz einer fixpunktfreien Automorphismengruppe eine sehr restriktive Forderung ist, die im Allgemeinen nicht immer erfüllbar ist. Hierfür werden wir später mit einem Satz von Thompson ein notwendiges Kriterium angeben, was bereits aus der Existenz eines einzigen fixpunktfreien Automorphismus folgt.

2.3 Normale p-Komplemente

Wir unterbrechen die Thematik mit einem eher handwerklichen Abschnitt, um später benötigte Bezeichnungen bereit zu stellen. Wir werden die Präsenz der genannten Begriffe stets an Frobeniusgruppen beispielhaft verdeutlichen.

Sei G eine Gruppe und $K \trianglelefteq G$ ein Normalteiler, dann nennen wir eine Untergruppe H in G ein Komplement von K, falls $KH = G$ mit $K \cap H = e$ und somit $G \approx K \rtimes H$ bezüglich der Operation von H durch Konjugation auf K. Ein Frobeniuskomplement ist daher offensichtlich ein Komplement. Fordert man nicht die Trivialität des Schnittes $K \cap H$, sondern nur $KH = G$, so nennen wir H ein teilweises Komplement oder Supplement zu K. Unter besonderen Umständen trägt auch der Normalteiler K den Namen eines Komplementes. Das ist der Fall wenn H ein Komplement und Sylowgruppe ist.

Definition 2.2. (Normale p-Komplemente) Einen Normalteiler $K \trianglelefteq G$ nennen wir ein normales p-Komplement, falls er eine p-Sylowgruppe als Komplement besitzt.

Zu einer Primzahl p bezeichnen wir eine p-Sylowgruppe in einer Gruppe G zumeist mit G_p. Den Fall, dass p und die Ordnung von G teilerfremd sind, lassen wir zu, dann gilt $G_p = e$ und G besitzt sich selbst als normales p-Komplement. Ist ein Normalteiler $K \trianglelefteq G$ ein normales p-Komplement, so folgt wegen

$$G_p K = G = G^g = G_p^g K^g = G_p^g K$$

für beliebige $g \in G$, dass es auf die Wahl der Sylowgruppe G_p nicht ankommt, sondern dass jede p-Sylowgruppe bereits Komplement zu K ist. Die Ordnung eines normalen p-Komplements ist stets teilerfremd zu seinem Index. Normale p-Komplemente sind also Hallsche Untergruppen.

Sei nun wieder $G = KH$ eine Frobeniusgruppe mit Kern K, Komplement H und p ein Primteiler der Ordnung von H. Dann ist für eine Sylowgruppe H_p auch KH_p eine Frobeniusgruppe. Da H und K teilerfremde Ordnungen besitzen, ist K dann ein normales p-Komplement in KH_p. Ein hinreichendes Kriterium für die Existenz normaler p-Komplemente gibt der folgende Satz von Burnside.

Satz 2.3. (Burnside) *Sei G eine Gruppe und $P \leq G$ eine beliebige p-Sylowgruppe mit $P \leq ZN_G P$. Dann besitzt G ein normales p-Komplement.*

Beweis. Gorenstein [8], S. 252, Theorem 4.3 □

Sei $S \subseteq \mathbb{P}$ eine Menge von Primzahlen und G eine Gruppe. Dann nennen wir G eine S-Gruppe, falls jeder Primteiler der Gruppenordnung in S enthalten ist. Wir nennen G eine S'-Gruppe, falls kein Primteiler der Ordnung in S enthalten ist, wenn also G eine $(\mathbb{P} \setminus S)$-Gruppe ist. Für $p \in \mathbb{P}$ bezeichnen wir $\{p\}$-Gruppen auch einfach als p-Gruppen. Entsprechend sind p'-Gruppen zu verstehen. Ein Element $g \in G$ nennen wir ein S-Element, falls $\langle g \rangle$ eine S-Gruppe ist. Analog sind die Bezeichnungen S'-Element, p-Element und p'-Element zu lesen. Der Fall $G = e$ ist zugelassen. Eine p-Gruppe hat demnach Primpotenzordnung p^n mit $n \in \mathbb{N}$ oder ist trivial.

Wir werden später noch folgenden Satz von Frobenius benötigen, der die Existenz normaler p-Komplemente charakterisiert.

Satz 2.4. (Frobenius) *Sei G eine Gruppe und p eine Primzahl. Dann sind folgende Aussagen äquivalent:*

1. *Es gibt ein normales p-Komplement in G.*
2. *Für jede p-Gruppe $P \leq G$ ist $\frac{N_G P}{C_G P}$ eine p-Gruppe.*
3. *Für jede p-Gruppe $P \leq G$ besitzt der Normalisator $N_G P$ ein p-Komplement.*

Beweis. Gorenstein [8], S. 253, Theorem 4.5 □

Ein unverzichtbares Werkzeug ist der nach Frattini benannte Schluss über Sylowgruppen von Normalteilern. Sei K ein Normalteiler der Gruppe G und K_p eine Sylowgruppe von K. Dann ist der Normalisator $\mathrm{N}_G K_p$ ein Supplement zu K, d.h.

$$K \trianglelefteq G \quad \Longrightarrow \quad \mathrm{N}_G K_p \cdot K = G.$$

Für eine Frobeniusgruppe $G = KH$ mit Kern K bedeutet das $\mathrm{N}_G K_p \cdot K = G$. Tatsächlich werden wir sehen, dass die Sylowgruppen von K sogar Normalteiler in G sind und deswegen für jede Sylowgruppe $K_p \leq K$ bereits $\mathrm{N}_G K_p = G$ ist. Zuletzt benötigen wir noch den folgenden Satz über normale (konjugationsinvariante) Teilmengen von Sylowgruppen, er stammt wieder von Burnside.

Satz 2.5. (Burnside) *Sei G eine Gruppe, $G_p \leq G$ eine p-Sylowgruppe und $S, T \subseteq G_p$ zwei in G_p normale Teilmengen, d.h. $S^g = S$ und $T^g = T$ für alle $g \in G_p$. Dann sind S und T genau dann konjugiert in G, wenn sie in $N_G G_p$ konjugiert sind.*

Beweis. Gorenstein [8], S. 240, Theorem 7.11 □

2.4 Struktur von Frobeniusgruppen

Kommutatoren schreiben wir als $[a,b] = aba^{-1}b^{-1}$ und höhere Kommutatoren induktiv beginnend mit $[a,b,c] = [[a,b],c]$ in nahe liegender Weise. Weiterhin bezeichnen wir mit

$$[A,B] = \langle [a,b] \mid a, \in A, b \in B \rangle$$

die von den Kommutatoren erzeugte Untergruppe. Eine Gruppe G heißt nilpotent, wenn es eine Maximallänge nicht trivialer iterierter Kommutatoren gibt. Das ist genau dann der Fall, wenn die mengenwertige Abbildung $L : X \mapsto [X,G]$ in dem Sinne nilpotent ist, dass $L^n G = e$ für ein $n \in \mathbb{N}$. Das minimale n mit dieser Eigenschaft nennen wir die Nilpotenzklasse von G. Die Abbildung L ist monoton bezüglich der Inklusion und bei nilpotenten Gruppen endet die absteigende Zentralreihe

$$G \geq LG \geq L^2G \geq \cdots \geq L^nG = e$$

bei der trivialen Untergruppe. Da die Urbildfunktion ebenfalls monoton im selben Sinne ist, erhält man daraus die aufsteigende Zentralreihe bestehend aus den Untergruppen $Z_n = L^{-n}e$, $n \in \mathbb{N}$ mit

$$e \leq Z_1 \leq Z_2 \leq \cdots \leq Z_n = G.$$

Sie eignet sich auch zur Charakterisierung von Nilpotenz, da sie genau dann stationär wird mit $Z_n = G$, wenn für die absteigende Zentralreihe $L^nG = e$ gilt. Für nilpotente Gruppen kennt man starke strukturelle Gesetzmäßigkeiten.

Satz 2.6. *Untergruppen, Faktorgruppen und direkte Produkte endlich vieler nilpotenter Gruppen sind nilpotent. Der Normalisator einer echten Untergruppe nilpotenter Gruppen ist stets echt größer, als die Untergruppe selbst.*

Beweis. Gorenstein [8], S. 22, Theoreme 3.3, 3.4 □

Die letzte Aussage bedeutet, dass die Normalisatorbildung streng monoton auf dem Verband der echten Untergruppen ist. Indirekt folgt daraus sofort, dass Frobeniusgruppen nicht nilpotent sind, denn für ein Frobeniuskomplement H ist der Normalisator mit $\mathrm{N}_G H = H$ niemals echt größer als H. Im endlichen Fall lässt sich Nilpotenz in einer Weise charakterisieren, die der Anschauung zugänglich und für unsere Zwecke am besten geeignet ist.

Satz 2.7. *Eine endliche Gruppe ist genau dann nilpotent, wenn sie direktes Produkt ihrer Sylowgruppen ist. Insbesondere sind p-Gruppen mit $p \in \mathbb{P}$ nilpotent.*

Beweis. Gorenstein [8], S. 23, Theorem 3.5 □

J. G. Thompson bewies 1959 in seiner bahnbrechenden Dissertation mit dem selbsterklärenden Titel "A Proof that a Finite Group with a Fixed-Point-Free Automorphism of Prime Order is Nilpotent" einen Satz, mit dem sich zeigen lässt, dass Frobeniuskerne stets nilpotent sind. Bereits Frobenius äußerte eine entsprechende Vermutung, die deswegen mitunter auch als Frobenius Vermutung bezeichnet wird und für über 50 Jahre ungelöst blieb. Das Ergebnis von Thompson fand nach dem Bekanntwerden sogar Erwähnung in der New York Times. Es stand jedoch im Schatten der Widerlegung der Eulerschen Vermutung, welche der Artikel thematisierte.

Satz 2.8. (Thompson) *Besitzt eine Gruppe G einen fixpunktfreien Automorphismus von Primzahlordnung, so ist G nilpotent.*

Beweis. Einen Beweis dieses Satzes findet man in einschlägiger Standardliteratur, etwa [8], S. 337, Theorem 2.1, oder in der original Publikation von Thompson [9], in der er die Ergebnisse seine Dissertation veröffentlichte. □

Im Sonderfall, dass eine Gruppe einen fixpunktfreie Automorphismus von Ordnung 2 besitzt, lässt sich sogar schließen, dass die Gruppe kommutativ ist. Diese Aussage werden wir später kurz benötigen.

Satz 2.9. *Besitzt eine Gruppe G einen fixpunktfreien Automorphismus der Ordnung 2, so ist G eine abelsche Gruppe.*

Beweis. Gorenstein [8], S. 336, Theorem 1.4 □

Wir betrachten nun wieder eine Frobeniusgruppe $G = KH$ mit Kern K und Komplement H. Als Normalteiler ist der Frobeniuskern K invariant gegenüber inneren Automorphismen. Wählt man also ein Element $g \in H$ von Primzahlordnung, so ist die Konjugation $x \mapsto gxg^{-1}$ ein fixpunktfreier Automorphismus von Primzahlordnung auf K. Aus dem Satz von Thompson folgt damit die Vermutung von Frobenius.

Korollar 2.2. *Sei $G = KH$ eine Frobeniusgruppe mit Kern K und Komplement H. Dann ist K nilpotent.*

Als unmittelbare Konsequenz aus der Vermutung von Frobenius können wir nun die Sätze 2.6 und 2.7 auf den Frobeniuskern anwenden. Damit erhalten wir teilweise als direkte Folgerung das

Korollar 2.3. *Sei $G = KH$ eine Frobeniusgruppe mit Kern K und Komplement H. Dann gelten:*

1. *K ist direktes Produkt seiner Sylowgruppen, ebenso alle Untergruppen und Faktorgruppen von K.*
2. *Für Untergruppen $U < K$ gilt $U < N_K U$.*
3. *Die Sylowgruppen K_p sind invariant gegenüber Automorphismen, insbesondere gibt es zu einer Primzahl höchstens eine Sylowgruppe und es gilt $K_p \lhd G$.*

Beweis. Es muss nur die dritte Aussage gezeigt werden, da die ersten beiden sich als direkte Folgerungen aus den Sätzen 2.6 und 2.7 ergeben.

Als Faktor im direkten Produkt $K = \bigotimes_\nu K_\nu$ enthält eine Sylowgruppe K_p alle p-Elemente. Da die Automorphismen von K die Ordnung nicht antasten, sind die Sylowgruppen invariant. Insbesondere sind sie invariant gegenüber Konjugation mit Elemente aus ganz G, sie sind also Normalteiler. □

Aus den genannten Eigenschaften von K können wir nunmehr auf wichtige strukturelle Merkmale der Komplemente schließen. H ist demnach auch eine Gruppe fixpunktfreier Automorphismen auf den einzelnen Sylowgruppen von K. Sei p ein Primteiler der Ordnung von K und K_p die eindeutige p-Sylowgruppe. Dann ist K_pH wieder eine Frobeniusgruppe. Ist weiterhin q ein Primteiler von H und H_q eine Sylowgruppe, so ist K_pH_q ebenfalls eine Frobeniusgruppe. Allgemeiner operiert jede Untergruppe von H fixpunktfrei auf K_p. Fixpunktfreie Automorphismengruppen nennt man auch regulär. H und seine Untergruppen sind demnach reguläre Automorphismengruppen einer p-Gruppe für jeden Primteiler p der Ordnung von K. Für solche Gruppen gelten wiederum die folgenden Sätze.

Satz 2.10. *Sei G eine reguläre Automorphismengruppe einer r-Gruppe, $r \in \mathbb{P}$ und p, q Primteiler der Ordnung von G. Dann gelten*

1. *Die Ordnung von G ist teilerfremd zu r.*
2. *Alle abelschen Untergruppen von G sind zyklisch.*
3. *Untergruppen der Ordnung pq sind zyklisch.* *(pq-Bedingung)*

Beweis. Gorenstein [8], S. 187, Theorem 3.14 □

Die erste Aussage von Satze 2.10 besagt, dass reguläre Automorphismengruppen von p-Gruppen stets p'-Gruppen sind. Auf die dritte Eigenschaft verweisen wir, wenn im Folgenden der Begriff pq-Bedingung fällt. Für p-Gruppen, welche die zweite der drei im Satz 2.10 gefolgerten Eigenschaften erfüllen, existieren nur wenige Isomorphietypen, die alle bekannt sind. Der folgende Satz berücksichtigt auch den allgemeineren Fall, dass lediglich alle abelschen Normalteiler zyklisch sind.

Satz 2.11. *Sei $p \in \mathbb{P}$ und G eine nicht triviale p-Gruppe, in der alle abelschen Normalteiler zyklisch sind. Dann sind nur folgende Isomorphietypen von G möglich:*

1. *$p \geq 2$ und $G \approx C_{p^n}$, $n \in \mathbb{N}$* *(Drehgruppe)*
2. *$p = 2$ und $G \approx D_{2^n}$, $n \in \mathbb{N}$, $n \geq 2$* *(Diedergruppe)*
3. *$p = 2$ und $G \approx Q_{2^n}$, $n \in \mathbb{N}$, $n \geq 4$* *(verallgemeinerte Quaternionengruppe)*
4. *$p = 2$ und $G \approx SD_{2^n}$, $n \in \mathbb{N}$, $n \geq 2$* *(Semidiedergruppe)*

Sind sogar alle abelschen Untergruppen zyklisch, so treten der zweite und dritte Fall nicht auf, d.h. G ist entweder zyklisch oder $p = 2$ mit $G \approx Q_{2^n}$, $n \geq 4$.

Beweis. Gorenstein [8], S. 199, Theorem 4.10 □

Als unmittelbare Folgerung aus der letzten, zusätzlichen Aussage folgt sofort das nächste

Korollar 2.4. *Sei $p > 2$ eine ungerade Primzahl und G eine nicht triviale p-Gruppe, in der alle abelschen Untergruppen von zyklisch sind. Dann ist G ebenfalls zyklisch. Ist hingegen G eine nicht zyklische 2-Gruppe mit nämlicher Eigenschaft, so ist G eine verallgemeinerte Quaternionengruppe.*

Auf die in Satz 2.11 genannten Isomorphietypen gehen wir der Vollständigkeit halber in Kürze nocheinmal ein und geben Konstruktionen dieser Gruppen durch Erzeuger und Relationen. Zunächst soll aber der Satz auf die Frobeniuskomplemente und alle ihre Untergruppen, insbesondere die p-Sylowgruppen, angewendet werden. Als Folgerung aus den Sätzen 2.10 und 2.11 können wir für Frobeniuskomplemente die wenigen möglichen Isomorphietypen der Sylowgruppen und aller Untergruppen deren Ordnung ein Produkt zweier Primzahlen sind, angeben.

Korollar 2.5. *Sei $G = KH$ eine Frobeniusgruppe mit Kern K und Komplement H. Für Primteiler p, q der Ordnung von H gilt dann:*

1. *Untergruppen von H mit der Ordnung pq sind zyklisch.* *(pq-Bedingung)*

2. *Für $p = 2$ sind alle p-Sylowgruppen von H zyklisch oder verallgemeinerte Quaternionengruppen.*

3. *Für $p > 2$ sind alle p-Sylowgruppen von H zyklisch.*

Beweis. Da H als reguläre Automorphismengruppe auf K wirkt, gilt nach Satz 2.10 die pq-Bedingung und alle abelschen Untergruppen von H sind zyklisch. Insbesondere sind dann auch alle abelschen Untergruppen der p-Sylowgruppen von H zyklisch. Nach der Zusatzaussage von Satz 2.11 folgen daher die letzten beiden Aussagen. □

Da Untergruppen zyklischer Gruppen wieder zyklisch sind und jede Gruppe von Primpotenzordnung in einer Sylowgruppe enthalten ist, folgt sofort

Korollar 2.6. *Sei $G = KH$ eine Frobeniusgruppe mit Kern K, Komplement H und $p > 2$ ein ungerader Primteiler der Ordnung von H. Dann ist jede p-Untergruppe von H zyklisch.*

Wir nennen eine Gruppe G perfekt, wenn sie nicht trivial ist und für ihre Kommutatorgruppe gilt $G' = LG = [G, G] = G$. Da eine Faktorgruppe genau dann kommutativ ist, wenn ihr Normalteiler die Kommutatorgruppe enthält, haben perfekte Gruppen keine kommutativen Faktorgruppen. Insbesondere sind sie daher nicht auflösbar. Ebenso können keine auflösbaren Faktorgruppen auftreten, da Faktorgruppen perfekter Gruppen wieder perfekt sind.

Nun kommen wir zum eigentlichen Thema der Arbeit. Gemäß dem folgenden und bereits erwähnten Hauptsatz ist Perfektheit eine Bedingung an Frobeniuskomplemente, unter der es für nämliche nur einen einzigen Isomorphietyp gibt.

Satz 2.12. (Hauptsatz) *Sei G eine endliche Frobeniusgruppe mit Komplement H. Ist H eine perfekte Gruppe, so folgt $H \approx SL_2(5)$.*

Zum Beweis werden wir den Hauptsatz äquivalent umformen in das bereits erwähnte $SL_2(5)$-Theorem von Zassenhaus. Der anschließende Beweis des $SL_2(5)$-Theorems in den nächsten Abschnitten begründet den Großteilteil dieser Diplomarbeit. Dabei folgen wir im Wesentlichen der Argumentation von Meierfrankenfeld in [4].

2.5 Das $SL_2(5)$ Theorem

Die Arbeit von Zassenhaus [2] 1934 hatte die Klassifikation endlicher Fastkörper zum Ziel. Die Bestimmung perfekter Frobeniuskomplemente mit dem $SL_2(5)$-Theorem war

keinesfalls das Hauptanliegen. Auch ist die Darstellung für heutige Leser etwas mühsam nachzuvollziehen. Wir zitieren den Satz daher aus seiner sehr viel spätere Publikation [3] von 1985, in der er das S$L_2\,(5)$-Theorem in den Mittelpunkt gestellt hat. Dort wird es wie folgt angegeben.

Satz 2.13. (Zassenhaus, 1985) *Ist G eine perfekte, irreduzible, endliche Matrizengruppe vom Grad $d > 1$ über den komplexen Zahlen $\mathbb{C}$ derart, dass kein Element $\neq I_d$ den Eigenwert 1 hat, dann ist $d = 2$ und $G \approx SL_2\,(5)$.*

Die Formulierung ist den charaktertheoretischen Methoden angemessen. Da aber unser Anliegen deren Vermeidung ist, wollen wir es allgemeiner formulieren. Beschränken wir uns nicht auf die komplexen Zahlen und fordern auch nicht die Irreduzibilität der Darstellung, so kommt man zum folgenden Satz, dessen Äquivalenz zum Hauptsatz hier bewiesen werden soll.

Satz 2.14. (S$L_2\,(5)$-Theorem) *Sei $\mathbb{K}$ ein Körper und V ein Vektorraum über $\mathbb{K}$. Ist dann $H \leq AutV$ eine perfekte Gruppe fixpunktfreier Vektorraumautomorphismen, so folgt $H \approx SL_2\,(5)$.*

Auf den ersten Blick scheint ein anderer Sachverhalt vorzuliegen, als beim Hauptsatz 2.12. Um die Äquivalenz der beiden Varianten des Hauptsatzes zu zeigen, benötigen wir noch einige Begriffe, die hier zusammen mit anderen, später gebrauchten Definitionen zusammengetragen werden sollen.

Ein Normalteiler N in einer Gruppe G zeichnet sich dadurch aus, dass G durch Konjugation auf N operiert, also $G \to \mathrm{Aut}N$. Der Zentralisator $\mathrm{C}_N G$ besteht dann gerade aus allen $h \in N$, die von jedem $g \in G$ fixiert werden. Zu $g \in G$ und $n \in N$ gibt der Kommutator $[g, n] = gng^{-1}n^{-1}$ gerade den qualitativen Unterschied zwischen n und gng^{-1} in dem Sinne an, als dass es sich hierbei um dasjenige Element handelt, mit welchem man n von links multipliziert, um gng^{-1} zu erhalten.

Diese Interpretation motiviert eine allgemeinere Definition dieser Begriffe für beliebige Gruppenoperationen der Form $G \to \mathrm{Aut}H$, wobei G und H nun beliebige Gruppen sein können. Mit $\mathrm{C}_H G$ bezeichnen wir dann die Menge aller Fixpunkte von G in H, also

$$\mathrm{C}_H G = \{x \in H \mid Gx = x\}$$

und zu $g \in G$ und $h \in H$ ist der Kommutator

$$[g, h] = gh \cdot h^{-1}$$

gerade dasjenige Element aus H, mit welchem man h von links multipliziert, um gh zu erhalten. Entsprechend ist die Kommutatorgruppe $[G, H]$ als Erzeugnis aller Kommutatoren definiert. Den Begriff Normalteiler verschärft man zur charakteristischen Untergruppe. Damit meinen wir eine Untergruppe $N \leq H$ mit $\varphi N \leq N$ für alle Automorphismen $\varphi \in \mathrm{Aut}H$. Ist N charakteristisch in H, so schreiben wir N char H. Charakteristische Untergruppen sind insbesondere Normalteiler und es gilt stets

$$A \text{ char } B \trianglelefteq C \quad \Longrightarrow \quad A \trianglelefteq C.$$

Kehren wir zurück zu einer Frobeniusgruppe $G = KH$ mit Kern K und Komplement H. Mit genannten Begriffen können wir nun sagen, dass zu jedem Primteiler p der Ordnung von K die Sylowgruppe K_p charakteristisch in K ist, also K_p char K. Die Suche nach ebenfalls charakteristische Untergruppen von K_p führt zur allgemeinen Betrachtung charakteristischer Untergruppen von p-Gruppen.

Wichtige Typen von Untergruppen in p-Gruppen sind die Erzeugnisse aller Elemente von bestimmter, vorgegebener Ordnung. Da Automorphismen die Ordnung eines Elementes nicht antasten, sind diese Untergruppen charakteristisch. Ist G eine p-Gruppe und $n \in \mathbb{N}$, so bezeichnen wir mit

$$\Omega_n G = \langle g \in G \mid |g| \leq p^n \rangle$$

das Erzeugnis aller Elemente, deren Ordnung kleiner oder gleich p^n ist und mit

$$\mho^n G = \langle g \in G \mid |g| = p^n \rangle$$

das Erzeugnis aller p^n-Elemente. Wenn G sogar eine abelsche Gruppe ist, stellt sich die Lage sehr übersichtlich da. Gemäß dem Klassifikationssatz für endlich erzeugte abelsche Gruppen sind diese Isomorph zu einem direkten Produkt zyklischer Gruppen. Insbesondere sind also abelsche p-Gruppen direkte Produkte zyklischer p-Gruppen. Sind die Ordnungen aller direkten Faktoren untereinander gleich, so nennen wir die Gruppe homozyklisch. Falls alle Faktoren isomorph zu C_p sind, nennen wir die Gruppe elementar abelsch. Elementar abelsche p-Gruppen sind somit isomorph zu einem Vektorraum $C_p^n \approx \mathbb{Z}_p^n$ über $\mathbb{Z}_p$. Für eine abelsche p-Gruppe G ist $\Omega_1 G$ stets eine elementar abelsche Gruppe und damit als Vektorraum über $\mathbb{Z}_p$ zu begreifen.

Für den späteren Gebrauch hilfreich sind folgenden Notationskonventionen für spezielle charakteristische Untergruppen einer beliebigen Gruppe G. Wir schreiben

- $\mathrm{O}_p G$ für den größten p-Normalteiler in G,

- $\mathrm{O}G$ für den größten ungeraden Normalteiler und
- O^pG für den kleinsten Normalteiler mit p-Potenzindex.

O^pG ist der kleinste Normalteiler in G, der alle p'-Elemente enthält, hingegen ist $\mathrm{O}G$ der von allen ungeraden Elementen erzeugte Normalteiler. Im Falle des Frobeniuskerns ist O_pK identisch mit der Sylowgruppe K_p. Für eine abelsche Gruppen G gilt stets $G = \mathrm{O}_2G \cdot \mathrm{O}G$.

Wir beweisen nun die Äquivalenz der Sätze 2.12 und 2.14. Zunächst zeigen wir, wie aus dem Hauptsatz das $\mathrm{S}L_2\,(5)$-Theorem folgt. Gelte also der Hauptsatz, sei V ein Vektorraum über einem Körper $\mathbb{K}$ und H eine perfekte Gruppe fixpunktfreier Vektorraumautomorphismen von V. Definieren wir nur $G = V \rtimes H$, so folgt aus Satz 2.2 sofort, dass G eine Frobeniusgruppe mit perfektem Komplement $\{e\} \times H$ und $V \times \{e\}$ als Kern ist. Mithin nach Satz 2.12 folgt $H \approx \mathrm{S}L_2\,(5)$.

Die Rückimplikation ist etwas schwieriger. Gelte also Satz 2.14 und sei $G = KH$ eine Frobeniusgruppe mit perfektem Komplement H und Kern K. Da K nach Satz 2.2 nilpotent ist, lässt es sich gemäß Satz 2.6 als direktes Produkt seiner Sylowgruppen schreiben, welche charakteristisch und damit insbesondere Normalteiler sind.

Sei nun p ein Primteiler der Ordnung von K und K_p die zugehörige eindeutige p-Sylowgruppe. Das Zentrum einer nicht trivialen p-Gruppe ist niemals trivial, darum haben wir mit $\mathrm{Z}K_p \neq e$ eine nicht triviale, abelsche p-Gruppe und $V = \Omega_1\mathrm{Z}K_p$ ist eine elementar abelsche Untergruppe. Wir haben nun

$$V \text{ char } \mathrm{Z}K_p \text{ char } K_p \lhd G$$

und schließen daraus $V \lhd G$. Demnach operiert H auf V durch Konjugation als fixpunktfreie Automorphismengruppe. V ist aber auch ein Vektorraum über $\mathbb{Z}_p$ und damit Modul über dem Gruppenring $\mathbb{Z}_pH$, vermöge der Operation

$$\left(\sum k_h h\right) v = \sum k_h \left(hvh^{-1}\right).$$

Damit sind alle Voraussetzungen von Satz 2.14 erfüllt und wir können $H \approx \mathrm{S}L_2\,(5)$ und somit auf die Gültigkeit von Satz 2.12 schließen.

Anders als beim der ersten Beweisrichtung haben wir bei der Argumentation die bekannte Struktur des Frobeniuskomplements K massiv ausgenutzt. Die Erkenntnis darüber haben wir wiederum aus dem Satz von Frobenius erhalten, dessen Beweis nicht charakterfrei ist. Hierin liegt beim Beweis des Hauptsatzes die einzige implizite Anwendung

von Charaktertheorie. Der nachfolgende Beweis des S$L_2(5)$-Theorems und damit des Hauptsatzes ist hingegen vollständig charakterfrei. Zu seiner Durchführung werden ausführliche Vorbereitungen nötig, die in einer langen Sequenz von Hilfssätzen im nächsten Hauptabschnitt entwickelt werden.

3 Vorbereitungen zum Beweis des S$L_2\,(5)$-Theorems

Die Vorbereitungen, die für den Beweis des S$L_2\,(5)$-Theorems nötig werden, erscheinen ohne vorauseilende Erläuterungen vollkommen zusammenhanglos nebeneinander zu stehen. Um also das Vorgehen in diesem Abschnitt nicht allzu willkürlich erscheinen zu lassen, soll hier die Beweisidee erläutert und der Beweis grob skizziert werden, bevor wir die dafür nötigen Details ausformulieren. Wir gehen aus von einem Vektorraum V über einem Körper $\mathbb{K}$ und betrachten eine perfekte Gruppe fixpunktfreier Vektorraumautomorphismen $\mathcal{G} \leq \mathrm{Aut}V$. Wir wollen den Isomorphietyp von $\mathcal{G}$ bestimmen.

Auf der Suche nach dem Isomorphietyp einer gegebenen Gruppe wird man zunächst versuchen, die Gruppenordnung festzustellen. Sind die Ordnung und ihre Primfaktorzerlegung erst einmal bekannt, erschließt sich durch die reichhaltig verfügbaren gruppentheoretischen Sätze - allen voran die Sätze von Sylow - eine Vielzahl an Informationen über Untergruppen, Faktorgruppen, Normalteiler und deren Isomorphietypen. Oftmals reichen diese Informationen bereits aus, um den Isomorphietyp auf wenige mögliche Fälle einzugrenzen, die man dann in Fallunterscheidungen isoliert voneinander betrachten kann. Unser erklärtes Ziel wird also sein, die Ordnung von $\mathcal{G}$ zu bestimmen.

Ist die Ordnung einer Gruppe klein genug, so lassen sich viele gruppentheoretische Probleme algorithmisch oder durch systematisches Ausprobieren aller möglichen Fälle computergestützt lösen. Mit verschiedensten Methoden sind die möglichen Isomorphietypen zu vielen kleinen Ordnungen bestimmt worden. Im Rahmen des Projekts “Small Group Library” haben Bettina Eick, Eamonn O’Brien und Hans Ulrich Besche die Gruppen bishin zur Ordnung 2000 mit wenigen Ausnahmen katalogisiert und in den Computeralgebrasystemen GAP und MAGMA implementiert, so dass von dort aus auf den Katalog zugegriffen werden kann. Wir wollen GAP einsetzen, um unsere Vorgehensweise zu motivieren und um den Beweis für eine Teilaussage computergestützt zu lösen, den Meierfrankenfeld mit einem Verweis auf Darstellungsgruppen im Sinne von Schur nur angedeutet hat. Die Syntax der verwendeten Befehle sind zumeist intuitiv und bedürfen keinerlei Erläuterungen.

3.1 Die Beweisidee

Wir befinden uns in der glücklichen Lage, die Antwort auf das Klassifikationsproblem perfekter Frobeniuskomplemente bereits zu kennen. Wir können also den Gaul von hinten aufzäumen und die Ordnung eines perfekten Frobeniuskomplements einfach in GAP abfragen.

```
gap> Order(SL(2,5));
120
```

Die Ordnung der $\mathrm{S}L_2(5)$ ist also gerade 120 und somit zweifelsfrei in Reichweite der in GAP katalogisierten Gruppen. Die Möglichkeiten von GAP sind verlockend, dennoch sollen sie nicht überstrapaziert werden und nach Möglichkeit strukturelle Argumente bevorzugt werden. Für die genannte Gruppenordnung sei auf den später aus [8] zitierten Satz 3.2 verwiesen, der dieses leistet. Als vertrauensbildende Maßnahme können wir und nun davon überzeugen, dass die $\mathrm{S}L_2(5)$ tatsächlich perfekt ist.

```
gap> IsPerfect(SL(2,5));
true
```

In der Tat sind perfekte Gruppen kleiner Ordnung nicht besonders zahlreich, vielmehr ist Perfektheit ein starkes strukturelles Merkmal, welches nur wenige Isomorphietypen zulässt. Auch hiervon kann man sich leicht überzeugen. Wir erzeugen Listen $L60$ und $L120$ bestehend jeweils aus allen Gruppen der Ordnung 60 und 120.

```
gap> L60:=AllSmallGroups(60);;
gap> L120:=AllSmallGroups(120);;
```

Nun können wir Informationen der Listen elementweise abfragen. Wir bestimmen etwa die Isomorphietypen in $L60$.

```
gap> List(L60,StructureDescription);
[ "C5 x (C3 : C4)", "C3 x (C5 : C4)", "C15 : C4", "C60", "A5",
  "C3 x (C5 : C4)", "C15 : C4", "S3 x D10", "C5 x A4",
  "C6 x D10", "C10 x S3", "D60", "C30 x C2" ]
```

Aus nahe liegenden Gründen verzichten wir darauf, die Isomorphietypen in $L120$ abzufragen. Für unsere Zwecke sind sie ohnehin nicht von Belangen. Wir wollen nur wissen, wieviele derer perfekt sind, was wir mit den folgenden Listenbefehlen abfragen.

```
gap> List(L60,IsPerfect);
[ false, false, false, false, true,  false, false,... , false ]
gap> List(L120,IsPerfect);
[ false, false, false, false, true,  false, false,... , false ]
```

Die Ausgabe zeigt uns, dass zu den Ordnungen 60 und 120 jeweils das fünfte Listenelement die einzige perfekte Gruppe ist. Wir wissen bereits, das jene der Ordnung 120

isomorph zur $\mathrm{S}L_2(5)$ ist. Wir fragen die Isomorphietypen ab, um uns davon zu überzeugen.

```
gap> StructureDescription(L60[5]);
"A5"
gap> StructureDescription(L120[5]);
"SL(2,5)"
```

Mithin kennen wir mit A_5 nun auch den Isomorphietyp der einzigen perfekten Gruppe der Ordnung 60. Zuletzt finden wir mit

```
gap> StructureDescription(Center(SL(2,5)));
"C2"
```

das Zentrum $\mathrm{Z}SL_2(5) \approx C_2$ und demnach für die ebenfalls perfekte Zentrumsfaktorgruppe $\left|\frac{\mathrm{S}L_2(5)}{\mathrm{Z}SL_2(5)}\right| = 60$ und damit die Isomorphie $\frac{\mathrm{S}L_2(5)}{\mathrm{Z}SL_2(5)} \approx A_5$. Insgesamt merken wir uns also

Korollar 3.1. *Die $SL_2(5)$ ist die einzige perfekte Gruppe der Ordnungen* 120 *und die Zentrumsfaktorgruppe $\frac{SL_2(5)}{ZSL_2(5)} \approx A_5$ ist die einzige von Ordnung* 60.

Auf die Ergebnisse des Katalogprojektes zurückgreifend ist unser Klassifikationsproblem also durch die Bestimmung der Ordnung von $\mathcal{G}$ bereits gelöst. Nicht vergessen sollte man dabei jedoch, dass viele Jahre mühevoller Arbeit ist die Katalogisierung kleiner Gruppen geflossen sind und dass strukturelle Argumente für die daraus entnommenen Informationen auch bei den hier betrachteten sehr kleinen Ordnungen oftmals nur mit sehr trickreichen Schlüssen und Anwendung komplizierter Sätze gelingen. In diesem Fall steht aber außer Frage, dass die entsprechenden Beweise an geeigneter Stelle bereits erbracht worden sind, so dass wir die Ausgabe von GAP als verlässlich und Korollar 3.1 als bewiesen ansehen dürfen. Ziel wird also von nun an sein, die Ordnung von $\mathcal{G}$ zu bestimmen.

Beweisskizze Da $\mathcal{G}$ ein perfektes Frobeniuskomplement ist, erfüllt es die drei in Korollar 2.5 angegebenen Eigenschaften.

- Die 2-Sylowgruppen sind zyklisch oder verallgemeinerte Quaternionengruppen.
- Untergruppen der Ordnung pq mit zweie Primzahlen p und q sind zyklisch.
- Sylowgruppen von ungerader Ordnung sind zyklisch.

Diese Eigenschaften werden bei der Bestimmung der Ordnung die entscheidende Rolle spielen. Mit ihnen werden wir zunächst einige Teilbarkeitsaussagen über die Ordnung treffen, allen voran, ob sie gerade oder ungerade ist. Es wird sich zeigen, dass die Ordnung von $\mathcal{G}$ gerade ist, und dass es in $\mathcal{G}$ eine eindeutige Involution t gibt. Wir beweisen dann, dass t im Zentrum von $\mathcal{G}$ liegt, also haben wir mit $\langle t \rangle$ ein Normalteiler von $\mathcal{G}$. Ist dann $\overline{\mathcal{G}} = \frac{\mathcal{G}}{\langle t \rangle}$ die von $\langle t \rangle$ induzierte Faktorgruppe, so ist nach Lemma 3.1 der Beweis bereits fertig, wenn wir zeigen können, dass $\overline{\mathcal{G}}$ die Ordnung 60 besitzt. Genau so werden wir vorgehen.

Als Faktorgruppe einer perfekten Gruppe ist $\overline{\mathcal{G}}$ ebenfalls perfekt. Um die Ordnung von $\overline{\mathcal{G}}$ zu bestimmen werden wir zeigen, dass $\overline{\mathcal{G}}$ die folgenden drei Eigenschaften von $\mathcal{G}$ erbt.

- Alle 2-Sylowgruppen von $\overline{\mathcal{G}}$ sind zyklisch oder Diedergruppen.
- Alle Untergruppen von $\overline{\mathcal{G}}$, deren Ordnung das Produkt pq zweier ungerader Primzahlen p, q ist, sind zyklisch.
- Alle Sylowgruppen von ungerader Ordnung sind zyklisch.

Die Untersuchung von $\overline{\mathcal{G}}$ werden wir vom Beweis isolieren und in diesem Hauptabschnitt vorgezogen betrachten. Wir gehen also in umgekehrter Reihenfolge vor. In Abschnitt 3.4 werden wir daher eine perfekte Gruppe $\mathfrak{G}$ mit den drei zuletzt genannten Eigenschaften betrachten und eine hinreichende Bedingungen angeben, um bei einer Zählung $|\mathfrak{G}| = 60$ und damit $\mathfrak{G} \approx A_5$ zu schließen. Später übertragen wir die Ergebnisse dann auf $\overline{\mathcal{G}} \approx \mathfrak{G}$ und nach Lemma 3.1 schließen wir dann $\mathcal{G} \approx \mathrm{S}L_2(5)$. Entscheidend hierfür wird die Beobachtung sein, dass $\mathfrak{G}$ und damit auch $\overline{\mathcal{G}}$ eine zu A_4 isomorphe Untergruppe besitzt. Damit können wir zeigen, dass deren kanonisches Urbild in $\mathcal{G}$ eine zu $\mathrm{S}L_2(3)$ isomorphe Untergruppe ist, die eine Quaternionengruppe $Q_8 \hookrightarrow \mathrm{S}L_2(3)$ enthält. Diese Konstellation werden wir im Abschnitt 3.3 intensiv studieren.

3.2 Wichtige Eigenschaften bekannter Gruppen

Hilfreich für das Verständnis der nachfolgenden Argumentation ist eine gewisse Vertrautheit mit den vorkommenden Gruppen. Daher soll hier die Gelegenheit ergriffen werden, alle wichtigen Gruppen kurz vorzustellen und einige benötigte Eigenschaften zu nennen, damit diese an den entsprechenden Stellen nicht allzu sehr vom Himmel fallen. Dazu verwenden wir Konstruktionen durch Erzeuger und definierende Relationen, die nachfolgend erläutert sind.

Die Verknüpfungstafel einer endlichen Gruppen G lässt sich bereits vollständig angeben, wenn man sämtliche Produkte aus Potenzen von Elementen eines erzeugenden Systems

S kennt. Zur Kenntnis nämlicher Produkte sind oftmals nur einige wenige bekannte Relationen zwischen den Erzeugern nötig, die in Gleichungen der Form

$$g_1^{n_1} \cdots g_k^{n_k} = e \qquad g_\nu \in S, n_\nu \in \mathbb{Z}, \nu = 1, \ldots, k$$

angegeben werden können. Anschaulich werden durch die Relationen gewisse algebraischer Kompositionen der Erzeuger "neutral erklärt". Ein hinreichend großes System solcher Relationen nennen wir erzeugende Relationen. Damit hierdurch eine Gruppe vollständig charakterisiert ist, müssen sich alle Beziehungen zwischen den Erzeugern, die als Gleichungen zwischen Produkten von Potenzen der Erzeuger gegeben sind, aus den erzeugenden Relationen ableiten lassen. Ein Beispiel verdeutlicht die Idee.

Gegeben sei eine zyklische Gruppe $C_n \approx \langle x \rangle$, dann genügt die Relation $x^n = e$ als einzige erzeugende Relation. Jede Gleichung zwischen Potenzen von x lässt sich aus $x^n = e$ ableiten. Etwa folgt die Beziehung $x^{2n} = e$, die jedoch selbst keine alleinige erzeugende Relation ist, weil aus ihr die Gleichung $x^n = e$ nicht wieder zurückgewonnen werden kann.

Man kann nun umgekehrt vorgehen und Gruppen dadurch definieren, dass man ihre erzeugenden Elemente benennt und willkürlich einige Beziehungen zwischen ihnen als erzeugende Relationen erklärt. Man sieht etwa ein, dass $C_n \approx \langle x \rangle$ ist, wenn bekannt ist, dass $x^n = e$ die einzige erzeugende Relation ist. Die gängige Notation sei am genannten genannten Beispiel

$$C_n \approx \langle x \mid x^n = e \rangle$$

erläutert. Hierbei werden zunächst die Erzeuger aufgelistet und anschließend die zugehörigen Relationen. Erzeuger und ihre Relationen sind keineswegs eindeutig, nicht einmal ihre Anzahl ist festgelegt. So lässt sich etwa die zyklische Gruppe der Ordnung n auch umständlicher durch

$$C_n \approx \langle x, y \mid x^{n-1}y^{-1} = e, xy = e \rangle$$

konstruieren. Die Untersuchung durch Erzeuger und Relationen definierter Gruppen ist offensichtlich algorithmischer Natur und ihre Schwierigkeit klar erkennbar. Tatsächlich gibt es nicht einmal einen Algorithmus, der entscheiden kann, ob eine so präsentierte Gruppe endlich ist.

Eine mathematisch präzise Formulierung dieser eher intuitiven Definition von Gruppen soll hier nur angedeutet werden. Dazu konstruiert man zunächst zu einer gegebenen Menge von Erzeugern S eine freie Gruppe $\langle S \rangle$, die sich dadurch auszeichnet, dass es keine nicht trivialen Relationen zwischen den Potenzen der Elemente von S gibt. Jede Gruppe

G mit einer Erzeugermenge E von Ordnung $|E| \leq |S|$ lässt sich dann als Faktorgruppe in der freien Gruppe auffinden. Dazu sei $N \subseteq S$ eine erforderliche Menge von neutral erklärten Elemente und sei $K \trianglelefteq \langle S \rangle$ der von N erzeugte Normalteiler. Die zugehörige Faktorgruppe ist gerade die von den Relationen erzeugte Gruppe $G \approx \frac{\langle S \rangle}{K}$. Die angedeutete Konstruktion findet man ausführlicher etwa bei Serge Lang [10], S. 66.

Als einfachstes Beispiel dienen wieder die zyklischen Gruppen. Die freie Gruppe zur einelementigen Erzeugermenge $S = \{x\}$ ist gerade die additive Gruppe $\mathbb{Z}$. Jede zyklische Gruppe ist Faktorgruppe in $\mathbb{Z}$. Die erzeugende Relation $nx = 0$ erklärt alle Vielfachen von nx zur Null. So kann man schließlich die bekannte Beziehung

$$C_n \approx \langle x \mid nx = 0 \rangle \approx \frac{\mathbb{Z}}{n\mathbb{Z}}$$

wieder zurückgewinnen. Oft werden wir die Relationen nicht direkt in der Neutralform $g_1^{n_1} \cdots g_k^{n_k} = e$ nennen, sondern eine äquivalente Gleichung angeben.

Es sollen nun die Isomorphietypen aus Satz 2.11 noch einmal kurz beleuchtet werden, da sie eine tragende Rolle im Beweis einnehmen. Zu $n \in \mathbb{N}$ definieren wir eine Folge endlicher Gruppen mit zwei Erzeugen durch

$$D_{2n} = \left\langle x, y \mid x^n = y^2 = e, yxy^{-1} = x^{-1} \right\rangle \approx \langle x \rangle \rtimes \langle y \rangle \approx C_n \rtimes C_2.$$

Für $n \geq 3$ ist D_{2n} gerade eine Diedergruppe bestehend aus den Symmetrien eines regelmäßigen n-Ecks. Für $n = 2$ erhalten wir die Kleinsche Vierergruppe

$$D_4 \approx C_2 \rtimes C_2 \approx C_2 \times C_2,$$

für $n = 1$ ist $D_{2\cdot 1} = D_2 \approx C_2$. Der Einfachheit halber bezeichnen wir die abelschen Gruppen D_2 und D_4 auch als Diedergruppen, obwohl sie nicht im selben Sinne geometrisch interpretiert werden können. Für die Ordnung gilt $|D_{2n}| = 2n$. Als semidirektes Produkt zyklischer Gruppen ist D_{2n} auflösbar für alle $n \in \mathbb{N}$. Für $n \geq 3$ ist D_{2n} nicht kommutativ und wir erhalten für das Zentrum

$$\mathrm{Z}D_{2n} = \begin{cases} \langle e \rangle & \text{falls } n \text{ ungerade} \\ \left\langle x^{\frac{n}{2}} \right\rangle & \text{falls } n \text{ gerade} \end{cases}$$

und für die Kommutatorgruppe $[D_{2n}, D_{2n}] = \langle x^2 \rangle$ mit $\langle x^2 \rangle = \langle x \rangle \approx C_n$ für ungerade n.

Wir betrachten die Automorphismengruppen $\mathrm{Aut}D_{2n}$. Für $n = 1$ ist nichts weiter zu sa-

gen. Da ein Automorphismus das neutrale Element fixiert, ist für $n = 2$ ein solcher durch eine Permutation der übrigen drei Elemente bereits definiert. Tatsächlich rechnet man nach, dass $\mathrm{Aut}D_4 \approx S_3 \approx C_3 \rtimes C_2$ und damit insbesondere auflösbar ist. Für $n \geq 3$ ist die Untergruppe $\langle x \rangle \leq D_{2n}$ charakteristisch. In diesem Fall nimmt ein Automorphismus $\varphi \in \mathrm{Aut}D_{2n}$ auf den Erzeugern Funktionswerte der Form

$$\varphi x = x^k \quad \text{mit} \quad k \in \mathbb{N} \quad \text{und} \quad \mathrm{ggT}\,(k, n) = 1$$

sowie

$$\varphi y = x^m y \quad \text{mit} \quad m \in \mathbb{N}$$

an. In der Tat rechnet man leicht nach, dass der Automorphismus φ durch das Zahlenpaar (m, k) bereits festgelegt ist und umgekehrt jedes Zahlenpaar aus $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n^\times$ durch die Vorschrift

$$(a, b)\, x = x^b \qquad \text{und} \qquad (a, b)\, y = x^a y$$

eindeutig einen Automorphismus definiert. Deswegen dürfen wir hier die Identifikation $\varphi \approx (m, k)$ vornehmen. Wegen

$$(a, b)\,(m, k)\, x = x^{bk}$$

und

$$(a, b)\,(m, k)\, y = (a, b)\, x^m y = x^{bm+a} y$$

folgt

$$(a, b)\,(m, k) = (a + bm, bk)$$

und damit ist die Automorphismengruppe ein semidirektes Produkt $\mathrm{Aut}D_{2n} \approx \mathbb{Z}_n \rtimes \mathbb{Z}_n^\times$. Da die semidirekten Faktoren kommutativ sind, ist auch $\mathrm{Aut}D_{2n}$ auflösbar. Wir halten fest

Korollar 3.2. *Diedergruppen und deren Automorphismengruppen sind stets auflösbar.*

Untergruppen und Faktorgruppen von Diedergruppen sind zyklisch oder selbst wieder Diedergruppen. Ist überdies n eine gerade Zahl größer oder gleich 4, so gibt es in D_{2n} mindestens eine Untergruppen isomorph zur Kleinschen Vierergruppe D_4. Für $k, \ell \in \mathbb{N}$ mit $k - \ell = \frac{n}{2}$ ist etwa

$$\mathrm{Z}D_{2n} = \left\langle x^{\frac{n}{2}} \right\rangle < \left\langle x^k y, x^\ell y \right\rangle = \left\{ e, x^{\frac{n}{2}}, x^\ell y, x^{\ell + \frac{n}{2}} y \right\} \approx D_4 \hookrightarrow D_{2n}.$$

Jede Vierergruppe enthält also das Zentrum $\mathrm{Z}D_{2n}$ und da der Zentralisator einer nicht zentralen Involution stets eine Vierergruppe ist, sind die Vierergruppen bezüglich der Inklusion maximale, abelsche Untergruppen. Der Normalisator einer Vierergruppe ist echt größer als der Zentralisator, da Konjugation mit der Vierteldrehung $x^{\frac{n}{4}}$ stets zwei nicht triviale Involutionen in einer Vierergruppe vertauscht, gemäß

$$x^{\frac{n}{4}}x^{\ell}yx^{-\frac{n}{4}} = x^{\ell+\frac{n}{4}}yx^{-\frac{n}{4}}y^{-1}y = x^{\ell+\frac{n}{4}}x^{\frac{n}{4}}y = x^{\ell+\frac{n}{2}}y.$$

Wir untersuchen die Konjugationsklassen der Vierergruppen in D_{2n}. Dazu indizieren wir sie jeweils mit der natürlichen Zahl ℓ, die sie durch

$$D_2^{\ell} = \left\{e, x^{\frac{n}{2}}, x^{\ell}y, x^{\ell+\frac{n}{2}}y\right\} \leq D_{2n}$$

charakterisiert. Die Konjugierten sind dann

$$\begin{aligned} x^k y D_2^{\ell} x^k y &= D_2^{2k-\ell} \\ x^k D_2^{\ell} x^k &= D_2^{2k+\ell} \\ y D_2^{\ell} y &= D_2^{-\ell} \end{aligned}$$

und somit ist $D_2^{2\mathbb{Z}+\ell}$ die Klasse der zu D_2^{ℓ} konjugierten Vierergruppen. Wegen $D_2^{\ell} = D_2^{\ell+\frac{n}{2}}$ gibt es für den Fall, dass $\frac{n}{2}$ gerade ist, zwei Klassen konjugierter Vierergruppen, je nach dem, ob ℓ gerade oder ungerade ist. Wir halten also fest

Korollar 3.3. *Zu $n \in 4\mathbb{Z}$ gibt es in D_{2n} zwei Klassen konjugierter Vierergruppen $D_2^{2\mathbb{Z}}$ und $D_2^{2\mathbb{Z}+1}$ und jede Vierergruppe enthält das Zentrum ZD_{2n}. Im Normalisator gibt es stets ein Element, das die beiden nicht trivialen Involutionen durch Konjugation vertauscht.*

Ist D_{2n} wie bisher, so gilt $D_{2n} = \langle x, y\rangle = \langle xy, y\rangle$ und somit wird D_{2n} auch von zwei Involutionen erzeugt. Haben wir umgekehrt eine Gruppe $G = \langle a, b\rangle$, die von zwei voneinander verschiedenen Involutionen a und b erzeugt wird, so gilt mit $x = ab$ und $y = b$ schließlich auch $G = \langle x, y\rangle$. Wegen $yxy = babb = ba = (ab)^{-1} = x^{-1}$ erfüllen x und y die erzeugenden Relationen für die Diedergruppe $D_{2|x|}$. Wegen zusätzlich möglicher Relationen können wir nicht $G \approx D_{2|x|}$ schließen. Allerdings ist G zumindest eine Faktorgruppe von $D_{2|x|}$ und daher zyklisch oder selbst wieder eine Diedergruppe. Da wir $a \neq b$ angenommen haben, folgt $x \neq y$. Daher kann G nicht zyklisch sein und ist somit eine Diedergruppe.

Korollar 3.4. *Das Erzeugnis zweier voneinander verschiedener Involutionen ist stets eine Diedergruppe.*

Eine weitere Serie von Gruppen, die im Satz 2.11 genannt wurde, sind die Semidiedergruppen SD_n mit $n \in \mathbb{N}$. Sie sind durch

$$SD_n \approx \left\langle x, y \mid x^{2^{n-1}} = y^2 = e, y^{-1}xy = x^{2^{n-2}-1} \right\rangle$$

definiert und entziehen sich einer einfachen Anschauung. Da sie für den kommenden Beweis keine Rolle spielen, haben wir sie nur der Vollständigkeit halber genannt. Wichtig hingegen sind die verallgemeinerten Quaternionengruppen Q_{2^n}. Sie nehmen in unserer Argumentation eine Schlüsselposition ein, deshalb werden wir sie im nächsten Unterabschnitt gesondert untersuchen. In diesem Zusammenhang wird eine weitere Klasse von Gruppen angegeben, die metazyklischen Gruppen

$$\langle h \rangle \rtimes \langle k \rangle \approx C_{2n} \rtimes C_4 \approx \left\langle h, k \mid h^{2^n} = k^4 = e, khk^{-1} = h^{-1} \right\rangle.$$

Aus ihnen werden wir im nächsten Unterabschnitt die verallgemeinerten Quaternionengruppen als Faktorgruppen gewinnen.

Für die $\mathrm{S}L_2(5)$ gibt Zassenhaus in [3] neben einer komplexen Matrizendarstellung ebenfalls erzeugende Relationen an. Demnach erzeugen die beiden Matrizen

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \text{und} \qquad B = \begin{pmatrix} \frac{1}{2} + \frac{1+\sqrt{5}}{4}i & \frac{\sqrt{5}-1}{4} \\ \frac{1-\sqrt{5}}{4} & \frac{1}{2} - \frac{1+\sqrt{5}}{4}i \end{pmatrix}$$

eine Untergruppe in $\mathrm{S}L_2\mathbb{C}$, die isomorph zur $\mathrm{S}L_2(5)$ ist und mit den erzeugenden Relationen

$$\mathrm{S}L_2(5) \approx \left\langle A, B \mid A^2 = B^3 = (AB)^5 \right\rangle$$

definiert werden kann.

Kleine Gruppen und Ausnahmeisomorphismen

Zu jeder Primzahlpotenz $q = p^n$ gibt es einen Körper $\mathbb{F}_q$ mit q Elementen. Die zu den Primpotenzen gehörenden Matrizengruppen $\mathrm{G}L_2(q)$ und $\mathrm{S}L_2(q)$ mit Einträgen aus dem Körper $\mathbb{F}_q$ gehören wohl zu den am intensivsten untersuchten Objekten der Gruppentheorie. Auch hier werden sie eine dominante Rolle einnehmen. Elementare Rechnungen

zeigen, dass das Zentrum der $\mathrm{G}L_2(q)$ gerade aus den Skalarmatrizen der Form

$$\mathrm{Z}GL_2(q) = \{\left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right) \mid x \in \mathbb{F}_q\}$$

und das Zentrum von $\mathrm{S}L_2(q)$ nur aus den beiden Matrizen

$$\mathrm{Z}SL_2(q) = \left\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\right\}$$

besteht. Die Faktorgruppen

$$\mathrm{P}GL_2(q) \approx \frac{\mathrm{G}L_2(q)}{\mathrm{Z}GL_2(q)} \quad \text{und} \quad \mathrm{P}SL_2(q) \approx \frac{\mathrm{S}L_2(q)}{\mathrm{Z}SL_2(q)}$$

werden als projektive bzw. spezielle projektive lineare Gruppe bezeichnet. Neben der $\mathrm{S}L_2(5)$ wird auch die $\mathrm{S}L_2(3)$ eine entscheidende Rolle spielen. Bei ihrer Untersuchung helfen wird das sporadische Auftreten von Ausnahmeisomorphismen, die sich nicht in ein Muster bekannter Serien von Automorphismen einordnen lassen. Für uns von Bedeutung sind die Erscheinungen

$$\mathrm{P}SL_2(3) \approx A_4 \quad \text{und} \quad \mathrm{P}SL_2(5) \approx A_5,$$

deren Beweise wir hier nicht führen wollen. Sie sind gern gewähltes Thema für Übungsaufgaben, hier begnügen wir uns mit einem Verweis auf die Bibliothekfunktion von GAP und wollen statt dessen andere Eigenschaften der Gruppen A_4, A_5 und S_4 beleuchten.

Dank der übersichtlichen Zykelnotation lassen sich Aussagen über nämliche Gruppen durch direkte Angabe der Elemente treffen. So findet man etwa, dass es in der A_4 genau einen nicht trivialen Normalteiler gibt. Dieser ist isomorph zur Kleinsche Vierergruppe $D_4 \hookrightarrow A_4$ und besteht aus allen Doppeltranspositionen der Form $(a,b)(c,d)$. Die A_4 ist in A_5 enthalten, allerdings gibt es in A_5 bekanntlich keine echten, nicht trivialen Normalteiler. Beim Beweis der Einfachheit von A_5 wichtig ist die Beobachtung, dass alle alternierenden Gruppen A_n für $n \geq 3$ von den Dreizykeln erzeugt werden.

In A_4 und A_5 sind alle Involutionen Doppeltranspositionen. In der S_4 treten zusätzlich einzelne Transpositionen auf. Die Normalisatoren zweielementiger Untergruppen sind mit ihren Zentralisatoren identisch. Wir wollen zeigen, dass sie in allen drei Gruppen von Zweierpotenzordnung sind. Dazu betrachten wir

$$\begin{aligned}(12345)\,(12)\,(34)\,(54321) &= (13)\,(45)\\ (123)\,(12)\,(34)\,(321) &= (14)\,(23)\end{aligned}$$

in der A_4 respektive A_5 und

$$\begin{aligned}(123)\,(12)\,(321) &= (23)\\ (123)\,(14)\,(321) &= (24)\end{aligned}$$

in der S_4. Ohne Einschränkung haben wir damit gezeigt, dass die Normalisatoren von Involutionen keine ungeraden Elemente enthalten und folglich 2-Gruppen sind. Wir merken uns

Korollar 3.5. *In den Gruppen A_4, A_5 und S_4 werden keine Involutionen durch Elemente ungerader Ordnung normalisiert. Die Normalisatoren sind daher stets 2-Gruppen und es gilt umgekehrt, dass keine Elemente von ungerader Ordnung durch eine Involution zentralisiert werden.*

Wir betrachten noch die Normalisatoren der zu C_3 isomorphen Untergruppen von A_4. Wegen

$$(ab)\,(cd)\,(abc)\,(ab)\,(cd) = (adb)$$

und

$$(bcd)\,(abc)\,(dcb) = (acd)$$

gilt[1]

Korollar 3.6. *In A_4 sind Untergruppen der Ordnung 3 mit ihren Normalisatoren und Zentralisatoren identisch. Insbesondere wird kein Element der Ordnung 3 von durch Konjugation mit einem Element invertiert und das Zentrum ZA_4 ist trivial.*

Wir benötigen noch die Automorphismengruppe der A_4 und A_5. Hierfür zitieren wir den folgenden

[1] Die vorangegangene Begründung für das folgende Korollar ist fehlerhaft und unvollständig. Ich hatte mit der Begründung zwar angefangen aber, nachdem ich die Lösung nicht sofort gesehen hatte, aufgeschoben und später dummerweise vergessen. Bei der Korrekturlesung ist mir das auch nicht mehr aufgefallen. Ich denke, dass die Begründung nicht schwierig ist. Es sind schließlich Eigenschaften einer kleinen und gut studierten Gruppe. Ich erspare mir den Ärger, hier über diese Fußnote hinaus etwas zu schreiben. Wer diese Arbeit versteht, sollte in der Lage sein, selbst eine Begründung zu finden.

Satz 3.1. *Für $n \geq 3$ und $n \neq 6$ gilt $AutA_n \approx S_n$.*

Beweis. Suzuki [11], S. 299, (2.17) □

Die ganz erstaunliche Ausnahme für $n = 6$ hat weitreichende Folgen für die Gruppentheorie. Es gilt $\mathrm{Aut}A_6 \approx \mathrm{Aut}S_6$ und die Aufklärung der Struktur mit GAP erfordert bereits einige Minuten Rechenzeit.

```
gap> A:=AutomorphismGroup(AlternatingGroup(6));;
gap> Order(A);
1440
gap> StructureDescription(A);
"(A6 : C2) : C2"
```

Für uns ist dieser bemerkenswerte Sonderfall nicht wichtig, er wurde daher nur interessehalber erwähnt.

3.3 Die Quaternionengruppe in der S$L_2(3)$

Die Bedeutung der verallgemeinerten Quaternionengruppen lässt sich aus dem folgenden Satz ableiten, der wesentliche Eigenschaften zweidimensionaler spezieller linearer Gruppen S$L_2(q)$ über endlichen Körpern $\mathbb{F}_q$ wiedergibt.

Satz 3.2. *Es gilt $|SL_2(q)| = \left(q^2-1\right)q$ und für ungerade q sind die 2-Sylowgruppen von $SL_2(q)$ stets verallgemeinerte Quaternionengruppen. Das Zentrum dieser besteht nur aus den beiden Matrizen $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ und $\left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right)$.*

Beweis. Gorenstein [8], S. 40-42, Theorem 8.1, 8.3 □

Sei $\langle h\rangle \approx C_{2^n}$ und $\langle k\rangle \approx C_4$ mit der Operation $kh = h^{-1}$. Verallgemeinerte Quaternionengruppen lassen sich dadurch konstruieren, dass man in der metazyklischen Gruppe

$$\langle h\rangle \rtimes \langle k\rangle \approx C_{2n} \rtimes C_4 \approx \left\langle h,k \mid h^{2^n} = k^4 = e, khk^{-1} = h^{-1}\right\rangle$$

die Unterscheidung zwischen den beiden Involutionen $h^{2^{n-1}}$ und k^2 "verwischt" indem man das Element $\left(h^{2^{n-1}}, k^{-2}\right) \leftrightarrow h^{2^{n-1}}k^{-2}$ zur Eins erklärt und den auf diese Weise

erzeugten Normalteiler D herausfaktorisiert. Das lässt sich durch Hinzufügen der identifizierenden Relation $h^{2^{n-1}} = k^2$ erreichen, so dass schließlich

$$Q_{2^{n+1}} \approx \frac{C_{2^n} \rtimes C_4}{D} \approx \left\langle h, k \mid h^{2^n} = k^4 = e, h^{2^{n-1}} = k^2, khk^{-1} = h^{-1} \right\rangle$$

gilt.

Man kann zeigen, dass alle kommutativen Untergruppen generalisierter Quaternionen zyklisch sind. Gemäß der letzten Aussage von Satz 2.11 sind sie als nicht zyklische Gruppen durch diese Eigenschaft sogar charakterisiert. Alle nicht zyklischen Untergruppen sind hingegen ebenfalls verallgemeinerte Quaternionengruppen. Das Zentrum von $Q_{2^{n+1}}$ besteht gerade aus der Involution $h^{2^{n-1}} = k^2$. Die Zentrumsfaktorgruppe bildet man durch Hinzunahme der Relation $h^{2^{n-1}} = k^2 = e$. Dadurch wird die bisherige Relation $h^{2^n} = k^4 = e$ redundant und wir erhalten mit

$$\frac{Q_{2^{n+1}}}{\left\langle h^{2^{n-1}} = k^2 \right\rangle} \approx D_{2^n} \approx \left\langle h, k \mid h^{2^{n-1}} = k^2 = e, khk^{-1} = h^{-1} \right\rangle$$

eine Diedergruppe. Wir fassen die Aussagen über verallgemeinerte Quaternionengruppen zusammen.

Korollar 3.7. *Untergruppen verallgemeinerter Quaternionengruppen sind zyklisch oder ebenfalls verallgemeinerte Quaternionengruppen. Die Zentrumsfaktorgruppe von Q_{2^n} ist stets eine Diedergruppe $D_{2^{n-1}}$.*

Für $n = 2$ erhält man durch die oben erwähnte Konstruktion gerade die bekannte multiplikative Untergruppe $Q_8 \approx \{\pm e, \pm i, \pm j, \pm k\}$ der Hamiltonschen Quaternionen $\mathbb{H}$. Die Zentrumsfaktorgruppe ist eine Kleinsche Vierergruppe D_4. Aus Satz 3.2 folgt, dass die Sylowgruppen sowohl von $\mathrm{S}L_2(3)$, als auch $\mathrm{S}L_2(5)$ isomorph zur nämlichen Q_8 sind. Wir wollen diesen Einzelfall weiter vertiefen und untersuchen die Q_8 näher.

Satz 3.3. *Für $Q_8 \approx \{\pm e, \pm i, \pm j, \pm k\}$ ist $-e$ die einzige Involution. Die Elemente $\pm i$, $\pm j$, $\pm k$ haben alle die Ordnung 4 und je zwei der Elemente i, j und k erzeugen die gesamte Gruppe*

$$\langle i, j \rangle = \langle i, k \rangle = \langle j, k \rangle \approx Q_8.$$

Beweis. $ij = k$, $jk = i$ und $ki = j$. □

Gruppen, in denen jede Untergruppe bereits ein Normalteiler ist, wird man erfahrungsgemäß als kommutativ vermuten. Die Quaterniongruppe Q_8 hat die ungewöhnliche Eigenschaft, dass alle Untergruppen Normalteiler sind, obwohl sie nicht kommutativ ist.

Derartige Gruppen werden Hamiltonsche Gruppen genannt. Die Quaternionengruppe ist die kleinste Hamiltonsche Gruppe, ihre Untergruppen sind $\langle e\rangle$, $\langle -e\rangle$, $\langle i\rangle$,$\langle j\rangle$ und $\langle k\rangle$.

Die gemeinhin übliche lineare Darstellung der Quaternionengruppe beruht auf zweidimensionalen komplexen Matrizen

$$Q_8 \approx \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\},$$

die den Paulimatrizen aus der Quantenmechanik ähneln. Aus Satz 3.2 folgt $|\mathrm{S}L_2(3)| = 2^3 \cdot 3$ und somit ist Q_8 als 2-Sylowgruppe in $\mathrm{S}L_2(3)$ eingebettet. Wir finden also eine alternative Darstellung gleicher Dimension, wenn wir in $\mathbb{Z}_3$ rechnen. Als angemessenes Repräsentantensystem verwenden wir $\mathbb{Z}_3 \approx \{-1, 0, 1\}$. Durch elementares Rechnen mit Matrizen findet man nun die Matrizendarstellung

$$Q_8 \approx \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}.$$

Wir sehen, dass Q_8 das Zentrum von $\mathrm{S}L_2(3)$ enthält und somit das einzige nichttriviale Zentrumselement $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ in jeder 2-Sylowgruppe von $\mathrm{S}L_2(3)$ enthalten ist. Tatsächlich ist Q_8 sogar die einzige 2-Sylowgruppe in $\mathrm{S}L_2(3)$. Das ist gleichbedeutend damit, dass Q_8 ein Normalteiler ist, was im Folgenden gezeigt werden soll.

Um zu sehen, dass Q_8 ein Normalteiler ist, zeigen wir, dass $Q_8 \setminus \mathrm{Z}SL_2(3)$ eine disjunkte Vereinigung von Konjugationsklassen ist. Aus der linearen Algebra ist bekannt, dass die Spur einer Matrix invariant gegenüber Konjugation ist. Das Urbild einer Zahl unter der Spurabbildung ist demnach eine disjunkte Vereinigung von Konjugationsklassen. Wir zeigen, dass $Q_8 \setminus \mathrm{Z}SL_2(3) = \mathrm{tr}^{-1}0$ ein Urbild unter der Spurabbildung ist.

Sei also $\varphi \in \mathrm{S}L_2(3)$ mit $\mathrm{tr}\,\varphi = 0$. Dann gilt $\varphi = \left(\begin{smallmatrix} a & c \\ b & -a \end{smallmatrix}\right)$, $a, b, c \in \mathbb{Z}_3$ und aus $\det\varphi = 1$ folgt

$$-a^2 - bc = 1 \iff a^2 = -1 - bc.$$

Für $a = \pm 1$ folgt durch elementares Rechnen in $\mathbb{Z}_3$ schließlich $bc = 1$ und somit $b = c = \pm 1$. Insgesamt also $\varphi = \left(\begin{smallmatrix} -1 & \pm 1 \\ \pm 1 & 1 \end{smallmatrix}\right)$ oder $\varphi = \left(\begin{smallmatrix} 1 & \pm 1 \\ \pm 1 & -1 \end{smallmatrix}\right)$. Für $a = 0$ folgt hingegen $bc = -1$ und somit $b = -c = \pm 1$, was wiederum $\varphi = \pm \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ impliziert. Mithin ist $Q_8 \setminus \mathrm{Z}SL_2(3) = \mathrm{tr}^{-1}0$ und da das Zentrum ein Normalteiler ist, ist auch $Q_8 = \mathrm{Z}SL_2(3) \cup \mathrm{tr}^{-1}0$ ein Normalteiler.

Die Argumentation über die Spurabbildung kann umgangen werden, indem man die kanonische Abbildung $\mathrm{S}L_2(3) \to \mathrm{P}SL_2(3)$ betrachtet und den Isomorphismus $\mathrm{P}SL_2(3) \approx A_4$

ausnutzt. Da die Kleinschen Vierergruppe D_4 isomorph zum einzigen nicht trivialen, echten Normalteiler in $A_4 \approx \mathrm{P}SL_2(3)$ ist und ihr kanonisches Urbild in $\mathrm{S}L_2(3)$ die Ordnung 8 hat ist Q_8 ein Normalteiler. Wählt man ein Element $g \in \mathrm{S}L_2(3)$ der Ordnung 3, so haben wir ein semidirektes Produkt

$$Q_8 \langle g \rangle = \mathrm{S}L_2(3) \approx Q_8 \rtimes C_3$$

und Q_8 ist ein normales 3-Komplement. Da jeder Automorphismus der Ordnung 3 auf Q_8 die 4-elementigen Untergruppen zyklisch durchpermutiert, und keine Auswahl von deren Erzeugern $(\nu, \kappa, \ell) \in \{\pm i\} \times \{\pm j\} \times \{\pm k\}$ ausgezeichnet ist, sind alle Operationen von C_3 auf Q_8 äquivalent und führen auf ein zu $\mathrm{S}L_2(3)$ isomorphes semidirektes Produkt. Aus der semidirekten Zerlegung $\mathrm{S}L_2(3) \approx Q_8 \rtimes C_3$ schließen wir für die projektive Gruppe

$$\frac{\mathrm{S}L_2(3)}{\langle -e \rangle} \approx \mathrm{P}SL_2(3) \approx A_4 \approx D_4 \rtimes C_3.$$

Hier gilt die ähnliche Situation, dass alle nicht trivialen Operationen $C_3 \to \mathrm{Aut}D_4$ die vier Involutionen zyklisch durchtauschen und ein zu A_4 isomorphes semidirektes Produkt definieren. Wir erhalten teilweise als direkte Folgerung

Satz 3.4. *Ein echt semidirektes Produkt $Q_8 \rtimes C_3$ ist stets isomorph zu $SL_2(3)$. Ein echt semidirektes Produkt $D_4 \rtimes C_3$ ist stets isomorph zu $PSL_2(3) \approx A_4$. Die $SL_2(3)$ wird von den Elementen der Ordnung 3 erzeugt.*

Beweis. Wir müssen nur noch die letzte Aussage zeigen. Dazu betrachten wir die natürliche Matrizendarstellung von $\mathrm{S}L_2(3)$ über $\mathbb{Z}_3$. Die beiden Matrizen $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ haben die Ordnung 3 und es gilt

$$\left(\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)\right)^2 = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} 5 & 3 \\ 3 & 2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right).$$

Mithin ist also das Element $-e$ im Erzeugnis der Elemente von Ordnung 3. Da die A_4 von den Dreizykeln erzeugt wird, folgt aus $\mathrm{P}SL_2(3) = \frac{\mathrm{S}L_2(3)}{\langle -e \rangle} \approx A_4$, dass auch $\mathrm{S}L_2(3)$ von den Elementen der Ordnung 3 erzeugt wird. □

Die Erkenntnisse über die Quaternionengruppe in $\mathrm{S}L_2(3)$ erweisen sich im folgenden Hilfssatz als nützlich. Wir betrachten die sehr spezielle Lage der Dinge, dass eine zu $\mathrm{S}L_2(3)$ isomorphe Gruppe auf einem Vektorraum V linear operiert. Dabei soll sich der mit $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ assoziierte Automorphismus genauso verhalten, wie die Matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ auf

dem zweidimensionalen Vektorraum $\mathbb{Z}_3 \times \mathbb{Z}_3$ über dem Körper $\mathbb{Z}_3$. Weiterhin sollen die Elemente der Ordnung 3 fixpunktfrei sein.

Satz 3.5. *Sei V ein $\mathbb{K}$-Vektorraum, $G \approx SL_2(3)$, $Z = ZG$, $Q \lhd G$ die Quaternionengruppe in G und $G \to AutV$ derart, dass für das eindeutige $z \in Z \setminus \{e\}$*

$$zv = -v = -ev \qquad \forall v \in V$$

gilt und jedes Element der Ordnung 3 fixpunktfrei operiert. Ist dann $g \in G$ mit Ordnung 3 und $h \in Q \setminus Z$ derart, dass gh ebenfalls Ordnung 3 hat, so gelten:

1. $\langle h, h^g \rangle = Q$
2. $g(h+e) = h^g - e$ *und* $2g = (h^g - e)(e - h)$ *in* $\mathrm{End}V$.
3. *Ist* $charK = 2$, *so gilt* $C_V(h) = C_V(h^g) = C_V(Q)$.
4. *Ist* $charK \neq 2$, *so ist jeder Q-invariante Unterraum bereits G-invariant.*

Beweis.

1. Da h^g von Ordnung 4 ist folgt $h^g \in Q$. Wegen Satz 3.3 genügt es $h^g \notin \langle h \rangle$ zu zeigen, was mit $g \notin \mathrm{N}_G \langle h \rangle$ gleichbedeutend ist. Das kanonische Bild hZ in $\mathrm{P}SL_2(3) \approx A_4$ ist von Ordnung 2 aber gZ von Ordnung 3. Aus $g \in \mathrm{N}_G \langle h \rangle$ folgt dann mit

   $$gZ \langle h \rangle Zg^{-1}Z = g \langle h \rangle g^{-1}Z = \langle h \rangle Z$$

   ein Widerspruch, da nach Korollar 3.5 in der A_4 keine Untergruppen der Ordnung 2 von einem Element der Ordnung 3 normalisiert werden. Also schließen wir

   $$g \notin N_G \langle h \rangle \quad \Longrightarrow \quad h^g \notin \langle h \rangle \quad \Longrightarrow \quad \langle h, h^g \rangle = Q.$$

2. Die folgenden Gleichungen sind stets im Endomorphismenring des Vektorraums V zu interpretieren. Da g von Ordnung 3 ist, folgt zunächst die Beziehung

   $$\left(e + g + g^2\right)(g - e) = g + g^2 + e - e - g - g^2 = 0.$$

   Da g aber als fixpunktfrei angenommen wurde, kann $(g - e)$ invertiert werden und es folgt

   $$e + g + g^2 = 0. \tag{1}$$

Da laut Annahme gh ebenfalls Ordnung 3 hat und fixpunktfrei ist, folgt analog

$$e + gh + ghgh = 0. \tag{2}$$

Aus Gleichung (1) folgt mit der Ordnungvon g schließlich $g^2 = -(e+g) = g^{-1}$. Multiplizieren wir Gleichung (2) von links mit g, so erhalten wir

$$g + g^2h + g^2hgh = g - (e+g)h + g^{-1}hgh = g - h - gh + h^gh = 0$$

und somit folgt

$$g - gh = h - h^gh \quad \Longleftrightarrow \quad g\,(e-h) = (e-h^g)\,h. \tag{3}$$

Aus Satz 3.3 kann $h^2 = -e$ gefolgert werden. Multipliziert man die rechte Gleichung von (3) nun rechts mit h, erhält man daher

$$g\,(h+e) = h^g - e. \tag{4}$$

Multipliziert man nun noch mit $(e-h)$ von rechts, erhält man zuletzt

$$g\,(h+e)\,(e-h) = 2g = (h^g - e)\,(e-h)\,. \tag{5}$$

Mit der Gleichungen (4) und (5) ist die zweite Aussage bewiesen.

3. Für die dritte Aussage sei char$K = 2$ und $v \in C_V h$ ein Fixpunkt von h. Wegen $1 = -1$ lautet dann die Fixpunktgleichung

$$hv = v = -v \quad \Longleftrightarrow \quad hv + v = (h+e)\,v = 0.$$

Durch Verkettung mit g in Verbindung mit Gleichung (4) erhalten wir

$$g\,(h+e)\,v = 0 \quad \Longrightarrow \quad (h^g - e)\,v = 0$$

und somit $v \in \mathrm{C}_V\,\langle h^g \rangle$. Wegen $Q = \langle h, h^g \rangle$ folgt somit auch $v \in \mathrm{C}_V Q$ und die dritte Behauptung ist bewiesen.

4. Ist hingegen char$K \neq 2$, so kann man in Gleichung (5) durch 2 dividieren und folgern, dass

$$g = \frac{1}{2}\,(h^g - e)\,(e-h)$$

gilt. Da $G = Q\,\langle g \rangle$ ein semidirektes Produkt ist, und g im Endomorphismen-

ring End$V$ als Polynom von Elementen aus Q geschrieben werden kann, sind Q-invariante Unterräume auch g-invariant und damit G-invariant.

□

3.4 Eine spezielle perfekte Gruppen $\mathfrak{G}$

Eine weitere Aussage, die Zassenhaus in [2] gemacht hat, betrifft perfekte Gruppen welche die pq-Bedingung erfüllen. Perfekte Frobeniuskomplemente gehören nach Korollar 2.5 gewiss dazu. Ist G eine solche Gruppe, so gibt Zassenhaus den Isomorphietyp als $G \approx \mathrm{S}L_2(F_n)$ mit einer Fermatschen Primzahl $F_n \geq 5$ an. Die Fermatsche Zahlen sind gegeben durch

$$F_n = 2^{(2^n)} - 1 \quad \text{mit} \quad n \in \mathbb{N}.$$

Während die ersten fünf Fermatschen Zahlen

$$\{F_1, \ldots, F_5\} = \{3, 5, 17, 257, 65537\}$$

Primzahlen sind, vermutet man, dass für $n > 5$ keine Primzahlen mehr auftreten. Falls diese Vermutung zutrifft, sind bereits hierdurch die Isomorphietypen perfekte Gruppen mit pq-Bedingung auf 4 Fälle begrenzt. Nach Satz 3.2 sind die 2-Sylowgruppen in allen Fällen verallgemeinerte Quaternionengruppen. Im Folgenden soll ein ähnliches, empfindlich geändertes Szenario betrachtet werden.

Wie in der Beweisskizze angekündigt, werden wir in diesem Unterabschnitt nun Gruppen untersucht, welche zumindest einige Eigenschaften perfekter Frobeniuskomplemente besitzt. Die pq-Eigenschaft wird auf ungerade Primzahlen eingeschränkt und im Gegenzug wird über die 2-Sylowgruppen eine zusätzliche Annahme gemacht. Bis auf weiteres sei $\mathfrak{G}$ eine Gruppe mit den folgenden drei Eigenschaften:

1. $\mathfrak{G}$ ist eine perfekte Gruppe.
2. Die 2-Sylowgruppen von $\mathfrak{G}$ sind zyklisch oder Diedergruppen.
3. Untergruppen von $\mathfrak{G}$ mit Ordnung pq für zweie ungerade Primzahlen p und q sind zyklisch.

Das $\mathrm{S}L_2(5)$-Theorem vorausgreifend sehen wir, dass eine Gruppe mit den genannten drei Eigenschaften niemals ein perfektes Frobeniuskomplement ist, sonst wäre $\mathfrak{G} \approx \mathrm{S}L_2(5)$ und die 2-Sylowgruppen verallgemeinerte Quaternionengruppen, im Widerspruch zur zweiten Eigenschaft. Allerdings wird eine Gruppe mit den genannten Eigenschaften als

Faktorgruppe $\overline{\mathcal{G}}$ eines perfekten Frobeniuskomplementes $\mathcal{G}$ in Erscheinung treten, hierdurch wird die Behandlung motiviert. Die dritte Eigenschaft nennen wir die "eingeschränkte pq-Bedingung". Hierbei ist der Fall $p = q$ zugelassen.

Lemma 3.1. *Sei p ein ungerader Primteiler der Ordnung von $\mathfrak{G}$. Dann sind alle p-Untergruppen von $\mathfrak{G}$ zyklisch. Insbesondere sind die p-Sylowgruppen zyklisch.*

Beweis. Wir betrachten zuvor den Sonderfall, abelschen p-Untergruppen. Sei also P zunächst eine abelsche p-Untergruppe von $\mathfrak{G}$. Im Fall, dass die Ordnung von P gleich p ist, folgt sofort $P \approx C_p$. Ist die Ordnung hingegen größer oder gleich p^2 und P nicht zyklisch, so können wir gemäß dem Klassifikationsatz endliche erzeugter, abelscher Gruppen in P eine elementar abelsche Untergruppe isomorph zu $C_p \times C_p$ finden. Da das jedoch einen Widerspruch zur eingeschränkten pq-Bedingung darstellt, muss P doch zyklisch sein. Es sind also alle abelschen p-Gruppen in $\mathfrak{G}$ zyklisch. Insbesondere sind dann auch alle abelschen Untergruppen einer beliebigen p-Untergruppen zyklisch. Aus Korollar 2.4 können wir nun folgern, dass bereits alle p-Untergruppen zyklisch sind. □

Zu einem ungeraden Primteiler p der Ordnung von $\mathfrak{G}$ wollen wir p'-Automorphismen der p-Untergruppen hinsichtlich des Auftretens nicht trivialer Fixpunkte näher untersuchen. Da wir nun nach Lemma 3.1 wissen, dass die p-Untergruppen von $\mathfrak{G}$ zyklisch sind, führt uns die Untersuchung der Automorphismen zu zahlentheoretischen Überlegungen in einem Restklassenring $\mathbb{Z}_{p^n}$ mit $n \in \mathbb{N}$.

Im allgemein Fall ist die Automorphismengruppe einer zyklischen Gruppe $C_q \approx \mathbb{Z}_q$ mit $q \in \mathbb{N}$ isomorph zur multiplikativen Gruppe $\mathbb{Z}_q^\times$, die durch Multiplikation auf $\mathbb{Z}_q$ operiert. Die Ordnung der Automorphismengruppe lässt sich mit der Eulerschen Phifunktion angeben und ist

$$\varphi(q) = |\{\nu \in \{1, \ldots, q\} \mid \mathrm{ggT}(\nu, q) = 1\}| = \left|\mathbb{Z}_q^\times\right|.$$

Nach dem Satz von Gauss über die Existenz von Primitivwurzeln, also Erzeugern der multiplikativen Gruppe $\mathbb{Z}_q^\times$, ist die Automorphismengruppe genau dann zyklisch, wenn q gleich 1, 2, 4, p^n oder $2p^n$ mit $n \in \mathbb{N}$ und einer ungeraden Primzahl p ist. Insbesondere haben also die p-Untergruppen von $\mathfrak{G}$ jeweils zyklische Automorphismengruppen. Für ungerade Primpotenzen p^n und dementsprechende Einheitengruppen ergibt die Eulersche Phi Funktion gerade die Ordnung

$$\left|\mathbb{Z}_{p^n}^\times\right| = \varphi(p^n) = p^{n-1}(p-1).$$

Ein p'-Automorphismus von $C_{p^n} \approx \mathbb{Z}_{p^n}$ entspricht daher einem Element $a \in \mathbb{Z}_{p^n}^\times$, dessen multiplikative Ordnung teilerfremd zu p ist. Wegen der Ordnung der multiplikativen Gruppe $\left|\mathbb{Z}_{p^n}^\times\right| = p^{n-1}(p-1)$ ist die Ordnung von a dann ein Teiler von $p-1$ und es folgt

$$\begin{aligned} a^{p-1} &= 1 \bmod p^n \\ \Longrightarrow \quad a^p &= a \bmod p^n \\ \Longrightarrow \quad a^p &= a \bmod p^\ell \end{aligned}$$

für alle natürlichen $\ell \leq n$. Hat nun der assoziierte Automorphismus $x \mapsto ax$ einen nicht trivialen Fixpunkt, so ist dies gleichbedeutend damit, dass $a-1$ ein Nullteiler ist. Wir wollen zeigen, dass dann $a = 1 \bmod p^n$ gilt. Mit anderen Worten, ein p'-Automorphismus von $\mathbb{Z}_{p^n}$ ist entweder fixpunktfrei oder trivial. Sei daher nun $a-1$ ein Nullteiler, also $a - 1 = mp^k$ mit $k \in \mathbb{N}$ und m teilerfremd zu p. Im Fall $n \leq k$ folgt dann sofort

$$a = 1 + mp^k = 1 \mod p^n$$

und a entspricht der Identität. Ist hingegen $k < n$ so folgt aus $a^p = a \mod p^\ell$ für $\ell = k+1 \leq n$ die Kongruenz

$$a = 1 + mp^k = \left(1 + mp^k\right)^p = \sum_{\nu=0}^{p} \binom{p}{\nu} m^\nu p^{k\nu} = 1 \mod p^{k+1}$$

und schließlich mit $mp^k = 0 \bmod p^{k+1}$ ein Widerspruch, da m teilerfremd zu p ist. Als Folgerung erhalten wir

Lemma 3.2. *Sei p eine ungerade Primzahl und P eine zyklische p-Gruppe. Dann gelten folgende Aussagen:*

1. *Ein p'-Automorphismus α von P ist entweder fixpunktfrei oder trivial. Insbesondere ist α bereits trivial, falls es auf einer nicht trivialen Untergruppe trivial ist.*
2. *Für eine p'-Gruppe Q mit einer Operation $Q \to AutP$ gilt entweder $C_P Q = P$ oder $C_P Q = e$. Die Operation ist also entweder trivial oder Q besitzt keine nicht-trivialen Fixpunkte.*

Beweis. Die erste Aussagen ist bereits bewiesen. Für die zweite Aussage sei $x \in \mathrm{C}_P Q$ mit $x \neq e$. Dann besitzen alle $q \in Q$ einen nicht trivialen Fixpunkt und operieren nach der vorangegangenen Überlegung trivial auf P. □

Lemma 3.3. *Sei p eine ungerade Primzahl und $P \approx \langle x \rangle \approx C_{p^n}$ eine zyklische p-Gruppe. Dann gibt es genau eine nicht triviale Involution $\alpha \in AutP$ und P wird von α invertiert, d.h. $\alpha x = x^{-1}$ für alle $x \in P$.*

Beweis. Die Ordnung der Automorphismengruppe Aut$P$ ist gerade $\varphi(p^n) = p^{n-1}(p-1)$. Da p ungerade ist, muss $p-1$ gerade sein und somit existiert mindestens eine nicht triviale Involution $\alpha \in \mathrm{Aut}P$. Da $\mathrm{Aut}P \approx \mathbb{Z}_{p^n}^{\times}$ zyklisch ist, gibt es genau eine Zweielementige Untergruppe von Aut$P$ und demnach ist die Involution einzig in $AutP$. Mit $\alpha x = x^m \neq x$, $m \in \mathbb{N}$ folgt dann aus $\alpha^2 x = x^{m^2} = x$ die Kongruenz $m^2 = 1 \mod p^n$. Da aber -1 die einzige Involution in $\mathbb{Z}_{p^n}^{\times}$ ist, folgt damit $m = -1 \mod p^n$ und P wird von α invertiert. □

Die beiden Lemmata setzen wir nun ein, um für ungerade Primteiler p der Ordnung von $\mathfrak{G}$ die p-Sylowgruppen $\mathfrak{G}_p$ zu untersuchen. Da nach Lemma 3.1 alle Sylowgruppen zyklisch sind, ist $\mathfrak{G}_p \leq C_{\mathfrak{G}}\mathfrak{G}_p$ und daher $Q = \frac{\mathrm{N}_{\mathfrak{G}}\mathfrak{G}_p}{\mathrm{C}_{\mathfrak{G}}\mathfrak{G}_p}$ eine p'-Gruppe, deren Operation durch Konjugation auf $\mathfrak{G}_p$ den Voraussetzungen von Lemma 3.2 entspricht. Wir wollen zeigen, dass Q stets eine nicht triviale 2-Gruppe ist.

Lemma 3.4. *Sei p ein ungerader Primteiler der Ordnung von $\mathfrak{G}$ und P eine p-Sylowgruppe von $\mathfrak{G}$. Dann ist $\frac{N_{\mathfrak{G}}P}{C_{\mathfrak{G}}P}$ eine nicht triviale 2-Gruppe und jede p-Gruppe in $\mathfrak{G}$ wird durch Konjugation mit einem geeigneten Element invertiert.*

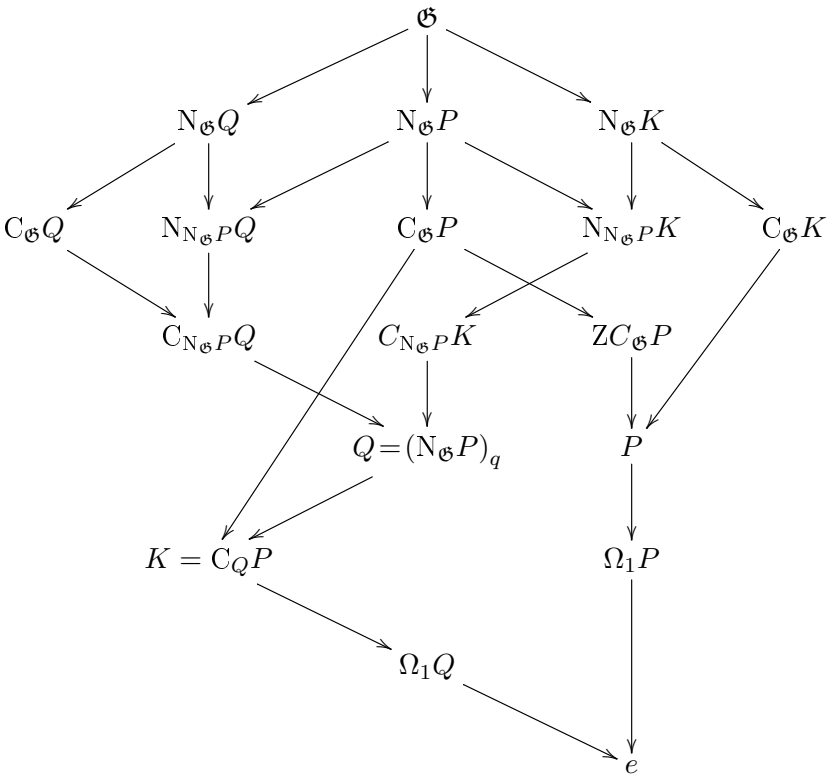
Beweis. Ist $\frac{\mathrm{N}_{\mathfrak{G}}P}{\mathrm{C}_{\mathfrak{G}}P}$ eine nicht triviale 2-Gruppe, so gibt es darin eine nicht triviale Involution. Nach Lemma 3.3 ist diese Involution eindeutig und invertiert P. Ein geeigneter Repräsentant aus dem kanonischen Urbild der Involution invertiert mit P natürlich auch alle Untergruppen von P durch Konjugation. Da jede p-Gruppe in einer Sylowgruppe enthalten ist, bleibt zu zeigen, dass die Faktorgruppe $\frac{\mathrm{N}_{\mathfrak{G}}P}{\mathrm{C}_{\mathfrak{G}}P}$ eine nicht triviale 2-Gruppe ist.

Zunächst zeigen wir die Nichttrivialität. Wir argumentieren indirekt, nehmen also an $\frac{\mathrm{N}_{\mathfrak{G}}P}{\mathrm{C}_{\mathfrak{G}}P}$ sei trivial und demnach $\mathrm{C}_{\mathfrak{G}}P = \mathrm{N}_{\mathfrak{G}}P$. Da P nach Lemma 3.1 kommutativ ist, haben wir dann $P \leq \mathrm{Z}C_{\mathfrak{G}}P = \mathrm{Z}N_{\mathfrak{G}}P$ und nach Satz 2.3 gibt es dann ein normales p-Komplement $N \trianglelefteq \mathfrak{G}$ mit $\mathfrak{G} = NP \approx N \rtimes P$. Als Konsequenz haben wir dann eine nicht triviale, zyklische Faktorgruppe $\frac{\mathfrak{G}}{N} \approx P$. Das widerspricht der Perfektheit von $\mathfrak{G}$ und wir können daher $\frac{\mathrm{N}_{\mathfrak{G}}P}{\mathrm{C}_{\mathfrak{G}}P} \neq e$ schließen.

Nach Lemma 3.1 ist $P \approx C_{p^n}$ mit $n \in \mathbb{N}$ und die Ordnung der Automorphismengruppe Aut$P$ ist gerade $\varphi(p^n) = p^{n-1}(p-1)$. Als kommutative Gruppe ist $P \leq \mathrm{C}_{\mathfrak{G}}P$ und daher

teilt die Ordnung von $\frac{\mathrm{N}_{\mathfrak{G}}P}{\mathrm{C}_{\mathfrak{G}}P} \hookrightarrow \mathrm{Aut}P$ die gerade Zahl $p-1$. Ein Primteiler q der Ordnung von $\frac{\mathrm{N}_{\mathfrak{G}}P}{\mathrm{C}_{\mathfrak{G}}P}$ ist dann ebenfalls ein Teiler von $p-1$ und somit echt kleiner als p. Insbesondere folgt in den Fällen $p = 3$ und $p = 5$ sofort $q = 2$. Die Argumentation verläuft nun induktiv. Sei also p eine Primzahl größer oder gleich 5 und gelte die Aussage für jede ungerade Primzahlen kleiner als p.

Der Induktionsschluss erfolgt indirekt. Wir nehmen also an, q sei ein ungerader Primteiler von $\frac{\mathrm{N}_{\mathfrak{G}}P}{\mathrm{C}_{\mathfrak{G}}P}$. Dann ist q insbesondere ein Teiler der Ordnung von $\mathrm{N}_{\mathfrak{G}}P$ und jede q-Sylowgruppe Q von $\mathrm{N}_{\mathfrak{G}}P$ ist nach Lemma 3.1 eine zyklisch p'-Gruppe, die durch Konjugation auf P operiert. Den Kern der Operation $Q \to \mathrm{Aut}P$ bezeichnen wir mit $K = \mathrm{C}_Q P$. Die komplizierte Lage der betrachteten Untergruppen ist auszugsweise im folgenden Diagramm verzeichnet. Am Ende eines Pfeils steht darin eine Untergruppe der am Pfeilanfang stehenden Gruppen. Alle kommenden Schlüsse können im Diagramm nachvollzogen werden. Bis auf wenige Ausnahmen sind alle Inklusionen im Diagramm sofort einsichtig.



Da $\Omega_1 P$ charakteristisch in P ist, haben wir eine Operation $Q \to \mathrm{Aut}\Omega_1 P$ und damit auch eine Operation der Untergruppe $\Omega_1 Q \to \mathrm{Aut}\Omega_1 P$ jeweils durch Konjugation. Insbe-

sondere ist $\Omega_1 Q$ im Normalisator von $\Omega_1 P$, daher kommutieren die Untergruppen $\Omega_1 P$ und $\Omega_1 P$, so dass deren Komplexprodukt wieder eine Untergruppe bildet. Wegen der eingeschränkten pq-Bedingung ist die so gewonnene Untergruppe

$$\Omega_1 Q \cdot \Omega_1 P = \Omega_1 P \cdot \Omega_1 Q \leq \mathfrak{G} \qquad \text{mit} \qquad |\Omega_1 Q \cdot \Omega_1 P| = pq$$

zyklisch und folglich operiert $\Omega_1 Q$ trivial auf $\Omega_1 P$. Nach Lemma 3.2 operiert $\Omega_1 Q$ damit auch trivial auf P. Insbesondere ist dann $\Omega_1 Q \leq \mathrm{C}_Q P = K \leq Q$ und somit K nicht trivial.

Als q-Gruppe wird K per Induktionsannahme durch Konjugation mit einem Element $g \in \mathrm{N}_{\mathfrak{G}} K$ invertiert. Da alle Elemente aus K mit den Elementen aus P kommutieren, ist P umgekehrt eine Sylowgruppe in $\mathrm{C}_{\mathfrak{G}} K$. Es gilt also

$$P = (\mathrm{C}_{\mathfrak{G}} K)_p \leq \mathrm{C}_{\mathfrak{G}} K \trianglelefteq \mathrm{N}_{\mathfrak{G}} K$$

und mit dem Frattinischluss folgt daraus die Zerlegung

$$\mathrm{N}_{\mathrm{N}_{\mathfrak{G}} K} P \cdot \mathrm{C}_{\mathfrak{G}} K = \mathrm{N}_{\mathfrak{G}} K.$$

Damit erhalten wir für g ebenfalls eine Zerlegung als Produkt $g = nh$ mit $n \in \mathrm{N}_{\mathrm{N}_{\mathfrak{G}} K} P$ und $h \in \mathrm{C}_{\mathfrak{G}} K$. Da h trivial auf K operiert, wird K bereits von n invertiert und P von n normalisiert. Aus $K \leq Q \leq \mathrm{N}_{\mathfrak{G}} P$ folgt wegen der Kommutativität von Q schließlich

$$Q \leq C_{\mathrm{N}_{\mathfrak{G}} P} K \trianglelefteq \mathrm{N}_{\mathrm{N}_{\mathfrak{G}} P} K \leq \mathrm{N}_{\mathfrak{G}} P$$

und Q ist demnach eine Sylowgruppe von $C_{\mathrm{N}_{\mathfrak{G}} P} K$. Abermals mit einem Frattiniargument erhalten wir dann

$$\mathrm{N}_{\mathrm{N}_{\mathrm{N}_{\mathfrak{G}} P} K} Q \cdot C_{\mathrm{N}_{\mathfrak{G}} P} K = \mathrm{N}_{\mathrm{N}_{\mathfrak{G}} P} K$$

mit

$$\mathrm{N}_{\mathrm{N}_{\mathrm{N}_{\mathfrak{G}} P} K} Q = \mathrm{N}_{\mathfrak{G}} Q \cap \mathrm{N}_{\mathrm{N}_{\mathfrak{G}} P} K = \mathrm{N}_{\mathfrak{G}} Q \cap \mathrm{N}_{\mathfrak{G}} K \cap \mathrm{N}_{\mathfrak{G}} P.$$

Daher gibt es eine Zerlegung $n = ab$ mit $a \in \mathrm{N}_{\mathfrak{G}} Q \cap \mathrm{N}_{\mathfrak{G}} K \cap \mathrm{N}_{\mathfrak{G}} P$ und $b \in \mathrm{C}_{\mathrm{N}_{\mathfrak{G}} P} K$. Nun operiert b trivial auf K und wir schließen daraus, dass K bereits von a invertiert wird. Wegen $K \leq Q$ ist die Konjugation mit a ist damit aber auch ein nicht trivialer Automorphismus der Ordnung 2 auf Q. Nach Lemma 3.3 wird demnach Q von a invertiert.

Sei nun $x \in Q$ ein Erzeuger der zyklischen Gruppe Q. Da q nicht von 2 geteilt wird, ist

das Element x^{-2} ebenfalls ein Erzeuger von Q und wir erhalten

$$[\mathrm{N}_{\mathfrak{G}}P, \mathrm{N}_{\mathfrak{G}}P] \geq \langle [a,x] \rangle = \left\langle axa^{-1}x^{-1} \right\rangle = \left\langle x^{-2} \right\rangle = \langle x \rangle = Q.$$

Da $\mathrm{Aut}P$ zyklisch ist, folgt insbesondere die Kommutativität von $\frac{\mathrm{N}_{\mathfrak{G}}P}{\mathrm{C}_{\mathfrak{G}}P} \hookrightarrow \mathrm{Aut}P$. Da eine Faktorgruppe genau dann kommutativ ist, wenn die Kommutatorgruppe im zugehörigen Normalteiler enthalten ist, folgt somit

$$Q \leq [\mathrm{N}_{\mathfrak{G}}P, \mathrm{N}_{\mathfrak{G}}P] \leq \mathrm{C}_{\mathfrak{G}}P.$$

Da aber Q eine Sylowgruppe in $\mathrm{N}_{\mathfrak{G}}P$ ist, folgt aus $Q \leq \mathrm{C}_{\mathfrak{G}}P$, dass q teilerfremd zur Ordnung von $\frac{\mathrm{N}_{\mathfrak{G}}P}{\mathrm{C}_{\mathfrak{G}}P}$ ist. Da q als von 2 verschiedener Primteiler von $\frac{\mathrm{N}_{\mathfrak{G}}P}{\mathrm{C}_{\mathfrak{G}}P}$ gewählt wurde, ist das ein Widerspruch. Folglich ist jeder Primteiler mit 2 identisch und $\frac{\mathrm{N}_{\mathfrak{G}}P}{\mathrm{C}_{\mathfrak{G}}P}$ demnach eine 2-Gruppe. □

Mit der Ordnung von $\frac{\mathrm{N}_{\mathfrak{G}}P}{\mathrm{C}_{\mathfrak{G}}P}$ ist auch $|\mathrm{N}_{\mathfrak{G}}P|$ und schließlich die Ordnung von $\mathfrak{G}$ durch 2 teilbar. Wir halten somit als Folgerung fest

Korollar 3.8. *Die Ordnung von $\mathfrak{G}$ ist gerade, die 2-Sylowgruppen sind daher nicht trivial und es gibt mindestens eine nicht triviale Involution in $\mathfrak{G}$.*

Wir wenden uns nun einer näheren Untersuchung der 2-Sylowgruppen in $\mathfrak{G}$ zu und können sogar den Isomorphietyp bestimmen. Eng verwoben damit sind Aussagen über die Involutionen in $\mathfrak{G}$.

Lemma 3.5. *Für jede 2-Sylowgruppe $\mathfrak{G}_2$ von $\mathfrak{G}$ gilt $C_{\mathfrak{G}}\mathfrak{G}_2 \leq \mathfrak{G}_2$.*

Beweis. Der Schluss erfolgt indirekt, wir nehmen also an, es gäbe ein $x \in \mathrm{C}_{\mathfrak{G}}\mathfrak{G}_2 \setminus \mathfrak{G}_2$ und unterscheiden 2 Fälle.

Fall 1. Ist $x \in \mathrm{C}_{\mathfrak{G}}\mathfrak{G}_2$ von gerader Ordnung, so können wir eine 2-Element $y \in \langle x \rangle$ wählen. Dann hätten wir jedoch mit $\langle y \rangle \mathfrak{G}_2$ eine 2-Gruppe, die echt größer ist als die Sylowgruppe $\mathfrak{G}_2$, was nicht sein kann.

Fall 2. Ist hingegen $x \in \mathrm{C}_{\mathfrak{G}}\mathfrak{G}_2$ von ungerader Ordnung, so können $y \in \langle x \rangle$ von ungerader Primzahlordnung p auswählen und haben mit $\langle y \rangle$ eine p-Gruppe. Wegen der Inklusionen $\mathfrak{G}_2 \leq \mathrm{C}_{\mathfrak{G}} \langle x \rangle \leq \mathrm{C}_{\mathfrak{G}} \langle y \rangle$ ist aber die höchste Zweierpotenz der Ordnung von $\mathfrak{G}$ bereits in der Ordnung von $\mathrm{C}_{\mathfrak{G}} \langle y \rangle$ enthalten, weshalb $\frac{\mathrm{N}_{\mathfrak{G}} \langle y \rangle}{\mathrm{C}_{\mathfrak{G}} \langle y \rangle}$ eine ungerade Ordnung hat. Dann gibt es aber kein Involution, die $\langle y \rangle$ durch Konjugation invertiert, was wiederum Lemma 3.4 widerspricht.

□

Den folgenden Hilfssatz von Thompson benötigen wir, um zu zeigen, dass alle Involutionen in $\mathfrak{G}$ einer einzigen Konjugationsklasse angehören.

Lemma 3.6. *Sei G eine Gruppe von gerader Ordnung, die keine Normalteiler vom Index 2 besitzt. Sei weiterhin H eine maximale echte Untergruppe einer 2-Sylowgruppe von G. Dann ist jede Involution konjugiert zu einem Element von H. Alle Konjugationsklassen von Involutionen schneiden H.*

Beweis. Suzuki [12], S. 127, (1.8). □

Lemma 3.7. *Es gibt nur eine Konjugationsklasse von Involutionen in $\mathfrak{G}$, alle Involutionen sind konjugiert zu einem Element in einer maximalen echten Untergruppe einer 2-Sylowgruppe von $\mathfrak{G}$.*

Beweis. Da eine Faktorgruppe genau dann kommutativ ist, wenn der entsprechende Normalteiler die Kommutatorgruppe enthält, besitzt $\mathfrak{G}$ wegen der Perfektheit keine nicht trivialen, abelschen Faktorgruppen. Insbesondere besitzt $\mathfrak{G}$ dann keine Untergruppen vom Index 2. Da wir wissen, dass die Ordnung von $\mathfrak{G}$ gerade ist, lässt sich Lemma 3.6 anwenden. Laut Annahme ist eine 2-Sylowgruppen $\mathfrak{G}_2$ zyklisch oder Diedergruppe. In beiden Fällen finden wir darin eine maximale Untergruppen H vom Index $[\mathfrak{G}_2 : H] = 2$. Diese ist überdies zyklisch, daher gibt es in H genau eine nicht triviale Involution. Lemma 3.6 besagt nun gerade, dass alle Involutionen in $\mathfrak{G}$ zur nämlichen konjugiert sind. Daher kann es auch nur eine einzige Konjugationsklasse von Involutionen geben. □

Laut Annahme sind alle 2-Sylowgruppen in $\mathfrak{G}$ zyklisch oder Diedergruppen. Wir zeigen nun, das der Fall einer zyklischen Sylowgruppe $\mathfrak{G}_2$ nicht eintritt.

Lemma 3.8. *Die 2-Sylowgruppen $\mathfrak{G}_2$ von $\mathfrak{G}$ sind stets Diedergruppen mit $|\mathfrak{G}_2| \geq 4$. Insbesondere gibt es in $\mathfrak{G}_2$ eine Kleinsche Vierergruppe und damit drei voneinander verschiedene Involutionen.*

Beweis. Nach Korollar 3.8 hat $\mathfrak{G}$ gerade Ordnung und die 2-Sylowgruppen sind daher nicht trivial. Wir nehmen nun an, dass $\mathfrak{G}_2$ zyklisch ist von Ordnung 2^n. Dann ist $\mathrm{Aut}\mathfrak{G}_2$ ebenfalls eine 2-Gruppe der Ordnung $\varphi(2^n) = 2^{n-1}$ und es gilt $\mathfrak{G}_2 \leq \mathrm{Z}C_{\mathfrak{G}}\mathfrak{G}_2 \leq \mathrm{C}_{\mathfrak{G}}\mathfrak{G}_2$. Folglich ist die Faktorgruppe $\frac{N_{\mathfrak{G}}\mathfrak{G}_2}{C_{\mathfrak{G}}\mathfrak{G}_2} \hookrightarrow \mathrm{Aut}\mathfrak{G}_2$ von ungerader Ordnung und somit trivial. Wir haben also $\mathrm{N}_{\mathfrak{G}}\mathfrak{G}_2 = \mathrm{C}_{\mathfrak{G}}\mathfrak{G}_2$ und schließen daraus $\mathfrak{G}_2 \leq \mathrm{Z}C_{\mathfrak{G}}\mathfrak{G}_2 = \mathrm{Z}N_{\mathfrak{G}}\mathfrak{G}_2$. Nach Satz

2.3 besitzt $\mathfrak{G}$ dann ein normales 2-Komplement $N \trianglelefteq \mathfrak{G}$ und eine semidirekte Zerlegung $\mathfrak{G} = \mathrm{N}\mathfrak{G}_2 \approx N \rtimes \mathfrak{G}_2$. Daraus folgt jedoch die Existenz einer zyklischen Faktorgruppe $\frac{\mathfrak{G}}{N} \approx \mathfrak{G}_2$, was der Perfektheit von $\mathfrak{G}$ widerspricht. Mithin schließen wir indirekt, dass $\mathfrak{G}_2$ eine Diedergruppe mit einer Ordnung größer oder gleich 4 ist. Insbesondere gibt es in $\mathfrak{G}_2$ eine Vierergruppe und somit drei voneinander verschiedene Involutionen. □

Lemma 3.9. *Für das Zentrum gilt $Z\mathfrak{G} = O_2\mathfrak{G} = e$. Insbesondere gibt es keine zentrale Involution in $\mathfrak{G}$.*

Beweis. Wir nehmen an $\mathrm{Z}\mathfrak{G} \neq e$ und zeigen, dass dann die Ordnung von $\mathrm{Z}\mathfrak{G}$ eine Zweierpotenz ist. Wäre die Ordnung von $\mathrm{Z}\mathfrak{G}$ ungerade, so gäbe es ein Element $g \in \mathrm{Z}\mathfrak{G}$ von ungerader Primzahlordnung. Dann folgt aber $\mathrm{C}_{\mathfrak{G}} \langle g \rangle = \mathrm{N}_{\mathfrak{G}} \langle g \rangle = \mathfrak{G}$ und somit ist $\frac{\mathrm{N}_{\mathfrak{G}}\langle g \rangle}{\mathrm{C}_{\mathfrak{G}}\langle g \rangle}$ trivial im Widerspruch zu Lemma 3.4. Also ist $\mathrm{Z}\mathfrak{G}$ eine 2-Gruppe und wegen der Konjugationsinvarianz in allen Sylowgruppen $\mathfrak{G}_2$ enthalten, präziser $\mathrm{Z}\mathfrak{G} \leq \mathrm{Z}\mathfrak{G}_2 \leq \mathfrak{G}_2$. Falls $\mathrm{Z}\mathfrak{G}$ nicht trivial ist, enthält es eine nicht triviale, zentrale Involution. Da nach Lemma 3.7 alle Involutionen in $\mathfrak{G}$ konjugiert sind, das Zentrum aber konjugationsinvariant ist, gäbe es dann nur eine einzige Involution in ganz $\mathfrak{G}$. Das ist ein Widerspruch, da wir nach Lemma 3.8 in $\mathfrak{G}_2$ bereits eine Vierergruppe und damit drei voneinander verschiedene Involutionen ausgemacht haben. Es folgt also $\mathrm{Z}\mathfrak{G} = e$.

Nun betrachten wir den größten 2-Normalteiler $\mathrm{O}_2\mathfrak{G}$. Dieser ist als Untergruppe einer Diedergruppe $\mathfrak{G}_2$ entweder zyklisch oder wieder eine Diedergruppe. Nach Korollar 3.2 über Diedergruppen sind $\mathrm{O}_2\mathfrak{G}$ und $\mathrm{Aut}\mathrm{O}_2\mathfrak{G}$ in jedem Fall auflösbar. Daraus folgt aber auch die Auflösbarkeit von

$$\frac{\mathrm{N}_{\mathfrak{G}}\mathrm{O}_2\mathfrak{G}}{\mathrm{C}_{\mathfrak{G}}\mathrm{O}_2\mathfrak{G}} = \frac{\mathfrak{G}}{\mathrm{C}_{\mathfrak{G}}\mathrm{O}_2\mathfrak{G}} \hookrightarrow \mathrm{Aut}\mathrm{O}_2\mathfrak{G}.$$

Da $\mathfrak{G}$ als perfekte Gruppen jedoch keine nicht trivialen, auflösbaren Faktorgruppen besitzen darf, folgt $\mathrm{C}_{\mathfrak{G}}\mathrm{O}_2\mathfrak{G} = \mathfrak{G}$ und somit ist $\mathrm{O}_2\mathfrak{G}$ kommutativ mit $\mathrm{O}_2\mathfrak{G} \leq \mathrm{Z}\mathfrak{G} = e$. □

Lemma 3.10. *Sei A eine Kleinsche Vierergruppe in einer Sylowgruppe $\mathfrak{G}_2$. Dann ist die Ordnung von $\frac{N_{\mathfrak{G}}A}{C_{\mathfrak{G}}A}$ durch 3 teilbar. Insbesondere ist $N_{\mathfrak{G}}A$ nicht trivial.*

Beweis. Es genügt, zu zeigen, dass $\mathrm{N}_{\mathfrak{G}}A$ durch Konjugation transitiv auf den drei Involutionen in $A^{\#}$ operiert. Da $A^{\#}$ genau 3 Elemente enthält, ist der Index eines Stabilisators dann gerade 3 und da $\mathrm{C}_{\mathfrak{G}}A$ in jedem Stabilisator enthalten ist, teilt 3 die Ordnung von $\frac{\mathrm{N}_{\mathfrak{G}}A}{\mathrm{C}_{\mathfrak{G}}A}$. Wir unterscheiden zwei Fälle.

Fall 1. Sei $A = \mathfrak{G}_2$. Da A kommutativ ist, bildet jede Involution eine normale Teilmenge in A. Da es nach Lemma 3.7 aber nur eine Konjugationsklasse von Involutionen in $\mathfrak{G}$ gibt, sind alle Elemente von $A^\#$ in $\mathfrak{G}$ konjugiert. Aus Satz 2.5 folgt dann aber, dass sie bereits in $\mathrm{N}_\mathfrak{G}\mathfrak{G}_2$ konjugiert sind. Also operiert $\mathrm{N}_\mathfrak{G}\mathfrak{G}_2$ transitiv auf $A^\# = \mathfrak{G}_2^\#$.

Fall 2. Sei $A \neq \mathfrak{G}_2$ und $A^\# = \{a, b, c\}$. Wir müssen zeigen, dass es ein $x \in \mathrm{N}_\mathfrak{G}A$ gibt mit $a^x = b$. Nach Korollar 3.3 ist eine der drei Involutionen gerade die in $\mathfrak{G}_2$ zentrale Involution $z \in \{a, b, c\}$ mit $\langle z \rangle = \mathrm{Z}\mathfrak{G}_2 \leq A$. Wieder nach Lemma 3.7 gibt es ein $g \in \mathfrak{G}$ mit $z^g = c$. Es gilt also $c \in (\mathrm{Z}\mathfrak{G}_2)^g = \mathrm{Z}\mathfrak{G}_2^g$ und somit ist $\mathfrak{G}_2^g$ eine 2-Sylowgruppe von $\mathrm{C}_\mathfrak{G}\langle c \rangle$. Als 2-Gruppe ist $A \leq \mathrm{C}_\mathfrak{G}\langle c \rangle$ ebenfalls in einer Sylowgruppe von $\mathrm{C}_\mathfrak{G}\langle c \rangle$ enthalten, daher gibt es $h \in \mathrm{C}_\mathfrak{G}\langle c \rangle$ mit $A \leq \mathfrak{G}_2^{gh}$ und $z^{gh} = c^h = c$. Da die Vierergruppen maximale, echte, abelsche Untergruppe der Diedergruppen sind, folgt

$$A = \mathrm{C}_{\mathfrak{G}_2^{gh}}A \leq \mathrm{N}_{\mathfrak{G}_2^{gh}}A \leq \mathfrak{G}_2^{gh} \leq \mathrm{C}_\mathfrak{G}\langle c \rangle$$

und folglich wird c von $\mathrm{N}_{\mathfrak{G}_2^g}A$ zentralisiert und erzeugt als zentrale Involution das Zentrum $\langle c \rangle = \mathrm{Z}\mathfrak{G}_2^{gh}$. Nach Korollar 3.3 gibt ein $x \in \mathrm{N}_{\mathfrak{G}_2^{gh}}A \leq \mathrm{N}_\mathfrak{G}A$ mit $a^x = b$, was zu zeigen war.

□

Wir betrachten nun eine zweielementige Untergruppe F des Zentrums $\mathrm{Z}\mathfrak{G}_2$. Wir wollen dabei nocheinmal auf die Fallunterscheidung im obigen Beweis eingehen. Je nach dem, ob $\mathfrak{G}_2 \approx D_4$ oder $\mathfrak{G}_2 \not\approx D_4$ gilt, ist $\mathfrak{G}_2$ eine abelsche Gruppe oder nicht. Für $\mathfrak{G}_2 \approx D_4$ haben wir $\mathrm{Z}\mathfrak{G}_2 \approx \mathfrak{G}_2$ und somit drei voneinander verschiedene Involutionen im Zentrum. Folglich haben wir drei Möglichkeiten, eine zweielementige Untergruppe $F \leq \mathrm{Z}\mathfrak{G}_2$ zu wählen. Gilt hingegen $\mathfrak{G}_2 \not\approx D_4$, so ist bereits $F = \mathrm{Z}\mathfrak{G}_2 \approx C_2$. Unter Berücksichtigung beider Fälle betrachten nun den Zentralisator $\mathrm{C}_\mathfrak{G}F$ mit dem Ziel, eine semidirekten Produktdarstellung

$$\mathrm{C}_\mathfrak{G}F = \mathrm{O}C_\mathfrak{G}F \cdot \mathfrak{G}_2 \approx \mathrm{O}C_\mathfrak{G}F \rtimes \mathfrak{G}_2$$

zu beweisen. Hierfür benötigen wir das nächste

Lemma 3.11. *Sei $F \leq Z\mathfrak{G}_2$ von Ordnung 2 und $R = O^2C_\mathfrak{G}F$ der von den $2'$-Elementen aus $C_\mathfrak{G}F$ erzeugte Normalteiler. Dann ist R ebenfalls eine $2'$-Gruppe und daher ein normales 2-Komplement von $C_\mathfrak{G}F$.*

Beweis. Da R von den Elementen ungerader Ordnung aus $\mathrm{C}_{\mathfrak{G}}F$ erzeugt wird, muss auch jede Faktorgruppe von R durch Elemente ungerader Ordnung erzeugt werden. Insbesondere besitzt R keinen Normalteiler $N \lhd R$ mit Index $[R : N] = 2$. Wir nehmen nun an, die Ordnung von R wäre gerade und erzeugen daraus einen Widerspruch. Sei dazu $R_2 \leq R$ eine Sylowgruppe. Diese ist unter der Annahme nicht trivial und als 2-Gruppe in einer 2-Sylowgruppe von $\mathfrak{G}$ enthalten. Somit ist R_2 entweder zyklisch oder eine Diedergruppe. Wir betrachten beide Fälle separat.

Fall 1. Sei zunächst R_2 zyklisch. Dann ist $\mathrm{Aut}R_2$ ebenfalls eine 2-Gruppe und da wegen $R_2 \leq \mathrm{Z}C_R R_2 \leq \mathrm{C}_R R_2$ die Faktorgruppe $\frac{\mathrm{N}_R R_2}{\mathrm{C}_R R_2} \hookrightarrow \mathrm{Aut}R_2$ ungerader Ordnung hat, ist sie trivial und somit $\mathrm{N}_R R_2 = \mathrm{C}_R R_2$. Wir schließen also $R_2 \leq \mathrm{Z}C_R R_2 = \mathrm{Z}N_R R_2$ und nach Satz 2.3 besitzt R dann ein normales 2-Komplement $S \lhd R$ mit

$$R = SR_2 \approx S \rtimes R_2.$$

Da R_2 zyklisch ist, können wir den eindeutige Normalteiler $T \lhd R_2$ mit Index $[R_2 : T] = 2$ betrachten. Dann haben wir mit

$$N = ST \approx S \rtimes T \leq S \rtimes R_2 \approx R$$

eine Untergruppe vom Index $[R : N] = 2$ und somit einen Widerspruch.

Fall 2. Sei nun nun $R_2 \approx \langle x \rangle \rtimes \langle y \rangle$ eine Diedergruppe. Dann enthält R_2 mindestens drei voneinander verschiedene Involutionen und $\langle x \rangle$ ist eine maximale echte Untergruppe der Sylowgruppe R_2, die jedoch nur eine Involution enthält. Nach Lemma 3.6 wird $\langle x \rangle$ von jeder Konjugationsklasse der Involutionen in R geschnitten. Da aber $\langle x \rangle$ nur eine einzige Involution enthält sind bereits alle Involutionen in R durch Konjugation mit Elementen aus R konjugiert.

Da $R = \mathrm{O}^2 C_{\mathfrak{G}}F$ ein Normalteiler in $\mathrm{C}_{\mathfrak{G}}F$ ist, sind alle Konjugierten R_2^g mit $g \in \mathrm{C}_{\mathfrak{G}}F$ wieder in R enthalten. Wegen $\mathfrak{G}_2 \leq \mathrm{C}_{\mathfrak{G}}F$ und $R_2 \leq R \trianglelefteq \mathrm{C}_{\mathfrak{G}}F$ gibt es demnach ein $g \in \mathrm{C}_{\mathfrak{G}}F$ derart, $R_2^g \leq \mathfrak{G}_2$ respektive $R_2^g = R \cap \mathfrak{G}_2$. Da jede Vierergruppe in $\mathfrak{G}_2$ das Zentrum $\mathrm{Z}\mathfrak{G}_2$ enthält, ist insbesondere $F \leq R_2^g \leq R$. Da F von R zentralisiert wird, und in R alle Involutionen konjugiert sind, besitzt R nur eine einzige Involution. Das steht im Widerspruch zu den drei voneinander verschiedenen Involutionen in R_2.

□

Wir können nun die Zerlegung des Zentralisators $\mathrm{C}_{\mathfrak{G}}F$ in ein semidirektes Produkt be-

weisen, in der $\mathfrak{G}_2$ ein normale 2-Komplement vervollständigt.

Lemma 3.12. *Sei $F \leq Z\mathfrak{G}_2$ von Ordnung 2. Dann gilt*

$$C_{\mathfrak{G}}F = OC_{\mathfrak{G}}F \cdot \mathfrak{G}_2 \approx OC_{\mathfrak{G}}F \rtimes \mathfrak{G}_2.$$

Beweis. Wir betrachten wieder den Normalteiler $R = \mathrm{O}^2\mathrm{C}_{\mathfrak{G}}F$. Nach dem eben bewiesenen Lemma 3.11 ist R von ungerader Ordnung. Daher ist R insbesondere im größten ungeraden Normalteiler $\mathrm{O}C_{\mathfrak{G}}F$ enthalten und $R \cap \mathfrak{G}_2 = e$. Da aber R per Konstruktion eine Zweierpotenz als Index in $\mathrm{C}_{\mathfrak{G}}F$ besitzt und $\mathfrak{G}_2 \leq \mathrm{C}_{\mathfrak{G}}F$ eine Sylowgruppe ist, folgt $|R|\,|\mathfrak{G}_2| \geq |R\mathfrak{G}_2| = |\mathrm{C}_{\mathfrak{G}}F|$. Damit ist $R = \mathrm{O}C_{\mathfrak{G}}F$ und $\mathrm{C}_{\mathfrak{G}}F = \mathrm{O}C_{\mathfrak{G}}F \cdot \mathfrak{G}_2$. □

Mit der semidirekten Zerlegung können wir sofort die Lage der Sylowgruppen ungerader Ordnung von $\mathrm{C}_{\mathfrak{G}}F$ eingrenzen.

Korollar 3.9. *Sei $F \leq Z\mathfrak{G}_2$ von Ordnung 2 und p eine ungerade Primzahl. Dann ist jede p-Sylowgruppe L von $C_{\mathfrak{G}}F$ bereits in $OC_{\mathfrak{G}}F$ enthalten.*

Beweis. Da die höchste $|\mathrm{C}_{\mathfrak{G}}F|$ teilende p-Potenz nach Lemma 3.12 auch die Ordnung von $\mathrm{O}C_{\mathfrak{G}}F$ teilt, ist eine p-Sylowgruppe L von $\mathrm{O}C_{\mathfrak{G}}F$ bereits eine Sylowgruppe von $\mathrm{C}_{\mathfrak{G}}F$. Da $\mathrm{O}C_{\mathfrak{G}}F$ ein Normalteiler ist, sind alle Konjugierten L^g mit $g \in \mathrm{C}_{\mathfrak{G}}F$ wieder in $\mathrm{O}C_{\mathfrak{G}}F$ enthalten. □

3.5 Die A_4 in $\mathfrak{G}$ und $\mathfrak{G} \approx A_5$

Wir beenden diesen Hauptabschnitt mit den beiden zentralen Aussagen über $\mathfrak{G}$. Hierfür benötigen wir noch den folgenden

Satz 3.6. *Sei $S \subseteq \mathbb{P}$ eine Menge von Primzahlen, G eine S-Gruppe und $H \leq AutG$ eine S'-Automorphismengruppe von G. Sind dann H oder G auflösbar, so gilt für jeden Primteiler $p \in S$:*

1. *Es gibt eine H-invariante Sylowgruppe $G_p \leq G$.*
2. *Je zwei H-invariante Sylowgruppen in G sind zueinander konjugiert durch ein Element aus $C_G H$.*
3. *Jede H-invariante p-Gruppe in G ist in einer H-invarianten Sylowgruppe G_p enthalten.*

4. Ist N ein H-invarianter Normalteiler von G, so gilt

$$\frac{C_G H \cdot N}{N} = C_{\frac{G}{N}} H.$$

Beweis. Gorenstein [8], S. 224, Theorem 2.2 □

Damit können wir nun die Existenz einer zu A_4 isomorphen Untergruppe von $\mathfrak{G}$ beweisen.

Satz 3.7. *$\mathfrak{G}$ besitzt eine Untergruppe isomorph zu A_4.*

Beweis. Sei A eine Kleinsche Vierergruppe in $\mathfrak{G}_2$. Wir unterscheiden bezüglich der Teiler von $|\mathrm{C}_{\mathfrak{G}} A|$.

Fall 1. Sei $\mathrm{C}_{\mathfrak{G}} A$ eine $3'$-Gruppe. Nach Lemma 3.10 ist eine 3-Sylowgruppe von $\mathrm{N}_{\mathfrak{G}} A$ stets nicht trivial. Sei daher D eine 3-Sylowgruppe von $\mathrm{N}_{\mathfrak{G}} A$. Aus der Annahme folgt dann

$$\mathrm{C}_D A = D \cap \mathrm{C}_{\mathfrak{G}} A = e$$

und somit ist $D \approx \frac{D}{\mathrm{C}_D A} \hookrightarrow \mathrm{Aut} A$ bezüglich der Operation durch Konjugation. Wegen

$$\mathrm{Aut} A \approx \mathrm{Aut} D_4 \approx S_3 \approx C_3 \rtimes C_2$$

folgt $D \approx C_3$. Mit $\mathrm{C}_D A = e$ ist die Operation von D nicht trivial und da es bis auf Äquivarianz nur eine nicht triviale operation von C_3 auf D_4 gibt, ist das Produkt

$$AD \approx A \rtimes D \approx D_4 \rtimes C_3 \approx A_4 \hookrightarrow \mathfrak{G}$$

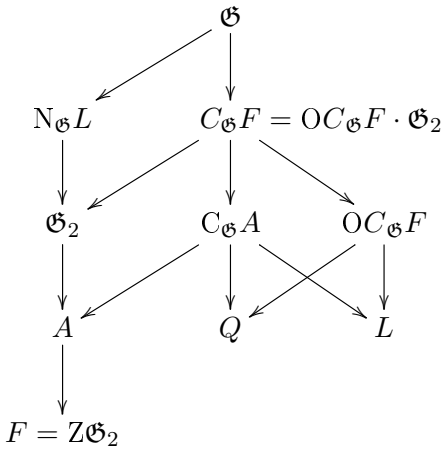
eindeutig und echt semidirekt nach Satz 3.4.

Fall 2. Sei nun die Ordnung von $\mathrm{C}_{\mathfrak{G}} A$ durch 3 teilbar und wieder $F \leq \mathrm{Z}\mathfrak{G}_2 \leq A \leq \mathfrak{G}_2$ von Ordnung 2. Wegen $\mathrm{C}_{\mathfrak{G}} A \leq \mathrm{C}_{\mathfrak{G}} F$ ist die Ordnung von $\mathrm{C}_{\mathfrak{G}} F$ dann ebenfalls durch 3 teilbar.

Wäre $\mathfrak{G}_2 = A$, so folgte mit Lemma 3.5 die Inklusion $\mathrm{C}_{\mathfrak{G}} A = \mathrm{C}_{\mathfrak{G}} \mathfrak{G}_2 \leq \mathfrak{G}_2 = A$. Sie impliziert einen Widerspruch, da die Ordnung von $\mathrm{C}_{\mathfrak{G}} A$ als teilbar durch 3 angenommen wurde. Wir schließen also $A \neq \mathfrak{G}_2$ und somit ist $F = \mathrm{Z}\mathfrak{G}_2 < A < \mathfrak{G}_2$.

Wegen $A < \mathfrak{G}_2 \leq \mathrm{C}_{\mathfrak{G}} F$ sind A und $\mathfrak{G}_2$ jeweils 2-Automorphismengruppe der $2'$-Gruppe $\mathrm{O}C_{\mathfrak{G}} F$. Da $\mathfrak{G}_2$ auflösbar ist, gibt es nach Satz 3.6.1 eine $\mathfrak{G}_2$-invariante und damit auch A-invariante 3-Sylowgruppe L von $\mathrm{O}C_{\mathfrak{G}} F$. Sei nun Q eine

3-Sylowgruppe von $\mathrm{C}_{\mathfrak{G}}A$. Wir haben also folgenden Auszug aus dem Untergruppenverband.



Nach Lemma 3.1 sind L und Q beide zyklisch. Wir wollen zeigen, dass $L = Q$ gilt, wenn man Q durch Konjugation in $\mathrm{C}_{\mathfrak{G}}A$ geeignet wählt. Nach Lemma 3.12 haben wir eine Zerlegung von $\mathrm{C}_{\mathfrak{G}}F$ als semidirektes Produkt

$$Q \leq \mathrm{C}_{\mathfrak{G}}A \leq \mathrm{C}_{\mathfrak{G}}F = \underbrace{\mathrm{O}C_{\mathfrak{G}}F}_{Q\leq} \cdot \mathfrak{G}_2 \approx \mathrm{O}C_{\mathfrak{G}}F \rtimes \mathfrak{G}_2,$$

und nach Korollar 3.9 sind alle Sylowgruppen ungerader Ordnung von $\mathrm{C}_{\mathfrak{G}}F$ bereits in $\mathrm{O}C_{\mathfrak{G}}F$ enthalten. Somit ist auch $Q \leq \mathrm{O}C_{\mathfrak{G}}F$ und wir können zumindest durch Konjugation mit einem Element $g \in \mathrm{O}C_{\mathfrak{G}}F$ erreichen, dass somit $Q^g \leq L$ enthalten ist.

Als Untergruppe des Zentralisators $\mathrm{C}_{\mathfrak{G}}A$ wird Q von A zentralisiert, ist also insbesondere A-invariante Untergruppe $Q \leq \mathrm{O}C_{\mathfrak{G}}F$. Nach Satz 3.6.3 ist Q in einer A-invarianten 3-Sylowgruppe von $\mathrm{O}C_{\mathfrak{G}}F$ enthalten. Aus 3.6.2 wissen wir aber, dass alle A-invarianten Sylowgruppen bereits in $\mathrm{O}C_{\mathfrak{G}}F$ konjugiert sind durch Elemente $\mathrm{C}_{\mathrm{O}C_{\mathfrak{G}}F}A = \mathrm{O}C_{\mathfrak{G}}F \cap \mathrm{C}_{\mathfrak{G}}A \leq \mathrm{C}_{\mathfrak{G}}A$. Wir können also g geeignet finden, so dass $g \in \mathrm{C}_{\mathfrak{G}}A$ und $Q^g \leq L$ gilt. Ohne Einschränkung können und wollen wir daher nun Q derart wählen, dass $Q \leq L$ ist.

Wir erinnern uns, dass L als $\mathfrak{G}_2$-invariant gewählt wurde und zyklisch ist. Nach Lemma 3.2 gilt für die Operation $A \to \mathrm{Aut}L$ dann entweder $\mathrm{C}_L A = L$ oder $\mathrm{C}_L A = e$. Wegen $e \neq L \leq \mathrm{C}_L A$ folgt $\mathrm{C}_L A = L$ und A zentralisiert L. Mithin ist L in einer 3-Sylowgruppe von $\mathrm{C}_{\mathfrak{G}}A$ enthalten. Da aber mit $Q = (\mathrm{C}_{\mathfrak{G}}A)_3$ bereits eine 3-Sylowgruppe in L enthalten ist, folgt somit $L = Q$.

Aus der $\mathfrak{G}_2$-Invarianz von L folgt, dass $\mathfrak{G}_2$ eine Sylowgruppe in $\mathrm{N}_{\mathfrak{G}}L$ ist. Wegen $L = Q$ ist $L \leq \mathrm{C}_{\mathfrak{G}}A$ und $A \leq \mathrm{C}_{\mathfrak{G}}L$. Da $\mathrm{C}_{\mathfrak{G}}L$ normal in $\mathrm{N}_{\mathfrak{G}}L$ ist, erhalten wir daraus schließlich $\left\langle A^{\mathfrak{G}_2} \right\rangle \leq \mathrm{C}_{\mathfrak{G}}L$. Nach Lemma 3.4 wird L durch Konjugation mit einem Element aus $h \in \mathrm{N}_{\mathfrak{G}}L$ invertiert. Da h eine Involution ist, gibt es nach Lemma 3.7 ein zu h konjugiertes Element in $\mathfrak{G}_2$, welches wegen $\mathfrak{G}_2 \leq N_{\mathfrak{G}}L$ ebenfalls L invertiert. Nach Lemma 3.3 gibt es eine Vierergruppe $B \leq \mathfrak{G}_2$, die in $\mathfrak{G}_2$ nicht zu A konjugiert mit $\mathfrak{G}_2 = \left\langle A^{\mathfrak{G}_2} \right\rangle B$. Wegen $\left\langle A^{\mathfrak{G}_2} \right\rangle \in \mathrm{C}_{\mathfrak{G}}L$ muss L schließlich von B invertiert werden. Insbesondere wird L nicht von B zentralisiert.

Wir führen die gesamte bisherige Argumentation des Beweises nun noch einmal mit B an Stelle mit A durch. Falls $\mathrm{O}_{\mathfrak{G}}B$ eine $3'$-Gruppe ist, konstruieren wir analog zum ersten Fall eine Untergruppe isomorph zu A_4. Verfolgen wir hingegen den Fall, dass die Ordnung von $\mathrm{C}_{\mathfrak{G}}B$ durch 3 teilbar ist, erhalten wir im Widerspruch zum ersten Durchlauf des Beweises $\mathrm{C}_L B = L$ und A invertiert L, womit wir fertig sind.

□

Um später noch einmal darauf verweisen zu können, isolieren wir einige Aussagen aus dem Beweis des zweiten Falls als

Korollar 3.10. *Sei $A \leq \mathfrak{G}_2$ eine kleinsche Vierergruppe, die Ordnung des Zentralisators $C_{\mathfrak{G}}A$ durch 3 teilbar, $F \leq Z\mathfrak{G}_2$ zweielementig und L eine $\mathfrak{G}_2$-invariante 3-Sylowgruppe von $OC_{\mathfrak{G}}F$. Dann gelten:*

1. *$A \neq \mathfrak{G}_2$.*
2. *L ist eine 3-Sylowgruppe von $C_{\mathfrak{G}}A$.*
3. *Ist $B \leq \mathfrak{G}_2$ eine Vierergruppe, die in $\mathfrak{G}_2$ nicht zu A konjugiert ist, so wird L von B invertiert.*

Als letzte Vorbereitung, bevor wir den Beweis des $\mathrm{S}L_2(5)$-Theorems in Angriff nehmen können, benötigen wir das folgende hinreichende Kriterium, um $\mathfrak{G} \approx A_5$ zu schließen.

Lemma 3.13. *Gibt es eine eine nicht triviale Involution $x \in \mathfrak{G}$ mit $|C_{\mathfrak{G}}\langle x\rangle| = 4$, so folgt $\mathfrak{G} \approx A_5$.*

Beweis. Sei also $x \in \mathfrak{G}$ eine nicht triviale Involution mit $|\mathrm{C}_{\mathfrak{G}}\langle x\rangle = 4|$. Da alle Involutionen der selben Konjugationsklasse angehören folgt aus $\mathrm{C}_{\mathfrak{G}}\langle x^g\rangle = (\mathrm{C}_{\mathfrak{G}}\langle x\rangle)^g$ für alle

$g \in \mathfrak{G}$, dass sämtliche nicht trivialen Involutionen einen Zentralisator der Ordnung 4 haben und x ist in einer geeigneten Sylowgruppe zentral mit $F = \langle x \rangle$ folgt dann aus Lemma 3.12

$$\mathrm{C}_{\mathfrak{G}} \langle x \rangle = \mathrm{C}_{\mathfrak{G}} F = \underbrace{O C_{\mathfrak{G}} F}_{=e} \cdot \mathfrak{G}_2 = \mathfrak{G}_2$$

für eine geeignete Sylowgruppe $\mathfrak{G}_2$. Aus Lemma 3.8 schließen wir daher $\mathrm{C}_{\mathfrak{G}} \langle x \rangle = \mathfrak{G}_2 \approx D_4$ und dass in $\mathfrak{G}$ alle 2-Elemente bereits Involutionen sind. Ist ferner $g \in \mathfrak{G}$ von gerader Ordnung $|g| = 2q$, so ist g^q eine Involutione und $g \in \mathrm{C}_{\mathfrak{G}} \langle g^q \rangle \approx D_4$. Folglich ist g bereits eine Involution und $q = 1$. Insgesamt sind also alle Elemente in von gerader Ordnung Involutionen.

Seien nun $M \leq \mathfrak{G}$ eine maximale, abelsche Untergruppen von ungerader Ordnung und $b \in M$ ein Element von Primzahlordnung. Dann haben wir $M \leq \mathrm{C}_{\mathfrak{G}} \langle b \rangle$. Gäbe es in $\mathrm{C}_{\mathfrak{G}} \langle b \rangle$ eine Involution i, so hätten wir mit $b \in \mathrm{C}_{\mathfrak{G}} \langle i \rangle$ einen Widerspruch zu $|\mathrm{C}_{\mathfrak{G}} \langle i \rangle| = 4$. Mithin ist $\mathrm{C}_{\mathfrak{G}} \langle b \rangle$ von ungerader Ordnung. Nach Lemma 3.4 wird b von einer Involution z invertiert. Darüber hinaus gilt

$$(\mathrm{C}_{\mathfrak{G}} \langle b \rangle)^z = \mathrm{C}_{\mathfrak{G}} \langle b^z \rangle = \mathrm{C}_{\mathfrak{G}} \left\langle b^{-1} \right\rangle = \mathrm{C}_{\mathfrak{G}} \langle b \rangle ,$$

weshalb $\mathrm{C}_{\mathfrak{G}} \langle b \rangle$ von z normalisiert wird. Aus $|\mathrm{C}_{\mathfrak{G}} \langle z \rangle| = 4$ folgt wegen der ungeraden Ordnung von $\mathrm{C}_{\mathfrak{G}} \langle b \rangle$ schließlich $\mathrm{C}_{\mathrm{C}_{\mathfrak{G}} \langle b \rangle} \langle z \rangle = \mathrm{C}_{\mathfrak{G}} \langle b \rangle \cap \mathrm{C}_{\mathfrak{G}} \langle z \rangle = e$. Somit ist die Konjugation mit z ein fixpunktfreier, involutorischer Automorphismus von $\mathrm{C}_{\mathfrak{G}} \langle b \rangle$. Nach Satz 2.9 ist $\mathrm{C}_{\mathfrak{G}} \langle b \rangle$ somit eine abelsche Gruppe. Aus der Maximalität von M folgt somit $M = \mathrm{C}_{\mathfrak{G}} \langle b \rangle$. Die Gruppe M ist also durch jedes ihrer Elemente von Primzahlordnung eindeutig festgelegt. Insbesondere gilt $M = \mathrm{C}_{\mathfrak{G}} M$.

Haben wir nun eine weitere, von M verschiedene, maximale, abelsche Untergruppe N von $\mathfrak{G}$ mit ungerader Ordnung, so schließen wir indirekt $M \cap N = e$. Wäre nämlich der Durchschnitt nicht leer, könnten wir das zuvor gewählte Element b daraus entnehmen und somit $M = \mathrm{C}_{\mathfrak{G}} \langle b \rangle = \mathrm{C}_{\mathfrak{G}} M = N$ schließen. Mithin ist also $b \notin N$ und $M \cap N = e$.

Als Konsequenz ist jedes $x \in \mathfrak{G}$ von ungerader Ordnung in genau einer maximalen, abelschen Untergruppen ungerader Ordnung enthalten. Die Menge aller $x \in \mathfrak{G}$ von ungerader Ordnung lässt sich somit durch nämliche Untergruppen überdecken, bei einer minimalen Überlappung von e. Dem zufolge wird die Menge der Elemente ungerader Ordnung in entsprechende "gelochte" Untergruppen partitioniert. Wir können hiermit die Elemente von $\mathfrak{G}$ zählen.

Seien dazu $M_1, \ldots, M_k \leq \mathfrak{G}$ Repräsentanten der Konjugationsklassen maximaler, abel-

scher Untergruppen ungerader Ordnung. Da $\mathfrak{G}$ transitiv auf den einzelnen Klassen operiert, besitzt M_ν gerade $\frac{|\mathfrak{G}|}{|\mathrm{N}_\mathfrak{G} M_\nu|}$ verschiedene Konjugierte. Auf diese Weise zählen wir die Elemente von $\mathfrak{G}$ durch

$$|\mathfrak{G}| = 1 + \frac{|\mathfrak{G}|}{|\mathrm{C}_\mathfrak{G} \langle x \rangle|} + \sum_{\nu=1}^{k} \frac{|\mathfrak{G}|}{|\mathrm{N}_\mathfrak{G} M_\nu|} \left(|M_\nu| - 1\right),$$

wobei $\frac{|\mathfrak{G}|}{|\mathrm{C}_\mathfrak{G} \langle x \rangle|} = \frac{|\mathfrak{G}|}{4}$ die Anzahl aller Elemente von gerader Ordnung ist, die nur aus der einzigen Konjugationsklasse der Involutionen besteht, da wir festgestellt haben, dass alle Elemente von gerader Ordnung Involutionen sind.

Wir betrachten nocheinmal die b invertierende und damit M normalisierende Involution z.

Als endliche abelsche Gruppe ist M ein direktes Produkt zyklischer Gruppen. Wir können also das Element $b \in M$ von Primzahlordnung aus jedem direkten Faktor Wählen. Aus $\mathrm{C}_\mathfrak{G} \langle b \rangle = M$ schließen wir daher, dass eine M normalisierende Involution u wegen $M \cap C_\mathfrak{G} \langle u \rangle = e$ auf keinem direkten Faktor von M trivial operiert. Nach Lemma 3.3 wissen wir, dass jeder nicht triviale, involutorische Automorphismus von M alle direkten Faktoren und damit ganz M invertiert, insbesondere also fixpunktfrei ist. Desweiteren kann M nicht von einer Kleinschen Vierergruppe normalisiert werden, da deren drei Involutionen alle als Inversenbildung wirken, aber das Produkt von je zweien nicht trivial ist. Mit $\mathrm{N}_\mathfrak{G} \langle z \rangle = \mathrm{C}_\mathfrak{G} \langle z \rangle \approx D_4$ folgt deshalb

$$\mathrm{N}_{\mathrm{N}_\mathfrak{G} M} \langle z \rangle = \mathrm{N}_\mathfrak{G} M \cap \mathrm{N}_\mathfrak{G} \langle z \rangle = \langle z \rangle .$$

Ist nun y eine weitere M invertierende Involution, so wird M von yz zentralisiert. Das bedeutet $yz = yz^{-1} \in \mathrm{C}_\mathfrak{G} M = M$ und somit $y \in Mz$. Ist umgekehrt $y = nz \in Mz$ und $m \in M$, so folgt $y^2 = e$ und

$$ymy^{-1} = nzmz^{-1}n^{-1} = nm^{-1}n^{-1} = m^{-1}.$$

Folglich ist besteht die Nebenklasse Mz gerade aus allen M invertierenden Involutionen. Wir betrachten nun die Untergruppe $M \langle z \rangle$. Offensichtlich ist $M \langle z \rangle \leq \mathrm{N}_\mathfrak{G} M$ und bezüglich der Operation

$$M \langle z \rangle \hookrightarrow \mathrm{N}_\mathfrak{G} M \to \mathrm{Aut} M$$

ist das Bild von $M \langle z \rangle$ im Zentrum von Aut M enthalten und somit Normalteile. Nach der zuvor gemachten Feststellung besteht $M \langle z \rangle$ aber aus allen Elementen, die entwe-

der M invertieren oder zentralisieren. $M\langle z\rangle$ ist also auch das Urbild des Normalteilers $\left\{\mathrm{id}, m \mapsto m^{-1}\right\} \lhd \mathrm{Aut}M$ und damit selbst ein Normalteiler. Mit dem Frattinischluss angewendet auf $M\langle z\rangle \lhd \mathrm{N}_{\mathfrak{G}}M$ folgt

$$\mathrm{N}_{\mathrm{N}_{\mathfrak{G}}M}\langle z\rangle \cdot M = \langle z\rangle M = \mathrm{N}_{\mathfrak{G}}M$$

und wir erhalten schließlich $|\mathrm{N}_{\mathfrak{G}}M| = 2|M|$. Insbesondere heißt das für die Repräsentanten der Konjugationsklassen $|\mathrm{N}_{\mathfrak{G}}M_\nu| = 2|M_\nu|$.

Damit können wir nun die Zählung der Elemente von $\mathfrak{G}$ zu Ende führen. Wir erhalten somit

$$\begin{aligned} |\mathfrak{G}| &= 1 + \frac{|\mathfrak{G}|}{4} + \sum_{\nu=1}^{k} \frac{|\mathfrak{G}|}{2|M_\nu|}(|M_\nu| - 1) \\ \Longrightarrow \qquad \frac{3}{2} &= \frac{2}{|\mathfrak{G}|} + \sum_{\nu=1}^{k} \frac{|M_\nu| - 1}{|M_\nu|} > \sum_{\nu=1}^{k} \frac{|M_\nu| - 1}{|M_\nu|}. \end{aligned}$$

Die kleinste mögliche Ordnung ist $|M_\nu| = 3$, die zugleich den Term $\frac{|M_\nu|-1}{|M_\nu|}$ minimiert. Da aber bereits $\frac{3}{2} > \frac{2}{3} + \frac{2}{3} + \frac{2}{3} = 2$ ist, folgt $k < 3$. Aus $k = 1$ folgt der Widerspruch

$$|\mathfrak{G}| = \frac{4|M_1|}{|M_1| + 2} = \frac{4|M_1| + 8}{|M_1| + 2} - \frac{8}{|M_1| + 2} = 4 - \frac{8}{|M_1| + 2} \in \mathbb{Q} \setminus \mathbb{N},$$

also ist $k = 2$. Wegen $\frac{3}{2} < \frac{2}{3} + \frac{6}{7} = \frac{32}{21}$ und $\frac{3}{2} < \frac{4}{5} + \frac{4}{5} = \frac{8}{5}$ sind nur die Kombinationen $\{|M_1|, |M_2|\} = \{3\}$ und $\{|M_1|, |M_2|\} = \{3, 5\}$ denkbar.

Aus $|M_1| = |M_2| = 3$ folgt $|\mathfrak{G}| = 12$. Nach Satz 3.7 schließen wir jedoch $\mathfrak{G} \approx A_4 \approx D_2 \rtimes C_3$, womit wir durch die zyklische Faktorgruppe $\frac{\mathfrak{G}}{D_2} \approx C_3$ einen Widerspruch zur Perfektheit von $\mathfrak{G}$ erhalten. Wir schließen also $\{|M_1|, |M_2|\} = \{3, 5\}$ und somit $|\mathfrak{G}| = 60$. □

4 Der Beweis des $\mathrm{S}L_2(5)$-Theorems

4.1 $\mathcal{G} \leq \mathrm{GL}V$ perfekt und fixpunktfrei

Nach den umfangreichen Vorarbeiten können wir nun den Beweis des $\mathrm{SL}_2(5)$-Theorems antreten. Sei dazu von nun an V ein Vektorraum über dem Körper $\mathbb{K}$ und $\mathcal{G} \leq \mathrm{GL}V$ eine perfekte Gruppe fixpunktfreier Vektorraumautomorphismen von V. Ohne Einschränkung können wir dabei $\mathbb{K}$ als algebraisch abgeschlossen annehmen. Ansonsten betrachten wir den algebraischen Abschluss $\overline{\mathbb{K}}$ und die entsprechende Fortsetzung von V zu einem $\overline{\mathbb{K}}$-Vektorraum.

Wir erinnern daran, dass $\mathcal{G}$ nach Satz 2.2 ein Frobeniuskomplement in $V \rtimes \mathcal{G}$ ist und nach Korollar 2.5 die pq-Bedingung erfüllt. Weiterhin sind die 2-Sylowgruppen von $\mathcal{G}$ zyklisch oder verallgemeinerte Quaternionengruppen und alle Sylowgruppen zu ungeraden Primzahlen sind zyklisch. Insbesondere sind dann bereits alle Untergruppen von ungerader Primpotenzordnung zyklisch.

Als ersten Schritt gilt es zu zeigen, dass die zentrale Involution $-e \in \mathrm{GL}V$ als einzige Involution in $\mathcal{G}$ enthalten ist. Wir argumentieren über die Ordnung. Ist die Ordnung von $\mathcal{G}$ ungerade, so erfüllt $\mathcal{G}$ gewiss alle definierenden Eigenschaften von $\mathfrak{G}$ aus dem Abschnitt 3.4. Da wir aber aus Lemma 3.4 gefolgert haben, dass $\mathfrak{G}$ gerade Ordnung hat, würde ein Widerspruch folgen. Mithin ist $\mathcal{G}$ von gerader Ordnung und es gibt daher mindestens eine nicht triviale Involution $t \in \mathcal{G}$. Da $\mathcal{G}$ fixpunktfrei ist, können wir aus der polynomialen Gleichung

$$0 = t^2 - e = (t + e)(t - e)$$

und der Nichttrivialität für ungerade Charakteristik von $\mathbb{K}$ schließen, dass $t = -e$ ist und demnach V von t invertiert wird. Der ungünstige Fall der Charakteristik $\mathrm{char}\,\mathbb{K} = 2$ impliziert $t = e$ und widerspricht der Nichttrivialität von t. Wir können diesen Fall demnach von nun an ausschließen. Mit $t = -e$ wissen wir nun, dass $t \in \mathrm{Z}GLV$ ist und daher $\langle t \rangle$ ein Normalteiler von $\mathrm{GL}V$ ist. Insbesondere haben wir dann

$$\langle t \rangle = \langle -e \rangle \trianglelefteq \mathcal{G} \leq GLV$$

und wir können die Faktorgruppe $\overline{\mathcal{G}} = \frac{\mathcal{G}}{\langle t \rangle}$ betrachten. Wir wollen zeigen, dass $\overline{\mathcal{G}}$ alle Eigenschaften der zuvor betrachteten Gruppe $\mathfrak{G}$ besitzt.

Die Perfektheit von $\mathcal{G}$ vererbt sich auf die Faktorgruppe $\overline{\mathcal{G}}$. Ist $\mathcal{G}_2$ eine zyklische 2-Sylowgruppe von $\mathcal{G}$, so ist auch jede Sylowgruppe $\overline{\mathcal{G}}_2$ von $\overline{\mathcal{G}}$ zyklisch. Haben wir hingegen

eine verallgemeinerte Quaternionengruppen als Sylowgruppe $\mathcal{G}_2 \approx Q_{2^n}$ mit $n \in \mathbb{N}$, so folgt nach Korollar 3.7 stets $\overline{\mathcal{G}}_2 \approx D_{2^{n-1}}$. Demnach sind die geraden Sylowgruppen von $\overline{\mathcal{G}}$ je nach Lage der Dinge entweder zyklisch oder Diedergruppen.

Seien $p, q \in \mathbb{P}$ ungerade Primzahlen, $\overline{\mathcal{U}} \leq \overline{\mathcal{G}}$ eine Untergruppe der Ordnung pq und $\mathcal{U}$ das kanonische Urbild mit $\overline{\mathcal{U}} \approx \frac{\mathcal{U}}{\langle t \rangle}$. Dann gilt für die Ordnung $|\mathcal{U}| = 2pq$ und da $-e$ im Zentrum liegt, ist $\langle -e \rangle$ die einzige 2-Sylowgruppe in $\mathcal{U}$. Mit $\frac{N_{\mathcal{U}}\langle t \rangle}{C_{\mathcal{U}}\langle t \rangle} \approx e$ folgt dann aus Satz 2.4 die Existenz eines normalen 2-Komplements $\mathcal{N} \leq \mathcal{U}$ mit der Ordnung $|\mathcal{N}| = pq$. Da $\mathcal{G}$ die pq-Bedingung erfüllt, ist $\mathcal{N}$ zyklisch und wegen

$$\mathcal{N} \approx \frac{\mathcal{N} \rtimes \langle t \rangle}{\langle t \rangle} \approx \frac{\mathcal{N}\langle t \rangle}{\langle t \rangle} = \frac{\mathcal{U}}{\langle t \rangle} = \overline{\mathcal{U}}$$

ist auch $\overline{\mathcal{U}}$ zyklisch. Wir halten also fest:

1. $\overline{\mathcal{G}}$ ist eine perfekte Gruppe.
2. Die 2-Sylowgruppen $\overline{\mathcal{G}}_2$ von $\overline{\mathcal{G}}$ sind zyklisch oder Diedergruppen.
3. Alle Untergruppen von $\overline{\mathcal{G}}$, deren Ordnung das Produkt zweier ungerader Primzahlen ist, sind zyklisch.

Es lassen sich somit alle $\mathfrak{G}$ betreffenden Ergebnisse aus dem vorherigen Kapitel auch auf $\overline{\mathcal{G}}$ anwenden. Enthält eine Untergruppe $\mathcal{U} \leq \mathcal{G}$ die zentrale Involution, so bezeichnen wir die zugehörige Faktorgruppe $\frac{\mathcal{U}}{\langle t \rangle}$ mit dem Symbol $\overline{\mathcal{U}}$. Umgekehrt versehen wir Untergruppen von $\overline{\mathcal{G}}$ stets mit einem Querstrich, den wir bei dem entsprechenden kanonischen Urbild wiederum weglassen. Es gilt $\overline{\mathcal{G}_2} \approx \overline{\mathcal{G}}_2$ und die Länge des Querstrichs degeneriert in diesem Fall zu einer notationstechnischen Spitzfindigkeit.

Aus Lemma 3.8 folgt nun zunächst, dass die 2-Sylowgruppen von $\overline{\mathcal{G}}$ stets Diedergruppen mit einer Ordnung $\left|\overline{\mathcal{G}}_2\right| \geq 4$ sind. Insbesondere ist also die Ordnung von $\overline{\mathcal{G}}$ mindestens durch 4 teilbar. Da eine zyklische Gruppe keine nicht zyklischen Faktorgruppen besitzt, schließen wir indirekt auf das nächste Lemma.

Lemma 4.1. *Die 2-Sylowgruppen von $\mathcal{G}$ sind verallgemeinerte Quaternionengruppen.*

Nach Satz 3.7 gibt es in $\overline{\mathcal{G}}$ eine Untergruppe isomorph zu A_4. Sei also von nun an $\overline{\mathcal{H}} \leq \overline{\mathcal{G}}$ mit $\overline{\mathcal{H}} \approx A_4$ und $\mathcal{H}$ das kanonische Urbild von $\overline{\mathcal{H}}$ in $\mathcal{G}$. Weiterhin bezeichnen wir ab jetzt $\mathcal{Q} = O_2\mathcal{H}$. Sei nun $\overline{D}$ die Vierergruppe in $\overline{\mathcal{H}}$ und $d \in \overline{\mathcal{H}}$ von Ordnung 3. Dann gilt

$$\overline{\mathcal{H}} = \overline{D}\langle d \rangle \approx D_4 \rtimes C_3$$

Da nicht zyklische Untergruppen verallgemeinerter Quaternionen wieder Quaternionengruppen sind, ist das Urbild der eindeutigen Vierergruppe in $\overline{\mathcal{H}}$ nach Lemma 4.1 eine Quaternionengruppe. Die Vierergruppe in $\overline{\mathcal{H}}$ ist ein Normalteiler, ihr kanonisches Urbild ebenfalls normal. Mit einem beliebigen Element $h \in \mathcal{H}$ der Ordnung 3 haben wir also $\mathcal{H} \approx Q_8 \rtimes C_3$ mit einer nicht trivialen Operation von C_3 auf Q_8. Nach Satz 3.4 folgt damit $\mathcal{H} \approx \mathrm{S}L_2(3)$ und $\mathcal{Q} = \mathrm{O}_2\mathcal{H}$ ist demnach die eindeutig bestimmte Quaternionengruppe in $\mathcal{H}$, die zugleich Sylowgruppe und Normalteiler in $\mathcal{H}$ ist. Für $\mathcal{H}$ gilt außerdem noch $\mathrm{Z}\mathcal{H} = \langle t \rangle = \{\pm e\}$. Da die Charakteristik des Körpers $\mathbb{K}$ von 2 verschieden ist, erhalten wir aus der 4. Aussage von Satz 3.5 das nächste

Korollar 4.1. *Alle $\mathcal{Q}$-invarianten Unterräume von V sind auch $\mathcal{H}$-invariant.*

Wir benötigen nun einige Argumente aus der linearen Algebra. Zunächst zeigen wir die Diagonalisierbarkeit aller Elemente aus $\mathcal{G}$. Anschließend wollen wir einige simultan diagonalisierbare Untergruppen von $\mathcal{G}$ finden.

Lemma 4.2. *Sei $p = \mathrm{char}\,\mathbb{K}$ und $g \in \mathcal{G}$. Dann ist die Ordnung von g teilerfremd zu p und g ist als Vektorraumautomorphismus diagonalisierbar.*

Beweis. Sei n die Ordnung von g. Zunächst zeigen wir $p \nmid n$. Der Fall $p = 0$ ist trivial, da 0 gewiss keine natürliche Zahl teilt. Den Fall $p \neq 0$ zeigen wir indirekt. Wäre andernfalls p ein Teiler von n, so folgte wegen

$$\left(g^{\frac{n}{p}} - e\right)^p = \sum_{\nu=1}^{p} \binom{p}{\nu} g^{\frac{\nu n}{p}} (-e)^{p-\nu} = g^n - e = 0,$$

dass $g^{\frac{n}{p}} - e$ nicht invertierbar ist, folglich besitzt $g^{\frac{n}{p}}$ den Eigenwert 1. Da jedoch $\langle g \rangle \leq \mathcal{G}$ fixpunktfrei ist, folgt bereits $g^{\frac{n}{p}} = e$. Wegen $\frac{n}{p} < n$ ist das ein Widerspruch zu $|g| = n$, also gilt $p \nmid n$.

Die formale Ableitung eines Polynoms $f = \prod (X - n_\nu)^\nu$ besitzt die Gestalt als Produkt $f' = h \cdot \prod (X - n_\nu)^{\nu-1}$, wobei f und h teilerfremde Polynome sind, also keine gemeinsamen Nullstellen besitzen. Da die formale Ableitung des Polynoms $f = X^n - 1 \in \mathbb{K}[x]$ mit $f' = nX^{n-1}$ bereits teilerfremd zu f ist, besitzt $X^n - 1$ keine mehrfachen Nullstellen und zerfällt somit in paarweise verschiedene Linearfaktoren. Als Teiler von f besitzt schließlich auch das Minimalpolynom von g keine mehrfache Nullstellen. Daraus schließen wir, dass die Eigenräume von g mit den verallgemeinerten Eigenräumen zusammen fallen und g somit diagonalisierbar ist. □

Seien nun allgemeiner $\varphi, \psi \in \mathrm{GL}V$ diagonalisierbar und gelte $\varphi\psi = \psi\varphi$. Sei weiterhin λ ein Eigenwert von φ und $x \in \mathrm{Eig}\,(\varphi, \lambda)$ ein zugehöriger Eigenvektor. Wegen

$$\varphi\psi x = \psi\varphi x = \psi\lambda x = \lambda\psi x$$

ist der Eigenraum $\mathrm{Eig}\,(\varphi, \lambda)$ auch ψ-invariant. Per Induktion nach der Dimension schließen wir daraus, dass φ und ψ durch eine geeignete Basistransformation simultan diagonalisiert werden können. Umgekehrt sieht man leicht, dass simultan diagonalisierbare Automorphismen kommutieren. Zwei diagonalisierbare Automorphismen sind also genau dann simultan diagonalisierbar, wenn sie kommutieren. Mit dem selben Argument sieht man induktiv über die Anzahl, dass je n paarweise kommutierende, diagonalisierbare Automorphismen bereits simultan diagonalisiert werden. Insbesondere ist jede abelsche Gruppe diagonalisierbarer Automorphismen bereits simultan diagonalisierbar.

Als Folgerung aus Lemma 4.2 zerfällt V zu jedem $g \in \mathcal{G}$ in eine direkte Summe eindimensionaler, g-invarianter Unterräume

$$V = \bigoplus_{\nu=1}^{\dim V} E_\nu.$$

Die Zerlegung von V und die Lage der Unterräume ist hierbei jedoch von der Wahl des Elementes g abhängig und im Fall mehrdimensionaler Eigenräume nicht eindeutig. Für eine beliebige abelsche Untergruppen $M \leq \mathcal{G}$ ist jedoch eine simultane Diagonalisierung möglich, so dass die direkten Summanden zumindest für alle Elemente in M gleich gewählt werden können.

Korollar 4.2. *Zu jeder abelsche Untergruppe $M \leq \mathcal{G}$ zerfällt V in eine direkte Summe eindimensionaler, M-invarianter Unterräume $V = \bigoplus_\nu E_\nu$. Ist W ein M-invarianter Unterraum von V, so zerfällt auch W in eine entsprechende direkte Summe.*

4.2 Die $\mathrm{S}L_2\,(3)$ in $\mathcal{G}$

Wir wollen nun die Lage von $\mathcal{H} \approx \mathrm{S}L_2\,(3)$ in $\mathcal{G}$ näher untersuchen. Wir interessieren uns für den sehr speziellen Fall von Untergruppen zwischen $\mathcal{H}$ und $\mathcal{G}$, die einen zweidimensionalen Unterraum von V invariant lassen. Sei daher von nun an hypothetisch $\mathcal{R}$ eine Untergruppe von $\mathcal{G}$ mit $\mathcal{H} \leq \mathcal{R} \leq \mathcal{G}$ und W ein zweidimensionaler, $\mathcal{R}$-invarianter Unterraum von V.

Lemma 4.3. *Für je zwei verschiedene maximale abelsche Untergruppen $M, M^* \leq \mathcal{R}$ gilt*

$M \cap M^* = \mathrm{Z}\mathcal{R}$ und $\mathcal{R}$ wird von maximalen abelschen Untergruppen überdeckt. Für den Index von M gilt $\left|\frac{N_{\mathcal{R}}M}{M}\right| \in \{1,2\}$.

Beweis. Zunächst sei M eine maximale, abelsche Untergruppe von $\mathcal{R}$. Da die Operation von $\mathcal{G}$ auf V fixpunktfrei ist, sind die Operationen $M \hookrightarrow \mathcal{R} \hookrightarrow \mathrm{GL}W$ treu. Demnach können wir M und $\mathcal{R}$ wahlweise auch als Automorphismengruppen von W und bei Wahl einer Basis auch als Gruppen von 2×2 Matrizen mit Einträgen aus $\mathbb{K}$ auffassen. Wegen $t \in \mathrm{Z}\mathcal{G}$ haben wir folgende Inklusionskette von Untergruppen

$$\{\pm e\} = \langle t \rangle = \mathrm{Z}\mathcal{H} \leq \mathrm{Z}\mathcal{R} \leq M \leq \mathcal{R} \hookrightarrow \mathrm{GL}W \approx \mathrm{GL}_2\mathbb{K}.$$

Nach Korollar 3.3 schließen wir, dass $M \hookrightarrow \mathrm{GL}W$ simultan diagonalisierbar ist. Wir können also W zerlegen in eine direkte Summe eindimensionaler, M-invarianter Unterräume $W = E_1 \oplus E_2$. Für alle $m \in M$ gilt nun $(mE_1, mE_2) = (E_1, E_2)$. Wir haben also

$$M \leq \{g \in \mathcal{R} \mid (gE_1, gE_2) = (E_1, E_2)\} =: S \subseteq \mathcal{R}.$$

Man sieht leicht, dass S ein Untergruppe ist und bezüglich einer geeigneten Basis zu einer eine Gruppe von Diagonalmatrizen isomorph ist. Insbesondere ist S daher kommutativ und aus der Maximalität von M folgt dann $M = S$. Weiterhin ist S durch die beiden Unterräume $E_2, E_2 \leq W$ bereits vollständig charakterisiert.

Das Zentrum $\mathrm{Z}\mathcal{R}$ enthält alle Elemente aus $\mathcal{R}$, deren assoziierte Matrizen die skalare Gestalt $\left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right)$ besitzen. Für $m \in M \setminus \mathrm{Z}\mathcal{R}$ ist die assoziierte Matrix daher eine Diagonalmatrix mit zwei verschiedenen Diagonaleinträgen. Die Operationen von M auf E_1 und E_2 sind daher nicht äquivalent und es sind E_1 und E_2 gerade diejenigen eindimensionalen m-invarianten Unterräume von V, deren Durchschnitt mit W nicht trivial ist. Folglich sind E_1 und E_2 als Eigenräume des Elements $m \in M \setminus \mathrm{Z}\mathcal{R}$ bereits bestimmt. Da S wiederum durch E_1 und E_2 festgelegt ist, folgt aus $M = S$, dass M bereits durch die Mitgliedschaft eines einzelnen nicht zentralen Elementes $m \in M \setminus \mathrm{Z}\mathcal{R}$ bereits festgelegt ist. Enthalten zwei maximale, abelsche Untergruppen $M, M^* \leq \mathcal{R}$ ein gemeinsames, nicht zentrales Element $m \in (M \cap M^*) \setminus \mathrm{Z}\mathcal{R}$, so folgt demnach bereits $M = M^*$. Da jede maximale abelsche Untergruppe von $\mathcal{R}$ auch das Zentrum $\mathrm{Z}\mathcal{R}$ enthält, schließen wir

$$M \neq M^* \quad \Longrightarrow \quad M \cap M^* = \mathrm{Z}\mathcal{R}.$$

Jedes nicht zentrale $r \in \mathcal{R}$ ist in genau einer maximalen abelschen Untergruppe enthalten. Die nämlichen Gruppen überdecken $\mathcal{R}$ bei einer paarweisen Überlappung $\mathrm{Z}\mathcal{R}$.

Für die zweite Aussage betrachten wir nun die Operation von $\mathrm{N}_{\mathcal{R}}M$ auf der Menge der eindimensionalen Unterräume von V. Es gilt für beliebige $g \in \mathrm{N}_{\mathcal{R}}M$ und $E_\nu \in \{E_1, E_2\}$

$$MgE_\nu = gM^gE_\nu = gME_\nu = gE_\nu$$

und somit ist $gE_\nu \leq W$ wieder M-invariant und damit $gE_\nu \in \{E_1, E_2\}$. Mithin operiert $\mathrm{N}_{\mathcal{R}}M$ auch auf der zweielementigen Menge $\{E_1, E_2\}$. Der Kern dieser Operation ist M. Daraus schließen wir

$$\frac{\mathrm{N}_{\mathcal{R}}M}{M} \hookrightarrow S_2 \approx C_2 \quad \text{und} \quad \left|\frac{\mathrm{N}_{\mathcal{R}}M}{M}\right| \in \{1, 2\}\,.$$

□

$\mathcal{R}$ operiert durch Konjugation auf der Menge der maximalen abelschen Untergruppen. Seien nun $M_1, \ldots, M_k$ Repräsentanten der Konjugationsklassen maximaler, abelscher Untergruppen von $\mathcal{R}$. Für M_ν, $\nu = 1, \ldots, k$ enthält die zugehörige Klasse dann insgesamt $\left|\frac{\mathcal{R}}{\mathrm{N}_{\mathcal{R}}M_\nu}\right|$ Konjugierte. Wir können also die Elemente von $\mathcal{R}$ anhand der Zugehörigkeit zu den Konjugationsklassen zählen und erhalten somit

$$|\mathcal{R}| = |\mathrm{Z}\mathcal{R}| + \sum_{\nu=1}^{k} \left|\frac{\mathcal{R}}{\mathrm{N}_{\mathcal{R}}M_\nu}\right| (|M_\nu| - |\mathrm{Z}\mathcal{R}|)\,.$$

Wir dividieren durch $|\mathrm{Z}\mathcal{R}|$ und erhalten die Ordnung der Faktorgruppe

$$\begin{aligned}
\left|\frac{\mathcal{R}}{\mathrm{Z}\mathcal{R}}\right| &= \frac{|\mathcal{R}|}{|\mathrm{Z}\mathcal{R}|} = 1 + \sum_{\nu=1}^{k} \frac{|\mathcal{R}|}{|\mathrm{N}_{\mathcal{R}}M_\nu|} \left(\frac{|M_\nu|}{|\mathrm{Z}\mathcal{R}|} - 1\right) \\
&= 1 + \sum_{\nu=1}^{k} \frac{\frac{|\mathcal{R}|}{|\mathrm{Z}\mathcal{R}|}}{\frac{|\mathrm{N}_{\mathcal{R}}M_\nu|}{|M_\nu|} \cdot \frac{|M_\nu|}{|\mathrm{Z}\mathcal{R}|}} \left(\frac{|M_\nu|}{|\mathrm{Z}\mathcal{R}|} - 1\right) \\
&= 1 + \sum_{\nu=1}^{k} \frac{n}{\epsilon_\nu \cdot m_\nu} (m_\nu - 1) = n \qquad (6)
\end{aligned}$$

mit den Abkürzungen

$$n = \left|\frac{\mathcal{R}}{\mathrm{Z}\mathcal{R}}\right| \qquad \epsilon_\nu = \left|\frac{\mathrm{N}_{\mathcal{R}}M_\nu}{M_\nu}\right| \qquad m_\nu = \left|\frac{M_\nu}{\mathrm{Z}\mathcal{R}}\right|.$$

Insgesamt kommen wir zur Gleichung

$$1 - \frac{1}{n} = \frac{n-1}{n} = \sum_{\nu=1}^{k} \frac{m_\nu - 1}{\epsilon_\nu m_\nu}. \tag{7}$$

Laut Lemma 4.3 gilt stets $\epsilon_\nu \in \{1, 2\}$. Die möglichen Belegungen der übrigen Parameter k, n und m_ν mit $\nu = 1, \ldots, k$ werden nachfolgend diskutiert. Dabei gelingt es, die vielen denkbaren Kombinationen auf vier Fälle einzuschränken.

Lemma 4.4. *Für die Belegung der Parameter k, n, ϵ_ν und m_ν mit $\nu = 1, \ldots, k$ sind höchstens die folgenden Fälle möglich:*

1. $k = 2$, $\{(\epsilon_1, m_1), (\epsilon_2, m_2)\} = \{(1, 3), (2, 2)\}$ *und* $n = 12$
2. $k = 3$, $\epsilon_1 = \epsilon_2 = \epsilon_3 = 2$, $\{m_1, m_2, m_3\} = \{2, 3, 3\}$ *und* $n = 12$
3. $k = 3$, $\epsilon_1 = \epsilon_2 = \epsilon_3 = 2$, $\{m_1, m_2, m_3\} = \{2, 3, 4\}$ *und* $n = 24$
4. $k = 3$, $\epsilon_1 = \epsilon_2 = \epsilon_3 = 2$, $\{m_1, m_2, m_3\} = \{2, 3, 5\}$ *und* $n = 60$

Beweis. Zunächst wollen wir k näher eingrenzen. Für $k = 1$ und $\epsilon_1 = 1$ folgt aus Gleichung (7)

$$\frac{n-1}{n} = \frac{m_1 - 1}{m_1} \quad \Longrightarrow \quad n = m_1 \quad \Longrightarrow \quad |\mathcal{R}| = |M_1|$$

und schließlich mit $\mathcal{R} = M_1$ ein Widerspruch, da $\mathcal{H} \approx \mathrm{S}L_2(3)$ nicht kommutativ ist. Für $\epsilon_1 = 2$ erhalten wir wegen

$$\frac{n-1}{n} = \frac{m_1 - 1}{2m_1} \quad \Longrightarrow \quad m_1(n-2) = -n$$

hingegen $n = 1$ und damit den selben Widerspruch $\mathcal{R} = \mathrm{Z}\mathcal{R} = M_1$. Damit ist $k = 1$ widerlegt.

Es gilt stets $m_\nu \geq 2$, da sonst $M_\nu = \mathrm{Z}\mathcal{R} \leq M_i$ für alle i und damit $k = 1$ und wieder $M_1 = \mathrm{Z}\mathcal{R} = \mathcal{R} \geq \mathcal{H}$ folgt. Für $k \geq 4$ können wir daher gemäß Gleichung (7) mit der Abschätzung

$$1 - \frac{1}{n} = \sum_{\nu=1}^{k} \frac{m_\nu - 1}{\epsilon_\nu m_\nu} \geq \frac{1}{2} \sum_{\nu=1}^{k} \frac{2-1}{2} = \frac{1}{2} \sum_{\nu=1}^{4} \frac{1}{2} = 1$$

ein Widerspruch erzeugen und haben damit $k \in \{2, 3\}$ auf zwei mögliche Fälle reduziert. Wir diskutieren nun die Möglichkeiten für die verbleibenden Parameter, beginnend mit ϵ_ν, $\nu = 1, \ldots, k$.

Zunächst betrachten wir den Fall, dass zwei der ϵ_ν gleich 1 sind, etwa $\epsilon_1 = \epsilon_2 = 1$. Dies führt abermals zur widersprüchlichen Abschätzung

$$1 - \frac{1}{n} = \sum_{\nu=1}^{k} \frac{m_\nu - 1}{m_\nu} \geq \sum_{\nu=1}^{2} \frac{m_\nu - 1}{m_\nu} \geq \frac{1}{2} + \frac{1}{2} = 1.$$

Es darf also höchstens ein $\epsilon_\nu = 1$ sein. Ohne Einschränkung nehmen wir daher $\epsilon_1 = 1$ und dementsprechend $\epsilon_\nu = 2$ für alle anderen ν an. Aus der Abschätzung

$$\begin{aligned} \frac{1}{2} + \frac{3-1}{4} = 1 \quad &> \quad 1 - \frac{1}{n} = \sum_{\nu=1}^{k} \frac{m_\nu - 1}{\epsilon_\nu m_\nu} = \frac{m_1 - 1}{m_1} + \sum_{\nu=2}^{k} \frac{m_\nu - 1}{\epsilon_\nu m_\nu} \\ &\geq \quad \frac{m_1 - 1}{m_1} + (k-1)\,\frac{(2-1)}{4} \geq \frac{1}{2} + \frac{(k-1)}{4} \end{aligned}$$

schließen wir dann $k = 2$ und mit

$$\frac{4-1}{4} + \frac{1}{4} = 1 > 1 - \frac{1}{n} \geq \frac{m_1 - 1}{m_1} + \frac{1}{4}$$

schließlich $m_1 \in \{2, 3\}$. Im Falle $m_1 = 2$ haben wir

$$1 - \frac{1}{n} = \frac{1}{2} + \frac{m_2 - 1}{2m_2} = 1 - \frac{1}{2m_2} \quad \Longrightarrow \quad n = 2m_2$$

und M_2 hat Index 2 in R. Da $\mathcal{H}$ keine Untergruppe vom Index 2 besitzt, folgt

$$\frac{\mathcal{H}}{\mathcal{H} \cap M_1} \approx \frac{\mathcal{H} M_1}{M_1} \approx e$$

und damit der Widerspruch $\mathrm{S}L_2(3) \approx \mathcal{H} \leq M_1$. Für $m_1 = 3$ hingegen bekommen wir

$$1 - \frac{1}{n} = \frac{2}{3} + \frac{m_2 - 1}{2m_2} \quad \Longrightarrow \quad n = \frac{6m_2}{3 - m_2},$$

was wegen $n \geq 0$ nur für $m_2 = 2$ sinnvoll ist und $n = 12$ ergibt. Hiermit ist der erste der vier Fälle eingetreten.

Nun betrachten wir die verbliebene Variante, dass alle e_ν gleich 2 sind. Für $k = 2$ erhalten wir abermals aus Gleichung (7)

$$\begin{aligned} 1 - \frac{1}{n} = \frac{m_1 - 1}{m_1} + \frac{m_2 - 1}{m_2} \quad &\Longrightarrow \quad n = \frac{2m_1 m_2}{m_1 + m_2} \\ &\Longrightarrow \quad m_1 n + m_2 n = 2m_1 m_2, \end{aligned}$$

was wegen $m_1, m_2 < n$ den Widerspruch

$$2m_1m_2 < m_1n + m_2n = 2m_1m_2$$

impliziert. Folglich ist $k = 3$ und wir schließen

$$1 - \frac{1}{n} = \sum_{\nu=1}^{3} \frac{m_\nu - 1}{2m_\nu} = \frac{1}{2}\left(\sum_{\nu=1}^{3} 1 - \frac{1}{m_\nu}\right) = \frac{1}{2}\left(3 - \frac{1}{m_1} - \frac{1}{m_2} - \frac{1}{m_3}\right)$$

und somit

$$\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} = 1 + \frac{2}{n}.$$

Wegen $\frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 1$ muss mindestens ein $m_\nu = 2$ sein. Ohne Einschränkung sei also $m_1 = 2$, dann folgt

$$\frac{1}{m_2} + \frac{1}{m_3} = \frac{1}{2} + \frac{2}{n}.$$

Da für $m_2, m_3 \geq 4$ bereits $\frac{1}{m_2} + \frac{1}{m_3} \leq \frac{1}{2}$ ist, muss mindestens ein $m_\nu \leq 3$ sein. Wir dürfen daher $m_2 = \min\{m_2, m_3\} \leq 3$ annehmen. Aus $m_2 = 2$ folgt $n = 2m_3$. Damit hat M_3 den Index 2 in $\mathcal{R}$ und wir erhalten wie eben einen Widerspruch. Also folgt $m_2 = 3$ und somit

$$n = \frac{12m_3}{6 - m_3},$$

was wegen $n > 0$ nur noch $m_3 \in \{3, 4, 5\}$ und dementsprechend $n \in \{12, 24, 60\}$ zulässt, womit die drei übrigen Fälle realisiert wären und der Beweis fertig ist. □

Lemma 4.5. *In den drei letzten Fällen von Lemma 4.4 gibt es stets ein Element der Ordnung 3 in $\mathcal{H}$, welches durch Konjugation mit einem geeigneten Element aus $\mathcal{R}$ invertiert wird. Die Zentrumsfaktorgruppe $\tilde{\mathcal{R}} = \frac{\mathcal{R}}{\mathrm{Z}\mathcal{R}}$ enthält eine Untergruppe isomorph zu A_4.*

Beweis. Jedes 3-Element in $\mathcal{R}$ ist in einer der maximalen, abelschen Untergruppen M_ν, $\nu = 1, \ldots, n$ enthalten. Ist daher $h \in \mathcal{H}$ von Ordnung 3, so können wir den Index ν fixieren, so dass $h \in \mathrm{O}_3 M_\nu \leq M_\nu$ ist. Wegen $h \notin \mathrm{Z}\mathcal{H} = \langle t \rangle = \mathcal{H} \cap \mathrm{Z}\mathcal{R}$ ist insbesondere $h \notin \mathrm{Z}\mathcal{R}$. Daher ist die Ordnung von $\frac{M_\nu}{\mathrm{Z}\mathcal{R}}$ durch 3 teilbar und nach Lemma 4.4 folgt $m_\nu = \left|\frac{M_\nu}{\mathrm{Z}\mathcal{R}}\right| = 3$. Folglich ist $\langle h \rangle$ eine Vertretergruppe was schließlich $M_\nu = \langle h \rangle \cdot \mathrm{Z}\mathcal{R}$ ergibt.

Wegen der Maximalität von M_ν ist $\mathrm{C}_\mathcal{R} M_\nu = M_\nu$, sonst könnte man M_ν durch ein $x \in \mathrm{C}_\mathcal{R} M_\nu \setminus M_\nu$ zu einer echt größeren abelschen Gruppe $M_\nu \langle x \rangle \geq M_\nu$ erweitern. Mit

$\epsilon_\nu = \left|\frac{N_\mathcal{R} M_\nu}{M_\nu}\right| = 2$ schließen wir daraus

$$C_2 \approx \frac{\mathrm{N}_\mathcal{R} M_\nu}{\mathrm{C}_\mathcal{R} M_\nu} = \frac{\mathrm{N}_\mathcal{R} M_\nu}{M_\nu} \hookrightarrow \mathrm{Aut} M_\nu,$$

die Operation von $\mathrm{N}_\mathcal{R} M_\nu$ auf M_ν ist also insbesondere nicht trivial. Da jedoch die Operation auf $\mathrm{Z}\mathcal{R}$ trivial ist, kann wegen $M_\nu = \langle h \rangle \cdot \mathrm{Z}\mathcal{R}$ die Operation auf $\langle h \rangle \approx C_3$ nicht ebenfalls trivial sein. Der einzige nicht triviale Automorphismus von C_3 ist die Inversion, mithin gibt es ein Element in $\mathcal{R}$, welches h invertiert.

Für die zweite Aussage sein $U = \mathcal{H} \cdot \mathrm{Z}\mathcal{R}$, $\tilde{U} = \frac{U}{\mathrm{Z}\mathcal{R}} = \frac{\mathcal{H} \cdot \mathrm{Z}\mathcal{R}}{\mathrm{Z}\mathcal{R}}$ und $\tilde{\mathcal{R}} = \frac{\mathcal{R}}{\mathrm{Z}\mathcal{R}}$. Dann ist $U \leq \mathcal{R}$, dementsprechend $\tilde{U} \leq \tilde{\mathcal{R}}$ und wir schließen

$$A_4 \approx \overline{\mathcal{H}} = \frac{\mathcal{H}}{\langle t \rangle} = \frac{\mathcal{H}}{\mathcal{H} \cap \mathrm{Z}\mathcal{R}} \approx \frac{\mathcal{H} \cdot \mathrm{Z}\mathcal{R}}{\mathrm{Z}\mathcal{R}} = \tilde{U} \leq \tilde{\mathcal{R}} = \frac{\mathcal{R}}{\mathrm{Z}\mathcal{R}}.$$

□

Die Definitionen $U = \mathcal{H} \cdot \mathrm{Z}\mathcal{R}$, $\tilde{U} = \frac{U}{\mathrm{Z}\mathcal{R}}$ und $\tilde{\mathcal{R}} = \frac{\mathcal{R}}{\mathrm{Z}\mathcal{R}}$ wollen wir im Folgenden beibehalten. Für den Index $[\mathcal{R} : U]$ gilt

$$\frac{|\mathcal{R}|}{|U|} = \frac{|\mathcal{R}|}{|\mathcal{H} \cdot \mathrm{Z}\mathcal{R}|} = \frac{\left|\frac{\mathcal{R}}{\mathrm{Z}\mathcal{R}}\right|}{\left|\frac{\mathcal{H} \cdot \mathrm{Z}\mathcal{R}}{\mathrm{Z}\mathcal{R}}\right|} = \frac{\left|\tilde{\mathcal{R}}\right|}{\left|\tilde{U}\right|}.$$

Nach Lemma 4.4 ist $\left|\widetilde{\mathcal{R}}\right| \in \{12, 24, 60\}$. Daher folgt wegen $|A_4| = \overline{\mathcal{H}} = \left|\tilde{U}\right| = 12$ für den Index von $U = \mathcal{H} \cdot \mathrm{Z}\mathcal{R}$ in $\mathcal{R}$ eines von drei möglichen Ergebnissen

$$\frac{|\mathcal{R}|}{|U|} = \frac{\left|\tilde{\mathcal{R}}\right|}{\left|\tilde{U}\right|} = \frac{n}{12} \in \{1, 2, 5\}$$

je nachdem, welchen Wert n annimmt. Aus den vier möglichen Belegungen der Parametern k, n, ϵ_ν und m_ν mit $\nu = 1, \ldots, k$ wollen wir im nächsten Hilfssatz Rückschlüsse auf die möglichen Isomorphietypen von $\tilde{\mathcal{R}}$ schließen.

Lemma 4.6. *$\tilde{\mathcal{R}} = \frac{\mathcal{R}}{\mathrm{Z}\mathcal{R}}$ ist isomorph zu A_4, S_4 oder A_5.*

Beweis. Wir gehen aus von den vier möglichen Belegungen der Zählparameter nach Lemma 4.4 und diskutieren jede für sich in der selben Reihenfolge.

Fall 1. Ohne Einschränkung seien $k = \epsilon_2 = m_2 = 2$, $\epsilon_1 = 1$, $m_1 = 3$ und dem entsprechend $n = 12$. Dann ist der Index von $\mathcal{H} \cdot \mathrm{Z}\mathcal{R}$ in $\mathcal{R}$ gerade 1 und somit $\mathcal{H} \cdot \mathrm{Z}\mathcal{R} = \mathcal{R}$, woraus wir dann schließen

$$\frac{\mathcal{R}}{\mathrm{Z}\mathcal{R}} = \frac{\mathcal{H} \cdot \mathrm{Z}\mathcal{R}}{\mathrm{Z}\mathcal{R}} \approx \frac{\mathcal{H}}{\mathcal{H} \cap \mathrm{Z}\mathcal{R}} = \frac{\mathcal{H}}{\mathrm{Z}\mathcal{H}} \approx PSL_2(3) \approx A_4.$$

Fall 2. Im zweiten Fall folgern wir aus $n = 12$ abermals $\mathcal{H} \cdot \mathrm{Z}\mathcal{R} = \mathcal{R}$. Nach Lemma 4.5 müsste dann aber ein Element der Ordnung 3 in $\mathcal{H}$ bereits durch Konjugation in $\mathcal{H}$ invertiert werden und dementsprechend auch dessen kanonisches Bild in $\overline{\mathcal{H}} \approx A_4$. Da aber nach Korollar 3.6 in A_4 kein Element der Ordnung 3 durch Konjugation invertiert wird, haben wir einen Widerspruch. Der zweite Fall ist somit widerlegt.

Fall 3. Für $n = 24$ ist sind die Indices $\left[\tilde{\mathcal{R}} : \tilde{U}\right] = [\mathcal{R} : U] = 2$ und daher U und $\tilde{U}$ insbesondere Normalteiler in $\mathcal{R}$ respektive $\tilde{\mathcal{R}}$ mit

$$C_2 \approx \frac{\mathcal{R}}{U} \approx \frac{\tilde{\mathcal{R}}}{\tilde{U}} \quad \text{und} \quad \left(\tilde{\mathcal{R}} \setminus \tilde{U}\right)^2 = \frac{(\mathcal{R} \setminus U)^2}{\mathrm{Z}\mathcal{R}} = \frac{U}{\mathrm{Z}\mathcal{R}} = \tilde{U},$$

sowie Operationen

$$\mathcal{R} \to \tilde{\mathcal{R}} \to \mathrm{Aut}\ \tilde{U} \approx \mathrm{Aut}\ A_4.$$

Da nach Satz 3.1 die Automorphismengruppe der A_4 isomorph zu S_4 ist, genügt es zu zeigen, dass der Kern der Operation $\tilde{\mathcal{R}} \to \mathrm{Aut}\ \tilde{U}$ trivial ist. Es folgt dann wegen

$$\left|\tilde{\mathcal{R}}\right| = \left|\mathrm{Aut}\ \tilde{U}\right| = |S_4| = 24 \qquad \Longrightarrow \qquad \tilde{R} \approx S_4$$

und wir sind in dem Fall fertig.

Nach Lemma 4.4 gibt es ein Element $g \in \mathcal{H} \leq U$ der Ordnung 3, welches durch Konjugation mit einem Element $x \in \mathcal{R}$ invertiert wird. Dementsprechend wird $\tilde{g} = g\mathrm{Z}\mathcal{R}$ durch $\tilde{x} = x\mathrm{Z}\mathcal{R}$ invertiert. Wäre $x \in U$, so hätten wir mit

$$\tilde{g}^{\tilde{z}} = (g\mathrm{Z}\mathcal{R})^{x\mathrm{Z}\mathcal{R}} = g^x\mathrm{Z}\mathcal{R} = g^{-1}\mathrm{Z}\mathcal{R} = \tilde{g}^{-1} \in \tilde{U}$$

einen Widerspruch, da innerhalb von $\tilde{U} \approx A_4$ kein Element der Ordnung 3 invertiert wird. Also gilt $x \in \mathcal{R} \setminus U$ und dementsprechend

$$\mathcal{R} = U \uplus xU \quad \textit{mit} \quad (xU)^2 = U.$$

Insbesondere ist $x^2 \in U$ und g wird von x^2 zentralisiert. Ebenso wird $\tilde{g}$ von $\tilde{x}^2$ invertiert, $\tilde{x}^2 \in \tilde{U}$ und

$$\tilde{\mathcal{R}} = \tilde{U} \uplus \tilde{x}\tilde{U} \quad \text{m}it \quad \left(\tilde{x}\tilde{U}\right)^2 = \tilde{U}.$$

Da nach Lemma 3.6 jedoch $C_{\tilde{U}} \langle \tilde{g} \rangle = \langle \tilde{g} \rangle$ ist, folgt $\tilde{x}^2 \in \langle \tilde{g} \rangle$ und die Ordnung von $\tilde{x}^2$ ist daher höchstens 3, womit die Ordnung von $\tilde{x}$ höchstens 6 ist. Für $h = x^3$ ist dann $\tilde{h} = \tilde{x}^3$ eine $\tilde{d}$ invertierende Involution, womit $\left\langle \tilde{h} \right\rangle \approx C_2$ eine Vertretergruppe von $\frac{\tilde{\mathcal{R}}}{\tilde{U}}$ ist. Wir haben also eine semidirekte Zerlegung

$$\tilde{\mathcal{R}} = \tilde{U} \uplus \tilde{h}\tilde{U} = \tilde{U} \uplus \tilde{U}\tilde{h} = \tilde{U} \left\langle \tilde{h} \right\rangle \approx \tilde{U} \rtimes \left\langle \tilde{h} \right\rangle.$$

Wegen $\tilde{g}^{\tilde{h}} = \tilde{g}^{-1}$ ist $\tilde{h} \notin C_{\tilde{\mathcal{R}}}\tilde{U}$ und die Operation von $\tilde{h}$ auf $\tilde{U}$ ist nicht trivial, weshalb die Produktzerlegung echt semidirekt ist. Wegen $\mathrm{Z}A_4 = e$ hat die Operation von $\tilde{U} \approx A_4$ auf sich selbst durch Konjugation einen trivialen Kern. Gäbe es ein Element $\tilde{u} \in \tilde{U}$ derart, dass $\tilde{u}\tilde{h}$ trivial auf $\tilde{U}$ operiert, so hätten wir

$$\tilde{g} = \tilde{u}\tilde{h}\tilde{g}\tilde{h}^{-1}\tilde{u}^{-1} = \tilde{u}\tilde{g}^{-1}\tilde{u}^{-1}$$

und somit würde $\tilde{g}$ von $\tilde{u}$ invertiert, was in $\tilde{U} \approx A_4$ nicht vorkommt. Folglich ist der Kern der Operation von $\tilde{\mathcal{R}} = \tilde{U} \langle h \rangle$ auf $\tilde{U}$ durch Konjugation trivial und wir erhalten schließlich $\tilde{\mathcal{R}} \approx S_4$.

Fall 4. Zuletzt sei $n = 60$, also $\left|\tilde{\mathcal{R}} : \tilde{U}\right| = 5$. Da $\tilde{\mathcal{R}}$ transitiv auf dem 5-elementigen Nebenklassenraum $\tilde{\mathcal{R}}/\tilde{U}$ operiert, haben wir eine Operation $\tilde{R} \to S_5$ mit Kern

$$N = \bigcap_{g \in \tilde{\mathcal{R}}} \tilde{U}^g \trianglelefteq \tilde{U} \approx A_4.$$

In A_4 gibt es nur einen nicht trivialen, echten Normalteiler, dieser ist isomorph zur Vierergruppe D_4. Ist also $N \neq e$, so kommt als nicht trivialer Normalteiler in der A_4 nur der Isomorphietyp $N \approx D_4$ in Frage. In diesem Fall ist allerdings das Bild von $\tilde{\mathcal{R}}$ in S_5 von Ordnung 15, was nicht sein kann, da es in S_5 keine Untergruppe der Ordnung 15 gibt. Für $N = e$ folgt $\tilde{\mathcal{R}} \hookrightarrow S_5$ und das Bild von $\tilde{\mathcal{R}}$ in S_5 hat Ordnung 60, Index 2 und ist daher ein Normalteiler. Die einzige derartige Untergruppe in S_5 ist die alternierende Gruppe A_5.

□

Lemma 4.7. *Sei $E = \langle \mathcal{H}^{\mathcal{R}} \rangle$. Dann gelten:*

1. $E \cap Z\mathcal{R} = \langle t \rangle = Z\mathcal{H} = \mathcal{H} \cap \mathrm{Z}\mathcal{R}$
2. $E = \mathcal{H}$ oder $E \approx SL_2(5)$
3. $C_{\mathcal{R}}E = \mathrm{Z}\mathcal{R} = \mathrm{O}Z\mathcal{R} \cdot \mathrm{Z}\mathcal{H}$

Beweis.

1. Da die Operation von $\mathcal{G}$ auf V fixpunktfrei ist, operiert $\mathcal{R}$ treu auf W. Zu jeder Untergruppe $X \leq \mathcal{R}$ bezeichnen wir die mit X assoziierte Untergruppe von $\mathrm{Aut}W$ mit X_W, also insbesondere $\mathcal{R} \approx \mathcal{R}_W \leq \mathrm{Aut}W$.

   Fassen wir nun $\mathcal{H}_W$ als Matrizengruppe über dem Körper $\mathbb{K}$ auf, so ist nach Lemma 4.2 jedes Element der Ordnung 3 diagonalisierbar, also ähnlich zu einer Matrix der Gestalt $x = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ mit $a^3 = b^3 = 1$. Wegen der Fixpunktfreiheit von $\mathcal{G}$ sind $a, b \neq 1$ und wegen $\mathrm{Z}\mathcal{H} = \langle t \rangle \approx C_2 \approx \mathrm{Z}\mathcal{H}_W$ liegt x nicht im Zentrum, ist also keine Skalarmatrix, sondern $a \neq b$. Da es in $\mathbb{K}$ nur zwei Elemente der Ordnung 3 gibt, folgt $a = b^{-1}$ und damit $\det x = ab = b^{-1}b = 1$. Da nach Satz 3.4 $\mathcal{H}$ von Elementen der Ordnung 3 erzeugt wird, schließen wir $\mathcal{H}_W \leq \mathrm{S}LW$. Wegen der Konjugationsinvarianz der Determinante folgt dann aber auch $\langle \mathcal{H}^{\mathcal{R}} \rangle_W = E_W \leq \mathrm{S}LW$.

   Das Zentrum $\mathrm{Z}GLW$ besteht aus allen Skalarmatrizen. Wir wollen zeigen, dass $(\mathrm{Z}\mathcal{R})_W$ in $\mathrm{Z}GLW$ enthalten ist, also ebenfalls nur skalare Matrizen enthält. Wir gehen indirekt vor, sei also $g \in (\mathrm{Z}\mathcal{R})_W$ nicht skalar. Nach Lemma 4.2 ist g diagonalisierbar und folglich zu einer Matrix der Gestalt $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ mit $\alpha \neq \beta$ ähnlich. Insbesondere besitzt g zwei eindeutige, voneinander verschiedene Eigenräume E_α und E_β. Da g mit allen Elementen aus $\mathcal{R}$ kommutiert, wird jedes Element $r \in \mathcal{R}$ mit g simultan diagonalisiert, besitzt also ebenfalls E_α und E_β als invariante Unterräume. Das bedeutet aber, dass $\mathcal{R}$ zu einer Gruppe von Diagonalmatrizen ähnlich und daher kommutativ ist. Da $\mathcal{H}$ nicht kommutativ ist, folgt damit aus $\mathcal{H} \leq \mathcal{R}$ ein Widerspruch. Mithin gilt $(\mathrm{Z}\mathcal{R})_W \leq \mathrm{Z}GLW$ und wegen $E_W \leq \mathrm{S}LW$ ist jedes Element in $E_W \cap (\mathrm{Z}\mathcal{R})_W$ skalar mit Determinante 1. Wegen

   $$\det(\lambda e) = \lambda^2 = 1 \quad \Longrightarrow \quad \lambda = \pm 1$$

   folgt schließlich $E_W \cap (\mathrm{Z}\mathcal{R})_W = \{\pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\}$ und die erste Aussage ist gezeigt.

2. Für $n \in \{12, 24\}$ hat $U = \mathcal{H} \cdot \mathrm{Z}\mathcal{R}$ den Index 2 in $\mathcal{R}$ und ist folglich ein Normalteiler $U \trianglelefteq \mathcal{R}$. Damit folgt

$$E \cdot \mathrm{Z}\mathcal{R} = \left\langle \mathcal{H}^{\mathcal{R}} \right\rangle \cdot \mathrm{Z}\mathcal{R} = \left\langle (\mathcal{H} \cdot \mathrm{Z}\mathcal{R})^{\mathcal{R}} \right\rangle = \left\langle U^{\mathcal{R}} \right\rangle = \langle U \rangle = U = \mathcal{H} \cdot \mathrm{Z}\mathcal{R}$$

und wegen $E \cap \mathrm{Z}\mathcal{R} = \mathcal{H} \cap \mathrm{Z}\mathcal{R}$ und

$$\frac{|E|\,|\mathrm{Z}\mathcal{R}|}{|E \cap \mathrm{Z}\mathcal{R}|} = |E \cdot \mathrm{Z}\mathcal{R}| = |\mathcal{H} \cdot \mathrm{Z}\mathcal{R}| = \frac{|\mathcal{H}|\,|\mathrm{Z}\mathcal{R}|}{|\mathcal{H} \cap \mathrm{Z}\mathcal{R}|}$$

schließlich $|E| = |\mathcal{H}|$. Da $\mathcal{H}$ eine Untergruppe von E ist, können wir daraus $\mathcal{H} = E$ schließen. Für $n = 60$ ist der Index von U in R gerade 5 und daher U eine maximale Untergruppe von $\mathcal{R}$. Wegen

$$U \leq \left\langle U^{\mathcal{R}} \right\rangle = \left\langle (\mathcal{H}\mathrm{Z}\mathcal{R})^{\mathcal{R}} \right\rangle = \left\langle \mathcal{H}^{\mathcal{R}} \cdot \mathrm{Z}\mathcal{R} \right\rangle = E \cdot \mathrm{Z}\mathcal{R} \leq \mathcal{R}$$

muss schließlich $E \cdot \mathrm{Z}\mathcal{R} = U$ oder $E \cdot \mathrm{Z}\mathcal{R} = \mathcal{R}$ gelten. Im ersten Fall hätten wir aber einen Normalteiler $U \trianglelefteq \mathcal{R}$ und dementsprechend in der Faktorgruppe mit $\tilde{U} \trianglelefteq \tilde{\mathcal{R}}$ ebenfalls einen Normalteiler. Da die alternierende Gruppe A_5 einfach ist, folgt aus $\tilde{U} \approx A_5$ ein Widerspruch und somit $E \cdot \mathrm{Z}\mathcal{R} = \mathcal{R}$. Damit können wir dann schließen

$$\overline{E} = \frac{E}{\langle t \rangle} = \frac{E}{E \cap \mathrm{Z}\mathcal{R}} \approx \frac{E \cdot \mathrm{Z}\mathcal{R}}{\mathrm{Z}\mathcal{R}} = \frac{\mathcal{R}}{\mathrm{Z}\mathcal{R}} = \tilde{\mathcal{R}} \approx A_5.$$

E ist also von Ordnung 120 und $\overline{E}$ ist perfekt. Das bedeutet, für $x \in E$ gibt es $y \in E'$ mit

$$\overline{x} = x\,\langle t \rangle = \{x, xt\} = y\,\langle t \rangle = \{y, yt\}$$

und daher $x = y \in E'$ oder $x = yt$. In der Quaternionengruppe Q_8 kann die zentrale Involution als Kommutator $-e = [i, j]$ geschrieben werden. Wegen der Inklusionen

$$Q_8 \approx \mathcal{Q} \leq \mathcal{H} \leq E$$

ist $t = -e$ demnach ein Kommutator in E. Damit folgt $x = yt \in E'$ und E ist perfekt. Nach Korollar 3.1 folgt damit $E \approx SL_2\,(5)$.

3. Als abelsche Gruppe ist $\mathrm{Z}\mathcal{R}$ ein direktes Produkt seiner Sylowgruppen und wir können die direkten Faktoren zu einer Zerlegung $\mathrm{Z}\mathcal{R} = \mathrm{O}Z\mathcal{R} \cdot \mathrm{O}_2\mathrm{Z}\mathcal{R}$ zusammenfassen. Da $\mathrm{O}_2\mathrm{Z}\mathcal{R}$ mit allen Elementen aus $\mathcal{R}$ vertauscht, ist $\mathrm{O}_2\mathrm{Z}\mathcal{R}$ im Zentrum jeder 2-Sylowgruppe von $\mathcal{R}$ enthalten. Da die 2-Sylowgruppen verallgemeinerte

Quaternionen mit Zentrum $\langle t\rangle$ sind, folgt $\mathrm{O}_2\mathrm{Z}\mathcal{R} = \langle t\rangle$.

□

Die Quaternionengruppe in $\mathcal{H}$ haben wir mit $\mathcal{Q}$ bezeichnet. Sei von nun an $\mathcal{S}$ eine $\mathcal{Q}$ enthaltende 2-Sylowgruppe von $\mathcal{G}$, also $\mathcal{Q} \leq \mathcal{S} = \mathcal{G}_2 \leq \mathcal{G}$ und dementsprechend $\overline{\mathcal{Q}} \leq \overline{\mathcal{S}} \leq \overline{\mathcal{G}}$ die entsprechenden Faktorgruppen. Wir wählen eine zweielementige Untergruppe $\overline{\mathcal{F}} \leq \mathrm{Z}\overline{\mathcal{S}}$ und betrachten ihr kanonisches Urbild $\mathcal{F} \leq \mathcal{G}$. Wegen $|\mathcal{F}| = 4 = 2 \cdot 2$ folgt aus der pq-Bedinugng $\mathcal{F} \approx C_4$. Da $\mathcal{S}$ eine verallgemeinerte Quaternionengruppe ist, haben wir nach Lemma 3.7 als Zentrumsfaktorgruppe $\overline{\mathcal{S}}$ eine Diedergruppe, deren Zentrum entweder von der Drehung um 180° erzeugt wird oder eine Kleinsche Vierergruppe ist. Wir haben also je nach Lage der Dinge $C_2 \approx \overline{\mathcal{F}} = \mathrm{Z}\overline{\mathcal{S}}$ oder eine echte Inklusion $C_2 \approx \overline{\mathcal{F}} < \mathrm{Z}\overline{\mathcal{S}} \approx D_4$. Die Faktorgruppe $\overline{\mathcal{Q}}$ ist eine Vierergruppe in $\overline{\mathcal{S}}$ und da jede Vierergruppe in einer Diedergruppe stets das Zentrum enthält, haben wir die Inklusionenkette von Untergruppen

$$\overline{\mathcal{F}} \leq \mathrm{Z}\overline{\mathcal{S}} \leq \overline{\mathcal{Q}} \leq \overline{\mathcal{S}} = \overline{\mathcal{G}}_2$$

und $\overline{\mathcal{F}}$ wird von einer geeigneten Involution aus $\overline{\mathcal{Q}}$ erzeugt. Wir können weiterhin im Urbild auf die Inklusion $\mathcal{F} \leq \mathcal{Q}$ schließen. Mit $\mathcal{Q} = \{\pm e, \pm i, \pm j, \pm k\}$ ist $\mathcal{F}$ also eine der Gruppen $\langle i\rangle$, $\langle j\rangle$ oder $\langle k\rangle$. Da in Q_8 keines der drei Elemente i, j oder k ausgezeichnet ist, können wir ohne Einschränkung $\mathcal{F} = \langle i\rangle$ schreiben.

Im Fall einer echten Untergruppe $\mathcal{Q} < \mathcal{S}$ ist $\overline{\mathcal{S}}$ keine Vierergruppe. Dann ist $\overline{\mathcal{F}} = \mathrm{Z}\overline{\mathcal{S}} \approx C_2$ eindeutig bestimmt und die Untergruppe $\langle i\rangle$ in $\mathcal{Q}$ ist dadurch ausgezeichnet, dass ihr kanonisches Bild gerade $\mathrm{Z}\overline{\mathcal{S}}$ ergibt. Intuitiv entspricht das nicht der Situation, dass zumindest innerhalb von $\mathcal{Q}$ die Elemente i, j oder k alle gleichberechtigt sind. Tatsächlich werden wir diesen Fall widerlegen und $\mathcal{Q} = \mathcal{S}$ und damit

$$\mathrm{Z}\overline{\mathcal{Q}} = \overline{\mathcal{Q}} = \overline{\mathcal{S}} = \mathrm{Z}\overline{\mathcal{S}} \approx D_4$$

zeigen. Für das folgende Lemma behalten wir die Inklusion $C_4 \approx \mathcal{F} = \langle i\rangle \leq \mathcal{Q} \leq \mathcal{S}$ im Auge. Da in Q_8 jede Untergruppe ein Normalteiler ist, haben wir weiterhin $\mathcal{F} = \langle i\rangle \lhd \mathcal{Q} \trianglelefteq \mathrm{N}_{\mathcal{G}}\mathcal{F}$ zur Verfügung.

Lemma 4.8. *Es gelten $\mathcal{Q} \leq O_2 N_G \mathcal{F}$ und $O^2 N_G \mathcal{F} \leq C_G \mathcal{Q}$.*

Beweis. Sei zunächst $g \in \mathrm{N}_G\mathcal{F}$ und $a \in \mathcal{Q} \setminus \mathcal{F}$. Ohne Einschränkung nehmen wir $a = j$ an, wir haben also $\langle i, a\rangle = \langle i, j\rangle = \mathcal{Q}$. Über das Element g lässt sich nicht sofort absehen, ob es in $\mathcal{Q}$ enthalten ist.

Wir untersuchen die Beziehungen von j und g zueinander. Seien dazu $L = \langle j \cdot j^g \rangle$ und $D = \langle j, j^g \rangle$. Da in $\mathcal{Q}$ jede Untergruppe ein Normalteiler ist, folgt

$$j, g \in \mathrm{N}_{\mathcal{G}}\mathcal{F} \qquad \Longrightarrow \qquad L \leq D \leq \mathrm{N}_{\mathcal{G}}\mathcal{F}$$

und daher sind die Komplexprodukte $\mathcal{F}L$ und $\mathcal{F}D$ Untergruppen mit den Inklusionen

$$\langle t \rangle \leq \mathcal{F}L \leq \mathcal{F}D \leq \mathrm{N}_{\mathcal{G}}\mathcal{F}.$$

Die Operation von j auf $\mathcal{F}$ ist gerade die Umkehrung des Vorzeichens $jij^{-1} = -i$. Für die Operation von g auf $\mathcal{F}$ sind die Fälle $gig^{-1} = i$ oder $gig^{-1} = -i$ denkbar. Im ersten, trivialen Fall folgt sofort $\mathcal{F} \leq \mathrm{C}_G L$. Im zweiten Fall schließen wir

$$\begin{aligned} jg^{-1}jgig^{-1}j^{-1}gj^{-1} &= jg^{-1}j\,(-i)\,j^{-1}gj^{-1} \\ &= jg^{-1}igj^{-1} \\ &= j\,(-i)\,j^{-1} = i \end{aligned}$$

und demnach ebenfalls $\mathcal{F} \leq \mathrm{C}_G L$ so, dass $\mathcal{F}$ und L elementweise kommutieren und daher $\mathcal{F}L$ als Produkt zyklischer Faktoren sogar eine abelsche Gruppe ist. Nach Lemma 4.2 ist $\mathcal{F}L$ damit simultan diagonalisierbar.

Anders liegen hingegen die Dinge bei der Untergruppe $\mathcal{F}D$. Diese Gruppe ist nicht kommutativ, da sie mit $\langle j, i \rangle = \mathcal{Q} \trianglelefteq \mathcal{F}D$ eine Quaternionengruppe enthält. Die Lage von $\mathcal{F}L$ in $\mathcal{F}D$ soll präzisiert werden, wir gehen von der Faktorgruppe $\overline{D}$ aus. Da sie von zwei Involutionen erzeugt wird, ist sie nach Korollar 3.4 eine Diedergruppe

$$\overline{D} = \frac{D}{\langle t \rangle} = \left\langle \overline{j}, \overline{j^g} \right\rangle = \left\langle \overline{j \cdot j^g} \right\rangle \cup \left\langle \overline{j \cdot j^g} \right\rangle \overline{j}.$$

Wir wissen noch nicht, ob t in L enthalten ist. Wir betrachten daher die Gruppe $M = \langle t \rangle L$ und haben mit $\overline{M} = \left\langle \overline{j \cdot j^g} \right\rangle$ schließlich $\overline{D} = \overline{M} \cup \overline{M}\overline{j}$ und der Index von $\overline{M}$ in $\overline{D}$ ist kleiner oder gleich 2. Wir können also abschätzen

$$2 \geq \frac{|\overline{D}|}{|\overline{M}|} = \frac{|\overline{D}|\,|\overline{\mathcal{F}}|}{|\overline{M}|\,|\overline{\mathcal{F}}|} \geq \frac{|\overline{D}|\,|\overline{\mathcal{F}}|}{|\overline{M}|\,|\overline{\mathcal{F}}|} \cdot \frac{|\overline{M} \cap \overline{\mathcal{F}}|}{|\overline{D} \cap \overline{\mathcal{F}}|} = \frac{\frac{|\overline{D}||\overline{\mathcal{F}}|}{|\overline{D} \cap \overline{\mathcal{F}}|}}{\frac{|\overline{M}||\overline{\mathcal{F}}|}{|\overline{M} \cap \overline{\mathcal{F}}|}} = \frac{|\overline{D} \cdot \overline{\mathcal{F}}|}{|\overline{M} \cdot \overline{\mathcal{F}}|}$$

und da $t \in \mathcal{F}D \cap \mathcal{F}L$ ist, folgt

$$2 \geq \frac{\left|\overline{\mathcal{F}} \cdot \overline{D}\right|}{\left|\overline{\mathcal{F}} \cdot \overline{M}\right|} = \frac{\left|\overline{\mathcal{F}D}\right|}{\left|\overline{\mathcal{F}M}\right|} = \frac{\left|\overline{\mathcal{F}D}\right|}{\left|\overline{\mathcal{F}L}\right|} = \frac{|\mathcal{F}D|}{|\mathcal{F}L|}.$$

Dementsprechend hat $\mathcal{F}L$ höchstens den Index 2 in $\mathcal{F}D$. Da $\mathcal{F}D$ nicht kommutativ ist, können wir den Index 1 ausschließen und haben dann durch den Zweierindex eine Normalteilerinklusion $\mathcal{F}L \lhd \mathcal{F}D$ mit

$$\mathcal{F}D = \mathcal{F}L \uplus x\mathcal{F}L = \mathcal{F}L \uplus \mathcal{F}Lx^{-1}$$

für ein beliebiges $x \in \mathcal{F}D \setminus \mathcal{F}L$.

Wir wollen zunächst zeigen, dass $\mathcal{F}D$ einen 2-dimensionalen Unterraum W von V invariant lässt. Da $\mathcal{F}L$ nach Lemma 4.2 simultan diagonalisierbar ist, finden wir zumindest einen 1-dimensionalen $\mathcal{F}L$-invarianten Unterraum W_1 von V. Mit $W_2 = xW_1$ ist dann

$$\begin{aligned} \mathcal{F}LW_2 &= \mathcal{F}LxW_1 = x\mathcal{F}LW_1 = xW_1 = W_2 \\ x\mathcal{F}LW_2 &= \mathcal{F}Lx^{-1}W_2 = \mathcal{F}LW_1 = W_1 \\ x\mathcal{F}LW_1 &= xW_1 = W_2 \end{aligned}$$

und somit permutiert $\mathcal{F}D$ die Unterräume W_1 und W_2. Die direkte Summe $W = W_1 \oplus W_2$ ist demnach ein zweidimensionaler $\mathcal{F}\mathcal{D}$-invarianter Unterraum. Mit $\mathcal{Q} \leq \mathcal{F}D$ ist W insbesondere $\mathcal{Q}$-invariant und nach Lemma 4.1 auch $\mathcal{H}$-invariant. Die zuvor hypothetisch betrachtete Untergruppe $\mathcal{R}$ können wir daher als

$$\mathcal{R} = \langle D, \mathcal{H} \rangle = \langle j^g \mathcal{H} \rangle$$

konkretisieren. Dann ist $\mathcal{R}$ eine Untergruppe zwischen mit $\mathcal{H}$ und $\mathcal{G}$, die einen zweidimensionalen Unterraum W von V invariant lässt. Wir können also Lemma 4.6 auf $\mathcal{R}$ anwenden. Wir wissen auch, dass $\mathcal{R}$ nur dann von $\mathcal{H}$ verschieden ist, wenn j^g nicht bereits in $\mathcal{Q}$ enthalten ist.

Sei nun wie zuvor $E = \left\langle \mathcal{H}^{\mathcal{R}} \right\rangle$. Dann ist E ein Normalteiler in $\mathcal{R}$ und daher insbesondere $\langle j^g \rangle E = E \langle j^g \rangle \leq \mathcal{R}$ mit

$$\left|\langle j^g \rangle E\right| = \frac{\left|\langle j^g \rangle\right| |E|}{\left|\langle j^g \rangle \cap E\right|} = 4\frac{|E|}{\left|\langle j^g \rangle \cap E\right|} \in \{2\,|E|\,, |E|\}\,,$$

je nachdem, ob $j^g \in E$ ist oder nicht. Auf der anderen Seite haben wir

$$\mathcal{R} = \langle j^g \mathcal{H} \rangle = \left\langle j^g \mathcal{H}^{\mathcal{R}} \right\rangle = \langle \langle j^g \rangle E \rangle = \langle j^g \rangle E$$

und somit ist der Index von E in $\mathcal{R}$ gerade 2 oder $E = \mathcal{R}$. Das Element j^g kann nicht im Zentrum $\mathrm{Z}\mathcal{R}$ liegen, weil sonst $\langle j^g \rangle \mathcal{Q}$ keine verallgemeinerte Quaternionengruppe mehr ist. Ist hingegen $j^g b \in \mathrm{Z}\mathcal{R}$ mit $b \in E$, so folgt insbesondere

$$j^g b b^{-1} = b^{-1} j^g b \Longleftrightarrow b j^g = j^g b$$

und daher $(j^g b)^4 = b^4 \in E$. Da nach Lemma 4.7 aber $\mathrm{Z}\mathcal{R} \cap E = \langle t \rangle$ ist, folgt $b^4 \in \langle t \rangle$ und die Ordnung von $j^g b$ ist insbesondere gerade und daher $\mathrm{O}Z\mathcal{R} = e$. Wieder nach Lemma 4.7 haben wir dann aber $\mathrm{Z}\mathcal{R} = \langle t \rangle \cdot \mathrm{O}Z\mathcal{R} = \langle t \rangle$ und wir schließen aus Lemma 4.6, dass die Faktorgruppe

$$\overline{\mathcal{R}} = \frac{\mathcal{R}}{\langle t \rangle} = \frac{\mathcal{R}}{\mathrm{Z}\mathcal{R}} = \tilde{\mathcal{R}}$$

isomorph zu A_4, S_4 oder A_5 ist. Für die Ordnung einer 2-Sylowgruppe von $\mathcal{R}$ haben wir dann die Implikationen

$$\begin{aligned} \overline{\mathcal{R}} \approx A_4 &\implies |\mathcal{R}_2| \approx 8 \\ \overline{\mathcal{R}} \approx S_4 &\implies |\mathcal{R}_2| \approx 16 \\ \overline{\mathcal{R}} \approx A_5 &\implies |\mathcal{R}_2| \approx 8 \end{aligned}$$

und da $\mathcal{F}D$ eine 2-Gruppe in $\mathcal{R}$ ist, kann die Ordnung von $\mathcal{F}D$ nur noch 8 oder 16 sein. Da die 2-Sylowgruppen von $\mathcal{G}$ verallgemeinerte Quaternionen sind und $\mathcal{F}D$ nicht kommutativ ist, folgt mit Korollar 3.7 entweder $\mathcal{F}D = \mathcal{Q}$ oder $\mathcal{Q} < \mathcal{F}D \approx Q_{16}$. Betrachten wir die Normalisatoren von $\overline{\mathcal{F}} \approx C_2$ in $\overline{\mathcal{R}}$, so folgt aus Korollar 3.5 in allen drei Fällen, dass $\mathrm{N}_{\overline{\mathcal{R}}}\overline{\mathcal{F}}$ eine 2-Gruppe ist. Damit ist auch $\mathrm{N}_{\mathcal{R}}\mathcal{F}$ eine 2-Gruppe und daher isomorph zu Q_8 oder Q_{16}. Da $\mathrm{N}_{\mathcal{R}}\mathcal{F}$ somit höchstens die Ordnung 16 besitzt, sind schließlich $\mathcal{Q}, \mathcal{Q}^g \trianglelefteq \mathrm{N}_{\mathcal{R}}\mathcal{F}$ und damit insbesondere $\mathcal{Q} \cdot \mathcal{Q}^g = \mathcal{Q}^g \cdot \mathcal{Q} \trianglelefteq \mathrm{N}_{\mathcal{R}}\mathcal{F}$. Da $g \in \mathrm{N}_{\mathcal{G}}\mathcal{F}$ ohne Einschränkung gewählt wurde, folgt daher

$$\left\langle \mathcal{Q}^{\mathrm{N}_{\mathcal{G}}\mathcal{F}} \right\rangle = \prod_{x \in \mathrm{N}_{\mathcal{G}}\mathcal{F}} \mathcal{Q}^x \trianglelefteq \mathrm{N}_{\mathcal{G}}\mathcal{F}.$$

Andererseits ist $\prod_x \mathcal{Q}^x$ eine 2-Gruppe und daher im maximalen 2-Normalteiler $\mathrm{O}_2\mathrm{N}_{\mathcal{G}}\mathcal{F}$ enthalten. Damit ist die erste Aussage bewiesen.

$\mathrm{O}^2\mathrm{N}_{\mathcal{G}}\mathcal{F}$ ist der von den Elementen ungerader Ordnung erzeugte Normalteiler. Wegen

$F \approx C_4$ und $\mathrm{Aut}C_4 \approx C_2$ wird $\mathcal{F}$ von jedem Element ungerader Ordnung in $\mathrm{N}_\mathcal{G}\mathcal{F}$ zentralisiert. Folglich wird $\mathcal{F}$ von $O^2\mathrm{N}_\mathcal{G}\mathcal{F}$ zentralisiert. □

Lemma 4.9. *Die 2-Sylowgruppen $\mathcal{G}_2$ sind isomorph zu Q_8. Insbesondere ist $\mathcal{S} = \mathcal{Q}$.*

Beweis. Es genügt zu zeigen, dass $\mathcal{S} = \mathcal{Q}$ ist. Wir nehmen an, das wäre nicht der Fall, also $\mathcal{Q} < \mathcal{S}$. Dann können wir schreiben $Q_{2^n} \approx \mathcal{S} = \langle h, k\rangle$ mit $n \geq 4$ und $\langle h\rangle \approx C_{2^{n-1}}$ ist vom Index 2 in $\mathcal{S}$, also ein Normalteiler. Weiterhin ist die Zentrumsfaktorgruppe $\overline{\mathcal{S}}$ eine 2-Diedergruppe mit einer Ordnung mindestens 8. Nach Lemma 3.3 gibt es dann in $\overline{\mathcal{S}}$ zwei Konjugationsklassen von Vierergruppen und dementsprechend im Urbild zwei Klassen von Quaternionengruppen der Ordnung 8. Sei also $B \approx Q_8$ eine Quaternionengruppe in $\mathcal{S}$, die nicht zu $\mathcal{Q}$ konjugiert ist. Da jede Vierergruppe in $\overline{S}$ das Zentrum enthält, folgt $\overline{\mathcal{F}} \leq Z\overline{\mathcal{S}} \leq \overline{B} \approx D_4$ und daher $\mathcal{F} \leq B$ und des Weiteren $B \cap \mathcal{Q} = \mathcal{F}$, da $\mathcal{F}$ jeweils in $\mathcal{Q}$ und B maximal ist. Wir unterscheiden nun zwei Fälle.

Fall 1. Wir nehmen an, B ist in einer zu $\mathrm{S}L_2(3)$ isomorphen Untergruppe $\mathcal{H}^* \leq \mathcal{G}$ enthalten.

Dann gelten alle Aussagen über $\mathcal{Q}$ und $\mathcal{H}$ auch uneingeschränkt für B und $\mathcal{H}^*$. Die Untergruppe $\langle h\rangle \lhd \mathcal{S}$ ist ein Normalteiler vom Index 2, also $\mathcal{S} = \langle h\rangle \uplus k\langle h\rangle$. Nach Lemma 4.2 ist $\langle h\rangle$ simultan diagonalisierbar und wie im Beweis von Lemma 4.8 konstruieren wir dann aus einem 1-dimensionalen h-invarianten Unterraum W_1 einen 2-dimensionalen $\mathcal{S}$-invarianten Unterraum $W = W_1 \oplus kW_1$. Mit $B, \mathcal{Q} \leq \mathcal{S}$ ist W dann trivialerweise auch $\mathcal{Q}$- und B-invariant. Aus Lemma 4.1 folgt damit aber auch die $\mathcal{H}$- und $\mathcal{H}^*-$Invarianz von W. Definieren wir nun $\mathcal{R}^* = \langle \mathcal{H}^*, \mathcal{H}, \mathcal{S}\rangle$, so ist W insgesamt $\mathcal{R}^*$-invariant. Da nach Lemma 4.7 wegen $\mathrm{Z}\mathcal{R} = \mathrm{O}Z\mathcal{R} \cdot \mathrm{Z}\mathcal{H}$ die maximale 2-Potenz in $|\mathrm{Z}\mathcal{R}|$ gerade 2 ist, folgt mit

$$|\mathcal{Q}B| = \frac{|\mathcal{Q}|\,|B|}{|\mathcal{Q} \cap B|} = \frac{64}{|\mathcal{F}|} = 16 = 2^4 \leq |\mathcal{S}| \leq |\mathcal{R}^*|$$

aus Lemma 4.6 schließlich, dass 2^3 die Ordnung von $\frac{\mathcal{R}^*}{Z(\mathcal{R}^*)}$ teilt und daher $\frac{\mathcal{R}^*}{Z(\mathcal{R}^*)} \approx S_4$ ist. Wegen

$$\frac{\mathcal{H} \cdot \mathrm{Z}\mathcal{R}}{\mathrm{Z}\mathcal{R}} \approx \frac{\mathcal{H}}{\mathcal{H} \cap \mathrm{Z}\mathcal{R}} = \frac{\mathcal{H}}{\langle t\rangle} = \overline{\mathcal{H}} \approx A_4 \approx \overline{H^*} = \frac{\mathcal{H}^*}{\langle t\rangle} = \frac{\mathcal{H}^*}{\mathcal{H}^* \cap \mathrm{Z}\mathcal{R}} \approx \frac{\mathcal{H}^* \cdot \mathrm{Z}\mathcal{R}}{\mathrm{Z}\mathcal{R}}$$

schließen wir $\mathcal{H} \cdot \mathrm{Z}\mathcal{R} = \mathcal{H}^* \cdot \mathrm{Z}\mathcal{R}$. Wegen $(\mathrm{S}L_2(3))' \approx Q_8$ folgt durch Übergang

zur Kommutatorgruppe mit

$$\mathcal{Q} = \mathcal{H}' = (\mathcal{H} \cdot \mathrm{Z}\mathcal{R})' = (\mathcal{H}^* \cdot \mathrm{Z}\mathcal{R})' = (\mathcal{H}^*)' = B$$

ein Widerspruch.

Fall 2. Sei nun B nicht in einer zu $\mathrm{S}L_2(3)$ isomorphen Untergruppe enthalten.

Dann ist die Faktorgruppe $\overline{B}$ nicht in einer zu A_4 isomorphen Untergruppe von $\overline{\mathcal{G}}$ enthalten. Aus Lemma 3.10 folgt dann, dass 3 ein Teiler der Ordnung von $\mathrm{C}_{\overline{\mathcal{G}}}\overline{B}$ ist. Sei also $\overline{g} = g\langle t\rangle \in \mathrm{C}_{\overline{\mathcal{G}}}\overline{B}$ von Ordnung 3 und $\kappa \in B$ nicht trivial mit $\overline{\kappa} = \kappa\langle t\rangle$. Dann ist $\kappa^2 = -e$, die Ordnung von g entweder 3 oder 6 und wir haben

$$\overline{g}\,\overline{\kappa}\,\overline{g}^{-1} = g\kappa g^{-1}\langle t\rangle = \kappa\langle t\rangle = \overline{\kappa}.$$

Insbesondere ist dann $g\kappa g^{-1} \in \langle\kappa\rangle$ und g operiert als Automorphismus auf $\langle\kappa\rangle \approx C_4$. Wegen $\mathrm{Aut}\, C_4 \approx C_2$ wird daher κ von g zentralisiert, also $g \in \mathrm{C}_{\mathcal{G}}B$. Dann ist aber die Ordnung von $\mathrm{C}_{\mathcal{G}}B$ ebenfalls durch 3 teilbar. Wegen $\mathcal{F} \leq B$ folgt $\mathrm{C}_{\mathcal{G}}B \leq \mathrm{C}_G\mathcal{F}$ und daher ist auch die Ordnung von $\mathrm{C}_G\mathcal{F}$ durch 3 teilbar. Nach Lemma 4.8 ist aber $\mathrm{O}^2\mathrm{N}_{\mathcal{G}}\mathcal{F} \leq \mathrm{C}_{\mathcal{G}}\mathcal{Q}$ und auch die Ordnung von $\mathrm{C}_G\mathcal{Q}$ ist darum durch 3 teilbar. Nach Lemma 2.6 sind alle 3-Sylowgruppen von $\mathrm{N}_G\mathcal{Q}$ zyklisch. Demnach sind alle Elemente der Ordnung 3 in $\mathrm{N}_G\mathcal{Q}$ sind bereits in $\mathrm{C}_G\mathcal{Q}$ enthalten. Dies ist jedoch ein Widerspruch zu $\mathcal{H} \leq \mathrm{N}_{\mathcal{G}}\mathcal{Q}$.

□

Wir können nun den Beweis des $\mathrm{S}L_2(5)$-Theorems zuende führen. Die letzten Argumente hierfür sind dank der geleisteten Arbeit eher kurz und bündig.

Korollar 4.3. $\mathcal{G} \approx SL_2(5)$

Beweis. Da $\mathcal{Q}$ nach Lemma 4.9 eine 2-Sylowgruppe von $\mathcal{G}$ ist, haben wir mit $\overline{\mathcal{Q}} \approx D_4$ ebenfalls eine 2-Sylowgruppe in $\overline{\mathcal{G}}$. Aus Lemma 3.5 folgt, dass $\mathrm{C}_{\overline{\mathcal{G}}}\overline{\mathcal{Q}}$ eine 2-Gruppe ist und folglich $\mathrm{C}_{\overline{\mathcal{G}}}\overline{\mathcal{Q}} = \overline{\mathcal{Q}}$. Wegen $\overline{\mathrm{C}_{\mathcal{G}}\mathcal{Q}} \leq \mathrm{C}_{\overline{\mathcal{G}}}\overline{\mathcal{Q}}$ ist dann mit $\overline{\mathrm{C}_{\mathcal{G}}\mathcal{Q}}$ auch $\mathrm{C}_{\mathcal{G}}\mathcal{Q}$ eine 2-Gruppe. Da nach 4.8 $\mathrm{O}^2\mathrm{N}_G\mathcal{F} \leq \mathrm{C}_G\mathcal{Q}$ ist, folgt $\mathrm{O}^2\mathrm{N}_G\mathcal{F} = e$ und $\mathrm{N}_{\mathcal{G}}\mathcal{F}$ ist ebenfalls eine 2-Gruppe. Wegen $\mathcal{Q} \leq \mathrm{N}_{\mathcal{G}}\mathcal{F}$ folgt daher $\mathrm{N}_{\mathcal{G}}\mathcal{F} = \mathrm{N}_{\mathcal{G}}\langle i\rangle = \mathcal{Q}$ und offensichtlich gilt $\overline{\mathrm{N}_{\mathcal{G}}\mathcal{F}} = \overline{\mathcal{Q}} \leq \mathrm{C}_{\overline{\mathcal{G}}}\overline{\mathcal{F}}$. Ist nun $\overline{g} = g\langle t\rangle \in \mathrm{C}_{\overline{\mathcal{G}}}\overline{\mathcal{F}}$, so haben wir

$$\{i, it\} = \overline{i} = \overline{g} \cdot \overline{i} \cdot \overline{g}^{-1} = \overline{gig^{-1}} = gig^{-1}\langle t\rangle = \{gig^{-1}, gig^{-1}t\} \subset \mathcal{F}$$

und somit insbesondere $gig^{-1} \in \mathcal{F}$ und $g \in \mathrm{N}_{\mathcal{G}}\mathcal{F}$. Insgesamt ist daher $\mathrm{C}_{\overline{\mathcal{G}}}\overline{\mathcal{F}} = \overline{\mathrm{N}_{\mathcal{G}}\mathcal{F}} = \overline{\mathcal{Q}} \approx D_4$ von Ordnung 4. Nach Lemma 3.13 folgt damit $\overline{\mathcal{G}} \approx A_5$ und zuletzt nach Korollar 3.1 $\mathcal{G} \approx \mathrm{S}L_2(5)$. □

5 Der Satz von Frobenius

Mit dem Letzten Korollar ist das $\mathrm{S}L_2\,(5)$-Theorem bewiesen. Nach den Ausführungen im ersten Abschnitt ist damit auch das Klassifikationsproblem perfekter Frobeniuskomplemente gelöst und das Hauptziel der Arbeit erreicht. Im letzten Hauptabschnitt wollen wir uns wieder der Behandlung allgemeiner Frobeniusgruppen zuwenden und damit auch die letzte Frage im Zusammenhang mit dem Hauptsatz angehen.

Bei dem Beweis der Äquivalenz des $\mathrm{S}L_2\,(5)$-Theorems zum Klassifikationssatz haben wir den Satz von Frobenius vorausgesetzt, dessen Beweis bis heute nicht charakterfrei gelungen ist. Um die Eleganz charaktertheoretischer Methoden zu demonstrieren und um nocheinmal den Fokus auf diese Problematik zu richten, soll diese Arbeit mit einer Päsentation des neuen Beweises von Knapp und Schmid abgeschlossen werden. Die dafür nötigen Begriffe sollen aber nicht mehr entwickelt, sondern als bekannt vorausgesetzt und daher nur kurz vorgestellt werden. Der neue Ansatz in diesem Beweis ist kurz, elegant und wird vermutlich auch Einzug in kommende Lehrbücher erhalten.

5.1 Klassenfunktionen auf Frobeniusgruppen

Gruppencharaktere sind Klassenfunktionen, nehmen also auf den Konjugationsklassen stets die selben Werte an. Die irreduziblen Charaktere einer Gruppe G bilden eine Orthonormalbasis des Vektorraumes der Klassenfunktionen bezüglich des Skalarproduktes

$$\langle \varphi, \psi \rangle_G = \frac{1}{|G|} \sum_{g \in G} \varphi g \cdot \overline{\psi g}$$

und jede Klassenfunktion φ kann daher eindeutig als Linearkombination irreduzibler Charaktere

$$\varphi = \sum_{\chi} a_\chi \chi = \sum_{\chi} \langle \chi, \varphi \rangle \, \chi$$

geschrieben werden. Eine Klassenfunktion ist genau dann ein Charakter, wenn alle Koeffizienten a_χ nicht negative, ganze Zahlen sind.

Das Skalarprodukt schränken wir oft auf Untergruppen $U \leq G$ ein und verändern dabei dessen normierenden Vorfaktor. Wir definieren also

$$\langle \chi, \varphi \rangle_U = \frac{1}{|U|} \sum_{g \in U} \chi g \cdot \overline{\varphi g}.$$

Wegen des neuen Vorfaktors ist $\langle \cdot, \cdot \rangle_U$ streng genommen keine Einschränkung. Wir wollen die Bezeichnung hier trotzdem im verallgemeinerten Sinne verwenden. Eine Einschränkungen der Klassenfunktionen im gewöhnlichen Sinne $\chi\,|_U$ und $\varphi\,|_U$ mit $\langle \chi\,|_U, \psi\,|_U \rangle_U = \langle \chi, \psi \rangle_U$ ist dabei nicht erforderlich.

Sei nun $G = KH$ eine Frobeniusgruppe mit Komplement H und Frobeniuskern K. Die entscheidende Beobachtung ist nun, dass für eine beliebige Klassenfunktion φ die Gleichungen

$$\begin{aligned}\sum_{g\in G} \varphi g &= \sum_{g\in K} \varphi g + \sum_{g\in G\setminus K} \varphi g \\ &= \sum_{g\in K} \varphi g + |K| \sum_{g\in H^\#} \varphi g \\ &= \sum_{g\in K} \varphi g + |K| \sum_{g\in H} \varphi g - |K|\,\varphi e\end{aligned}$$

und daher auch

$$\sum_{g\in K} \varphi g = \sum_{g\in G} \varphi g - |K| \sum_{g\in H} \varphi g + |K|\,\varphi e$$

gilt. Das bedeutet insbesondere für das eingeschränkte Skalarprodukt

$$\langle \varphi, \psi \rangle_K = |H|\,(\langle \varphi, \psi \rangle_G - \langle \varphi, \psi \rangle_H) + \varphi e \cdot \overline{\psi e}. \tag{8}$$

und dementsprechend

$$\langle \varphi, \psi \rangle_G = \frac{\langle \varphi, \psi \rangle_K}{|H|} + \langle \varphi, \psi \rangle_H - \frac{\varphi e \cdot \overline{\psi e}}{|H|} \tag{9}$$

Mit Gleichung (9) wird die Auswertung des Skalarproduktes bezüglich G auf die Einschränkungen auf H und K zurückgeführt. Umgekehrt kann man wegen $\langle \varphi, \psi \rangle_K = \langle \varphi\,|_K, \psi\,|_K \rangle_K$ das Skalarprodukt zweier auf K definierten Klassenfunktion auf die Skalarprodukte beliebiger Fortsetzungen der Klassenfunktionen auf G und H zurückführen. Für die entsprechenden induzierten Normen gilt dann analog

$$|\varphi|_G^2 = \frac{|\varphi|_K^2}{|H|} + |\varphi|_H^2 - \frac{|\varphi e|^2}{|H|}$$

und für die Einschränkung im verallgemeinerten Sinne

$$\langle \varphi, \varphi \rangle_K = |\varphi|_K^2 = |H| \left(|\varphi|_G^2 - |\varphi|_H^2 \right) + |\varphi e|^2 . \tag{10}$$

5.2 Die Beweisidee

Da Normalteiler genau die Kerne von Gruppenhomomorphismen sind, ist es wünschenswert, zu einem Normalteiler $K \trianglelefteq G$ einen Gruppenhomomorphismus anzugeben, dessen Kern gerade K ist, um sich so den Umstand der Normalität von K plausibel zu machen. Der kanonische Homomorphismus $G \to \frac{G}{K}$ leistet dies nicht, da seine Existenz erst durch die Normalteilereigenschaft von K ersichtlich wird, und diese folglich auch nicht transparenter macht.

Die Idee ist es nun, die Existenz einer linearen Darstellung mit Kern K durch die Angabe eines zugehörigen Charakters ψ zu beweisen. Der Kern der Darstellung ist die Klasse aller Elemente, die unter dem zugehörigen Charakter den selben Funktionswert haben wie das neutrale Element. Daher betrachten wir zunächst den einfachsten denkbaren Fall, nämlich die charakteristische Funktion

$$1_K g = \begin{cases} 1 & \text{für } g \in K \\ 0 & \text{sonst} \end{cases}$$

von K. Im Unterabschnitt 2.2 haben wir konstatiert, dass der Frobeniuskern abgeschlossen gegenüber Konjugation ist. Folglich ist K eine Vereinigung von Konjugationsklassen und somit 1_K tatsächlich eine Klassenfunktion. Wir können also

$$1_K = \sum_{\chi} a_\chi \chi$$

schreiben und es gilt für die Koeffizienten

$$a_\chi = \langle \chi, 1_K \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi g \cdot \overline{1_K g} = \frac{1}{|H|\,|K|} \sum_{g \in K} \chi g \cdot \overline{1_K g} = \frac{\langle \chi, 1_K \rangle_K}{|H|}.$$

Um die Division durch $|H|$ zu eliminieren und damit das Auftreten ganzzahliger Koeffizienten zu begünstigen, betrachten wir nun das Vielfache $\psi = |H| \cdot 1_K$ von 1_K mit

$$\psi g = \begin{cases} |H| & \text{für } g \in K \\ 0 & \text{sonst} \end{cases}$$

und haben dann

$$\langle \chi, \psi \rangle_G = |H| \, \langle \chi, 1_K \rangle_G = \langle \chi, 1_K \rangle_K = \langle \chi, 1_G \rangle_K . \tag{11}$$

Wir wollen zeigen, dass durch $\psi = |H| \cdot 1_K$ tatsächlich der Charakter einer geeigneten Darstellung definiert wird. Wir sind also fertig, wenn wir beweisen können, dass in der Linearkombination

$$\psi = \sum_\chi c_\chi \chi = \sum_\chi \langle \chi, \psi \rangle \, \chi$$

alle Koeffizienten $c_\chi = \langle \chi, \psi \rangle$ ganzzahlig und nicht negativ sind. Die Darstellung selbst wird dabei nicht konkretisiert.

5.3 Der Beweis von Knapp und Schmid

Zunächst zeigen wir, dass alle Koeffizienten ganzzahlig sind. Nach den Gleichungen (8) und (11) erhalten wir für die Koeffizienten die Darstellung

$$\begin{aligned} c_\chi &= \langle \chi, \psi \rangle_G \overset{(11)}{=} \langle \chi, 1_K \rangle_K \overset{(11)}{=} \langle \chi, 1_G \rangle_K \\ &\overset{(8)}{=} |H| \left(\langle \chi, 1_G \rangle_G - \langle \chi, 1_G \rangle_H \right) + \chi e \end{aligned}$$

und wir können nun zwei Fälle unterscheiden. Für $\chi = 1_G$ folgt sofort

$$c_{1_G} = \langle 1_G, 1_K \rangle_K = \langle 1_K, 1_K \rangle_K = 1 \in \mathbb{N}.$$

Sei daher nun $\chi \neq 1_G$, dann ist $\langle \chi, 1_G \rangle_G = 0$ und es folgt

$$c_\chi = \langle \chi, 1_K \rangle_K = \chi e - |H| \, \langle \chi, 1_G \rangle_H \in \mathbb{Z}. \tag{12}$$

Es bleibt also nur noch zu zeigen, dass für $\chi \neq 1_G$ auch $c_\chi \in \mathbb{N}$ folgt.

Die nun folgende Argumentation basiert auf einer Abschätzung mit der Ungleichung von Cauchy und Schwarz. Dazu bemerken wir, dass in der bekannten Ungleichung die Differenz der Terme leicht angegeben werden kann. Es ist daher sinnvoll, die Cauchy-Schwarzsche Ungleichung von vornherein auch als Gleichung

$$|\langle x, y \rangle|^2 \leq \left| |y| \, x - \frac{\langle x, y \rangle}{|y|} y \right|^2 + |\langle x, y \rangle|^2 = |x|^2 \, |y|^2 \tag{13}$$

anzugeben. Der Beweis erfolgt dann einfach durch Überprüfung der Gleichheit durch Ausmultiplikation des Differenzterms. Die eigentliche Ungleichung ist zur Ungleichung

$$0 \leq \left| |y| \, x - \frac{\langle x, y \rangle}{|y|} y \right|^2 \tag{14}$$

äquivalent, die offensichtlich richtig ist. In der leicht geänderten Fassung des Beweises nach Müller wird die Ungleichung (14) verwendet und es kann so der Kontext der Cauchy-Schwarzschen Ungleichung abgestreift werden.

Wir betrachten die auf K eingeschränkte Norm $|\cdot|_K$ und wählen $y = 1_K$ und $x = \chi$, damit erhalten wir

$$\begin{aligned} 0 &\leq \left| |1_K|_K \, \chi - \frac{\langle \chi, 1_K \rangle_K}{|1_K|_K} 1_K \right|_K^2 \\ &\overset{(13)}{=} |\chi|_K^2 \, |1_K|_K^2 - |\langle \chi, 1_K \rangle_K|^2 \\ &\overset{(12)}{=} |\chi|_K^2 - c_\chi^2 \\ &\overset{(10)}{=} |H| \left(|\chi|_G^2 - |\chi|_H^2 \right) + |\chi e|^2 - c_\chi^2. \end{aligned} \tag{15}$$

Isolieren wir $|\chi|_G^2$, so erhalten schließlich die hierzu äquivalente Ungleichung

$$|\chi|_H^2 + \frac{c_\chi^2}{|H|} - \frac{|\chi e|^2}{|H|} \leq 1 = |\chi|_G^2 .$$

Es tritt Gleichheit genau dann auf, wenn $\chi \mid_K$ und $1_G \mid_K$ linear abhängig sind. Im rechten Term der Ungleichung (15) sind dann insbesondere alle Summanden identisch Null und daher

$$|\chi e - \langle \chi, 1_G \rangle_K| = |\chi e - c_\chi| = 0.$$

Mithin folgt also $c_\chi = \chi e \in \mathbb{N}_0$ und wir können von nun an eine strikte Ungleichheit

$$|\chi|_H^2 - \frac{|\chi e|^2}{|H|} + \frac{c_\chi^2}{|H|} = |\chi|_H^2 + \frac{|c_\chi|^2 - |\chi e|^2}{|H|} < 1$$

annehmen. Nach Gleichung (12) ist

$$\begin{aligned} |c_\chi|^2 - |\chi e|^2 &= (c_\chi - \chi e)\,(c_\chi + \chi e) \\ &\overset{(12)}{=} -|H| \, \langle \chi, 1_G \rangle_H \, (c_\chi + \chi e) \end{aligned}$$

teilbar durch $|H|$ und daher ist der linke Teil der Abschätzung ganzzahlig. Mithin dürfen wir

$$|\chi|_H^2 - \frac{|\chi e|^2}{|H|} + \frac{c_\chi^2}{|H|} \leq 0$$

folgern und da $\frac{|\chi e|^2}{|H|}$ ein Summand von $|\chi|_H^2$ ist, folgt

$$0 \leq |\chi|_H^2 - \frac{|\chi e|^2}{|H|}$$

und somit schließlich $c_\chi = 0$. Damit ist ψ eine Linearkombination irreduzibler Charaktere mit nicht negativen, ganzzahligen Koeffizienten und somit ein Gruppencharakter. Der Satz von Frobenius ist damit gezeigt und somit der Beweis des Hauptsatzes nun vollständig, allerdings nicht charakterfrei.

Literatur

[1] G. Frobenius, Über auflösbare Gruppen IV, Sitzungsbericht der Königlich-Preußische Akademie der Wissenschaften, Berlin, 1216-1230 (1901)

[2] H. Zassenhaus, Über endliche Fastkörper, Hamb. Abh. 11, 187-220 (1934)

[3] H. Zassenhaus, On Frobenius groups I, Results in Mathematics, Vol. 8, 132-145 (1985)

[4] U. Meierfrankenfeld, Perfect Frobenius complements, Arch. Math. 79, 19-26 (2002)

[5] V. Mazurov, A new proof of Zassenhaus theorem on finite groups of fixed-point-free automorphisms, Journal of Algebra 263 (2003) 1-7, Elsevier Science (USA), 2003

[6] H. Wielandt, Über die Existenz von Normalteilern in endlichen Gruppen, Math. Nachr., **18**, 274-208 (1958)

[7] W. Knapp, P. Schmid, A note on Frobenius groups, J. Group Theory (2009), **12**, 393-400 (2009)

[8] D. Gorenstein, Finite Groups, Harper & Row, New York, 1980

[9] J.G. Thompson, Finite groups with fixed point free automorphisms of prime order, Proc. Natl. Acad. Sci. U.S.A. 45, 578-581 (1959)

[10] S. Lang, Algebra, Revised Third Edition, Springer-Verlag, 2002

[11] M. Suzuki, Group Theory I. Grundlehren Math. 247, Berlin-Heidelberg-New 1982.

[12] M. Suzuki, Group Theory II. Grundlehren Math. 248, Berlin-Heidelberg-New 1986.