
# Konjugationsklassen und Charaktere in endlichen $p$-Gruppen

Diplomarbeit

zur Erlangung des akademischen Grades
Diplom-Mathematiker

Friedrich-Schiller-Universität Jena
Fakultät für Mathematik und Informatik

eingereicht von Benjamin Sambale
geb. am 10. 04. 1985 in Leipzig
Betreuer: Prof. Dr. B. Külshammer

Jena, den 19. November 2008

# Zusammenfassung

Sei $G$ eine endliche $p$-Gruppe für eine Primzahl $p$ und $K$ eine Konjugationsklasse von $G$. Das Produkt $KK^{-1}$ ist dann eine Vereinigung von Konjugationsklassen, und wir bezeichnen mit $\eta(K)$ die Anzahl der Konjugationsklassen in $KK^{-1}$. Wir beweisen in dieser Arbeit, dass in vielen Fällen $\eta(K)$ kongruent zu 1 modulo $p-1$ ist. Gelegentlich benutzen wir dabei das Computeralgebrasystem GAP (siehe [3]). Wir haben bisher kein Gegenbeispiel für diese Aussage gefunden.

Außerdem untersuchen wir ein duales Problem für komplexe Charaktere. Sei dazu $\chi$ ein beliebiger irreduzibler komplexer Charakter von $G$. Dann ist auch $\chi\overline{\chi}$ ein Charakter von $G$, und wir bezeichnen mit $\mathrm{Irr}(\chi\overline{\chi})$ die Menge aller irreduziblen Bestandteile von $\chi\overline{\chi}$. Auch hier zeigen wir in vielen Fällen, dass die Anzahl $|\mathrm{Irr}(\chi\overline{\chi})|$ der Elemente in $\mathrm{Irr}(\chi\overline{\chi})$ kongruent zu 1 modulo $p-1$ ist. Für diese Aussage ist ebenfalls kein Gegenbeispiel bekannt.

# Danksagung

Ich möchte mich an dieser Stelle bei Prof. Dr. Burkhard Külshammer für seine Unterstützung und die Vergabe dieses interessanten Themas bedanken. Außerdem danke ich meiner Freundin Teresa Jenke für ihre Geduld beim Korrekturlesen. Für die finanzielle Unterstützung während meines Studiums danke ich meinen Eltern. Zu guter Letzt möchte ich mich auch bei Jack Schmidt bedanken, der mir freundlicherweise zwei GAP-Dateien mit den Gruppen der Ordnung $3^7$ bzw. $5^7$ zur Verfügung stellte.

# Inhaltsverzeichnis

**Zusammenfassung** **2**

**Einleitung** **5**

**1 Grundlagen** **7**
1.1 Endliche $p$-Gruppen . . . . . 7
1.2 Konjugationsklassen . . . . . 9
1.3 Darstellungen und Charaktere . . . . . 10

**2 Problemstellung für Konjugationsklassen** **14**
2.1 Formulierung der Probleme . . . . . 14
2.2 Resultate . . . . . 15
2.3 Gruppen der Ordnung $p^6$ . . . . . 22
2.4 Metazyklische $p$-Gruppen . . . . . 33

**3 Problemstellung für Charaktere** **35**
3.1 Formulierung des Problems . . . . . 35
3.2 Resultate . . . . . 35

**Literaturverzeichnis** **40**

# Einleitung

Diese Arbeit wurde durch zwei Resultate über Konjugationsklassen bzw. Charaktere in endlichen $p$-Gruppen von Edith Adan-Bante motiviert. Wir möchten diese Ergebnisse hier kurz vorstellen. Sei dazu $G$ eine endliche $p$-Gruppe für eine Primzahl $p$ und $K$ eine Konjugationsklasse von $G$. Offenbar ist dann $KK^{-1}$ eine Vereinigung von Konjugationsklassen. Adan-Bante hat in [2] die Anzahl $\eta(K)$ der Konjugationsklassen in $KK^{-1}$ studiert. Sie hat unter anderem gezeigt, dass im Fall $|K| = p^n$ für ein $n \in \mathbb{N}_0$ stets $\eta(K) \geq n(p-1)+1$ gilt. Außerdem hat sie bewiesen, dass man diese Ungleichung im Allgemeinen nicht verbessern kann, indem sie für jede Primzahl $p$ und jedes $n \in \mathbb{N}_0$ eine endliche $p$-Gruppe $G$ mit einer Konjugationsklasse $K$ der Länge $p^n$ konstruiert hat, in der $\eta(K) = n(p-1)+1$ gilt. In diesen Gruppen ist offensichtlich auch $\eta(K) \equiv 1 \pmod{p-1}$. Lászlo Héthelyi und Burkhard Külshammer haben sich daher in [4] gefragt, ob die Kongruenz $\eta(K) \equiv 1 \pmod{p-1}$ möglicherweise für alle Konjugationsklassen $K$ einer beliebigen endlichen $p$-Gruppe richtig ist. Diese Vermutung bezeichnen wir mit (P1). Für die Untersuchung von (P1) stellen wir mit Hilfe der sogenannten Klassenmultiplikationskonstanten eine weitere Vermutung (P3) auf: Für eine endliche $p$-Gruppe $G$ und Konjugationsklassen $K$ und $L$ von $G$ gilt stets $c_{KK^{-1}L} = 0$ oder $c_{KK^{-1}L} \equiv 1 \pmod{p-1}$. Wir werden uns überlegen, dass man (P1) aus (P3) folgern kann, und daher oft versuchen (P3) zu beweisen. Im ersten Kapitel werden wir die dafür notwendigen Begriffe im Zusammenhang mit endlichen $p$-Gruppen, Konjugationsklassen, Darstellungen sowie Charakteren einführen. Anschließend wird in Kapitel 2 die Vermutung (P3) unter anderem für folgende Spezialfälle bewiesen:

- $p = 2$ (trivial)
- $|G| = p^n$ mit $n \geq 2$ und $|K| \in \{1, p, p^{n-2}\}$
- $G$ hat Nilpotenzklasse kleiner gleich 2
- $G$ besitzt einen abelschen Normalteiler vom Index $p$
- $|G| \leq p^6$
- $G$ ist metazyklisch

Im Gegensatz dazu haben wir mit Hilfe von GAP eine Gruppe der Ordnung $3^7$ gefunden, in der (P3) nicht mehr für jede Konjugationsklasse erfüllt ist. Allerdings beweisen wir auch, dass (P1) für alle 3-Gruppen gilt. Bislang ist kein Gegenbeispiel für die Vermutung (P1) bekannt.

Im dritten Teil der Arbeit studieren wir ein duales Problem für Charaktere in endlichen $p$-Gruppen. Ist $\chi$ ein beliebiger irreduzibler komplexer Charakter einer endlichen $p$-Gruppe $G$, so weiß man aus der Darstellungstheorie, dass auch $\chi\overline{\chi}$ wieder ein Charakter von $G$ ist. Folglich kann man $\chi\overline{\chi}$ als ganzzahlige Linearkombination irreduzibler Charaktere von $G$ schreiben. Die dabei auftretenden irreduziblen Bestandteile fassen wir in der Menge $\mathrm{Irr}(\chi\overline{\chi})$ zusammen. In [1] untersuchte Adan-Bante die Anzahl dieser irreduziblen Bestandteile. Im Fall $\chi(1) = p^n$ mit $n \in \mathbb{N}_0$ hat sie gezeigt, dass stets $|\mathrm{Irr}(\chi\overline{\chi})| \geq 2n(p-1)+1$ gilt. Wie bei ihrem Resultat über Konjugationsklassen konnte sie auch hier zeigen, dass die Ungleichung optimal ist. Dafür konstruierte sie wieder für jede Primzahl $p$ und jedes $n \in \mathbb{N}_0$ eine endliche $p$-Gruppe mit einem irreduziblen Charakter $\chi$ vom Grad $n$, sodass $|\mathrm{Irr}(\chi\overline{\chi})| = 2n(p-1)+1$ gilt. Insbesondere ist in diesen Gruppen $|\mathrm{Irr}(\chi\overline{\chi})| \equiv 1 \pmod{p-1}$. Daher haben Héthelyi und Külshammer auch hier vermutet, dass die Kongruenz $|\mathrm{Irr}(\chi\overline{\chi})| \equiv 1 \pmod{p-1}$ in größerer Allgemeinheit gilt. Diese Vermutung wird in der Arbeit mit (P4) bezeichnet. Wir werden (P4) unter anderem in folgenden Spezialfällen beweisen:

- $p = 2$ (trivial)
- $p = 3$
- $\chi(1) \in \{1, p\}$
- $G$ besitzt einen abelschen Normalteiler vom Index $p$
- $G$ hat Nilpotenzklasse kleiner gleich 2
- $\chi(1)^2 = |G : \mathrm{Z}(\chi)|$
- $|G| \leq p^5$
- $G' \subseteq \mathrm{Z}(\chi)$

Zusätzlich haben wir mit GAP gezeigt, dass (P4) auch für alle Gruppen der Ordnung $5^6$ erfüllt ist. Für die Vermutung (P4) ist auch noch kein Gegenbeispiel bekannt.

# 1 Grundlagen

## 1.1 Endliche $p$-Gruppen

Wir werden in dieser Arbeit ausschließlich endliche Gruppen betrachten, und daher gelegentlich den Zusatz „endlich“ weglassen. Außerdem wollen wir mit $p$ immer eine Primzahl bezeichnen. Eine endliche Gruppe $G$ heißt dann *$p$-Gruppe*, falls ihre Ordnung $|G|$ eine Potenz von $p$ ist. In der Gruppentheorie spielen endliche $p$-Gruppen eine wichtige Rolle, und sie werden vielfach in der Literatur beschrieben. In diesem Abschnitt werden wir einige ihrer elementaren Eigenschaften angeben, die im Laufe der Arbeit noch benötigt werden. Alle diese Resultate findet man in der Standardliteratur, zum Beispiel in [5].

**Definition 1.1.** Für eine Gruppe $G$ nennt man

$$\mathrm{Z}(G) = \{x \in G : xy = yx \text{ für alle } y \in G\}$$

das *Zentrum* von $G$.

**Satz 1.1.** *Für eine nichttriviale endliche $p$-Gruppe $G$ gilt stets:* $\mathrm{Z}(G) \neq 1$.

Offenbar ist jede Untergruppe des Zentrums einer Gruppe $G$ stets ein Normalteiler in $G$. Umgekehrt liegt in einer endlichen $p$-Gruppe jeder minimale Normalteiler im Zentrum. Ist $G$ eine nichtabelsche Gruppe, so ist $G/\mathrm{Z}(G)$ niemals zyklisch.

**Definition 1.2.** Sei $G$ eine Gruppe. Setzt man $Z_0(G) := 1$ und $Z_n(G)/Z_{n-1}(G) := \mathrm{Z}(G/Z_{n-1}(G))$ für $n \in \mathbb{N}$, so erhält man die *aufsteigende Zentralreihe*

$$1 = Z_0(G) \leq \mathrm{Z}(G) = Z_1(G) \leq Z_2(G) \leq \ldots$$

von $G$. Eine Gruppe $G$ heißt *nilpotent*, falls ein $n \in \mathbb{N}_0$ mit $Z_n(G) = G$ existiert. Gegebenenfalls nennt man das kleinste $n$ mit dieser Eigenschaft *(Nilpotenz-)Klasse* von $G$.

Man überlegt sich leicht, dass Gruppen von Nilpotenzklasse kleiner gleich 1 abelsch sind. Mit vollständiger Induktion kann man dann folgenden Satz zeigen.

**Satz 1.2.** *Sei $G$ eine endliche $p$-Gruppe der Ordnung $p^n$. Dann ist $G$ nilpotent, und im Fall $n \geq 2$ ist die Nilpotenzklasse von $G$ stets kleiner als $n$.*

Eine endliche $p$-Gruppe hat *maximale Klasse*, falls sie Ordnung $p^n$ und Nilpotenzklasse $n-1$ für ein $n \in \mathbb{N}$ hat. Wir werden jetzt noch eine weitere Charakterisierung von nilpotenten Gruppen angeben.

**Definition 1.3.** Für eine Gruppe $G$ und zwei Elemente $x, y \in G$ bezeichnet man mit $[x, y] := xyx^{-1}y^{-1}$ den *Kommutator* von $x$ und $y$. Für zwei Teilmengen $X, Y \subseteq G$ bezeichnet man analog

$$[X, Y] := \langle [x, y] : x \in X,\ y \in Y \rangle$$

als den *Kommutator* von $X$ und $Y$. Für $X = Y = G$ erhält man die *Kommutatorgruppe* $G' := [G, G]$ von $G$.

Die Kommutatorgruppe einer Gruppe $G$ ist eine charakteristische Untergruppe, d. h., sie ist invariant gegenüber allen Automorphismen von $G$. Sie misst, wie stark die Elemente einer Gruppe kommutieren. Denn eine Gruppe ist genau dann abelsch, wenn ihre Kommutatorgruppe trivial ist. Folgende Eigenschaft der Kommutatorgruppe ist sehr nützlich.

**Lemma 1.1.** *Sei $G$ eine Gruppe und $H$ eine Untergruppe von $G$. Dann ist $H$ genau dann ein Normalteiler mit abelscher Faktorgruppe, wenn $G' \subseteq H$ gilt. Insbesondere ist $G'$ der „kleinste“ Normalteiler mit abelscher Faktorgruppe.*

**Definition 1.4.** Definiert man für eine Gruppe $G$ induktiv $G^1 := G$ und $G^{n+1} := [G, G^n]$ für $n \in \mathbb{N}$, so erhält man die *absteigende Zentralreihe*

$$G = G^1 \geq G' = G^2 \geq G^3 \geq \dots$$

von $G$.

**Satz 1.3.** *Eine Gruppe $G$ ist genau dann nilpotent der Klasse $c > 0$, wenn $G^c > G^{c+1} = 1$ gilt.*

Später werden wir noch die folgende Charakterisierung von Gruppen der Nilpotenzklasse kleiner gleich 2 benötigen.

**Lemma 1.2.** *Eine Gruppe $G$ hat genau dann Nilpotenzklasse kleiner gleich 2, falls $G' \subseteq \mathrm{Z}(G)$ gilt.*

*Beweis.* Sei $c$ die Nilpotenzklasse von $G$. Dann gilt

$$\begin{aligned} c \leq 2 &\Leftrightarrow Z_2(G) = G \Leftrightarrow G/\mathrm{Z}(G) = \mathrm{Z}(G/\mathrm{Z}(G)) \\ &\Leftrightarrow G/\mathrm{Z}(G) \text{ abelsch } \Leftrightarrow G' \subseteq \mathrm{Z}(G) \end{aligned}$$

nach Lemma 1.1. □

**Definition 1.5.** Für eine endliche Gruppe $G$ definiert man $\Phi(G)$ als den Durchschnitt aller maximalen Untergruppen von $G$. Man nennt $\Phi(G)$ die *Frattinigruppe* von $G$.

Speziell für $p$-Gruppen kann man eine Reihe von Aussagen über die Frattinigruppe treffen.

**Satz 1.4.** *Sei $G$ eine endliche $p$-Gruppe. Dann ist $G/\Phi(G)$* elementarabelsch*, d. h., $G/\Phi(G)$ ist abelsch, und es gilt $(x\Phi(G))^p = x^p\Phi(G) = 1$ für alle $x \in G$. Ist umgekehrt $N$ ein Normalteiler von $G$ mit elementarabelscher Faktorgruppe $G/N$, so gilt $\Phi(G) \subseteq N$. Daher ist $\Phi(G)$ der „kleinste“ Normalteiler von $G$ mit elementarabelscher Faktorgruppe.*

Als Folgerung erhält man $G' \subseteq \Phi(G)$ für jede endliche $p$-Gruppe $G$. Eine elementarabelsche Gruppe $G$ kann man auch als Vektorraum über dem Körper $\mathbb{Z}/p\mathbb{Z}$ auffassen, indem man $(k+p\mathbb{Z})x := x^k$ für $k+p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$ und $x \in G$ definiert. Burnsides Basissatz stellt dann eine Beziehung zwischen der minimalen Anzahl von Erzeugern von $G$ und der Dimension von $G/\Phi(G)$ her.

**Satz 1.5** (Burnsides Basissatz)**.** *Sei $G$ eine endliche $p$-Gruppe und $x_1, \ldots, x_n \in G$. Genau dann ist $G = \langle x_1, \ldots, x_n\rangle$, wenn $G/\Phi(G) = \mathrm{Span}_{\mathbb{Z}/p\mathbb{Z}}(x_1\Phi(G), \ldots, x_n\Phi(G))$ gilt. Ist also $|G/\Phi(G)| = p^d$, so besitzt $G$ ein Erzeugendensystem mit $d$ Elementen, aber keines mit weniger als $d$ Elementen.*

Gilt $|G/\Phi(G)| = p$ für eine endliche $p$-Gruppe $G$, so ist also $G$ zyklisch. Hat $G$ die Ordnung $p^n$ mit $n \geq 2$, so gilt mit $G' \subseteq \Phi(G)$ daher stets $|G : G'| \geq p^2$.

**Definition 1.6.** Für eine Gruppe $G$ bezeichnen wir mit $\mathrm{Aut}(G)$ die *Automorphismengruppe* von $G$.

Ist $G$ eine elementarabelsche $p$-Gruppe der Ordnung $p^d$, so entsprechen die Gruppenautomorphismen von $G$ gerade den Vektorraumautomorphismen von $G$. Auf diese Weise sieht man, dass die Automorphismengruppe von $G$ isomorph zur Gruppe $\mathrm{GL}(d, p)$ der invertierbaren $d \times d$-Matrizen über dem Körper $\mathbb{Z}/p\mathbb{Z}$ ist.

**Definition 1.7.** Eine Gruppe $G$ heißt *metazyklisch*, falls ein zyklischer Normalteiler $N$ von $G$ mit zyklischer Faktorgruppe $G/N$ existiert.

## 1.2 Konjugationsklassen

Sei $G$ eine beliebige Gruppe. Man nennt zwei Elemente $x, y \in G$ *konjugiert* in $G$, falls ein Element $z \in G$ mit $x = zyz^{-1}$ existiert. Die Menge aller zu $x \in G$ konjugierten Elemente nennt man *Konjugationsklasse* von $x$ in $G$. Man kann sich leicht überlegen, dass eine Gruppe die disjunkte Vereinigung ihrer Konjugationsklassen ist. Wir bezeichnen die Menge aller Konjugationsklassen von $G$ mit $\mathrm{Cl}(G)$ und ihre Mächtigkeit $|\mathrm{Cl}(G)|$ als *Klassenzahl* von $G$. Für $K \in \mathrm{Cl}(G)$ nennen wir die Anzahl $|K|$ von Elementen in $K$ die *Länge* von $K$. Außerdem wollen wir für $x \in G$ den *Zentralisator* von $x$ in $G$ mit $\mathrm{C}_G(x)$ bezeichnen, d. h. $\mathrm{C}_G(x) := \{y \in G : xy = yx\}$. Es gilt dann folgende Beziehung.

**Satz 1.6.** *Für eine Gruppe $G$ und ein Element $x \in G$ ist die Abbildung $y\,\mathrm{C}_G(x) \mapsto yxy^{-1}$ für $y \in G$ eine Bijektion zwischen der Menge der Linksnebenklassen $G/\,\mathrm{C}_G(x)$ und der Konjugationsklasse $K$ von $x$. Insbesondere ist die Länge $|K| = |G : \mathrm{C}_G(x)|$ von $K$ stets ein Teiler der Gruppenordnung.*

Für eine Gruppe $G$ erhält man damit die *Klassengleichung*

$$|G| = \sum_{x \in R} |G : \mathrm{C}_G(x)|,$$

wobei $R$ ein Repräsentantensytem für die Konjugationsklassen von $G$ ist. Das Zentrum einer Gruppe ist gerade die Vereinigung ihrer einelementigen Konjugationsklassen. Insbesondere ist jede Konjugationsklasse einer abelschen Gruppe einelementig. Analog zum Zentralisator wollen wir für eine Teilmenge $U$ einer Gruppe $G$ den *Normalisator* von $U$ in $G$ mit $\mathrm{N}_G(U) := \{x \in G : xUx^{-1} = U\}$ bezeichnen.

Für drei Konjugationsklassen $K$, $L$ und $M$ einer Gruppe $G$ und $z, z' \in M$ ist

$$|\{(x, y) \in K \times L : xy = z\}| = |\{(x', y') \in K \times L : x'y' = z'\}|,$$

denn für $a \in G$ mit $z' = aza^{-1}$ beschreibt die Abbildung $(x, y) \mapsto (axa^{-1}, aya^{-1})$ eine Bijektion zwischen der Menge der Paare $(x, y) \in K \times L$ mit $xy = z$ und der Menge der Paare $(x', y') \in K \times L$ mit $x'y' = z'$. Also ist die folgende Definition sinnvoll.

**Definition 1.8.** Für drei Konjugationsklassen $K$, $L$ und $M$ einer Gruppe $G$ und $z \in M$ definiert man

$$c_{KLM} := |\{(x, y) \in K \times L : xy = z\}|.$$

Die Zahl $c_{KLM}$ ist unabhängig von der Wahl des Repräsentanten $z \in M$. Man nennt sie *Klassenmultiplikationskonstante* von $K$, $L$ und $M$.

Für eine Gruppe $G$ und $K, L, M \in \mathrm{Cl}(G)$ ist $KL := \{xy : x \in K,\ y \in L\}$ offenbar wieder eine Vereinigung von Konjugationsklassen von $G$. Folglich ist $c_{KLM} \neq 0$ genau dann, wenn $M \subseteq KL$ gilt.

## 1.3 Darstellungen und Charaktere

Die Resultate in diesem Abschnitt findet man zum Beispiel in [6]. Sei $G$ eine Gruppe und $V$ ein endlich-dimensionaler komplexer Vektorraum. Einen Homomorphismus $\Delta$ von $G$ in die allgemeine lineare Gruppe $\mathrm{GL}(V)$ von $V$ nennt man *Darstellung* von $G$ auf $V$. Die Dimension von $V$ bezeichnet man als *Grad* von $\Delta$. Zum Beispiel ist die Abbildung $\Delta : G \to \mathbb{C}$, $g \mapsto 1$ eine Darstellung vom Grad 1. Man nennt sie *triviale Darstellung* von $G$. Eine Darstellung vom Grad $n$ kann man auch als Abbildung in die Gruppe der invertierbaren komplexen $n \times n$-Matrizen $\mathrm{GL}(n, \mathbb{C})$ betrachten, indem man eine Basis von $V$ wählt. Man nennt dann die Abbildung

$$\chi : G \to \mathbb{C},\ g \mapsto \mathrm{spur}(\Delta(g))$$

den *Charakter* von $\Delta$. Mit linearer Algebra zeigt man, dass $\chi$ unabhängig von der Wahl der Basis von $V$ ist. Außerdem ist jeder Charakter $\chi$ eine *Klassenfunktion*, d. h., es gilt $\chi(g) = \chi(h)$, falls $g, h \in G$ konjugiert sind. Die Menge $\mathrm{CF}(G)$ aller

komplexwertigen Klassenfunktionen einer Gruppe $G$ bildet einen komplexen Vektorraum, wenn man die Verknüpfungen komponentenweise definiert. Zusätzlich kann man durch

$$\mathrm{CF}(G) \times \mathrm{CF}(G) \to \mathbb{C},\ (\varphi, \psi) \mapsto (\varphi|\psi)_G := \frac{1}{|G|} \sum_{g \in G} \varphi(g)\psi(g^{-1})$$

eine symmetrische Bilinearform auf $\mathrm{CF}(G)$ definieren. Ist $\Delta$ eine Darstellung einer Gruppe $G$ und $\chi$ der Charakter von $\Delta$, so ist $\chi(1)$ offenbar genau der Grad von $\Delta$. Man spricht dann auch vom *Grad* des Charakters $\chi$.

Einen Untervektorraum $U$ von $V$ mit der Eigenschaft $(\Delta(g))(u) \in U$ für alle $g \in G$ und $u \in U$ nennt man $\Delta$-*invariant*. Sind 0 und $V$ die einzigen $\Delta$-invarianten Untervektorräume von $V \neq 0$, so bezeichnet man die Darstellung $\Delta$ als *irreduzibel*. Ein Charakter heißt *irreduzibel*, falls die entsprechende Darstellung irreduzibel ist. Offenbar ist jeder Charakter vom Grad 1 irreduzibel. Insbesondere ist der zur trivialen Darstellung gehörige *triviale Charakter* irreduzibel. Wir bezeichnen ihn mit $1_G$. Man kann zeigen, dass der Grad eines irreduziblen Charakters einer endlichen Gruppe $G$ stets ein Teiler von $|G|$ ist.

**Definition 1.9.** Die Menge aller irreduziblen Charaktere einer Gruppe $G$ bezeichnet man mit $\mathrm{Irr}(G)$.

**Satz 1.7.** *Die Elemente in* $\mathrm{Irr}(G)$ *bilden eine Orthonormalbasis von* $\mathrm{CF}(G)$ *bezüglich* $(\,.\,|\,.\,)_G$*, und ihre Anzahl* $|\mathrm{Irr}(G)| = \dim \mathrm{CF}(G)$ *stimmt mit der Klassenzahl von* $G$ *überein.*

Jeder Charakter einer Gruppe $G$ lässt sich also eindeutig als komplexe Linearkombination irreduzibler Charaktere schreiben. Man kann zeigen, dass die dabei auftretenden Koeffizienten nichtnegative ganze Zahlen sind.

**Definition 1.10.** Sei $G$ eine Gruppe, $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_n\}$ und $\chi$ ein beliebiger Charakter von $G$. Wir schreiben $\chi = a_1\chi_1 + \ldots + a_n\chi_n$ mit $a_1, \ldots, a_n \in \mathbb{N}_0$, und definieren

$$\mathrm{Irr}(\chi) := \{\chi_i : 1 \leq i \leq n,\ a_i \neq 0\}.$$

Man bezeichnet die Elemente in $\mathrm{Irr}(\chi)$ als *irreduzible Bestandteile* von $\chi$ und $a_i$ als *Vielfachheit* des irreduziblen Bestandteils $\chi_i$ von $\chi$.

Mit den Bezeichnungen aus Definition 1.10 gilt $a_i = (\chi|\chi_i)_G$ für $i = 1, \ldots, n$ nach Satz 1.7. Außerdem ist

$$|G| = \chi_1(1)^2 + \ldots + \chi_n(1)^2. \qquad (\star)$$

Oft hat man Operationen auf den Konjugationsklassen sowie auf den irreduziblen Charakteren einer Gruppe gegeben. Mit Brauers Permutationslemma kann man dann die Fixpunkte dieser Operationen in Beziehung setzen.

**Satz 1.8** (Brauers Permutationslemma)**.** *Seien $G$ und $H$ Gruppen, sodass $G$ auf* $\mathrm{Cl}(H)$ *sowie auf* $\mathrm{Irr}(H)$ *operiert. Außerdem sei vorausgesetzt, dass der Wert von $\chi$ auf ${}^gK$ mit dem Wert von ${}^g\chi$ auf $K$ für alle $g \in G$, $K \in \mathrm{Cl}(H)$ und $\chi \in \mathrm{Irr}(H)$ übereinstimmt. Dann gilt $|\{\chi \in \mathrm{Irr}(H) : {}^g\chi = \chi\}| = |\{K \in \mathrm{Cl}(G) : {}^gK = K\}|$ für jedes $g \in G$.*

Für einen Charakter $\chi$ einer Gruppe $G$ definiert man $\overline{\chi}$ durch $\overline{\chi}(g) := \overline{\chi(g)}$. In der Darstellungstheorie zeigt man, dass $\overline{\chi}$ wieder ein Charakter von $G$ ist, und dass $\overline{\chi}(g) = \chi(g^{-1})$ gilt. Man nennt $\overline{\chi}$ den *dualen Charakter* zu $\chi$. Außerdem ist die Menge der Charaktere einer Gruppe abgeschlossen bezüglich (komponentenweiser) Addition und Multiplikation.

**Definition 1.11.** Für einen Charakter $\chi$ einer Gruppe $G$ bezeichnen wir mit $\mathrm{Ker}(\chi)$ den Kern der entsprechenden Darstellung, d. h. $\mathrm{Ker}(\chi) := \{g \in G : \chi(g) = \chi(1)\}$. Man spricht dann auch vom *Kern* des Charakters $\chi$. Außerdem definieren wir $\mathrm{Z}(\chi) := \{g \in G : |\chi(g)| = \chi(1)\}$. Man nennt $\mathrm{Z}(\chi)$ das *Zentrum* von $\chi$.

Man kann zeigen, dass $\mathrm{Ker}(\chi)$ und $\mathrm{Z}(\chi)$ für einen Charakter $\chi$ einer Gruppe $G$ stets Normalteiler von $G$ sind. Ist $\Delta$ die zu $\chi$ gehörige Darstellung auf einem Vektorraum $V$, so gilt außerdem $\mathrm{Z}(\chi) = \{g \in G : \Delta(g) \in \mathbb{C}^\times \mathrm{id}_V\}$. Offenbar ist $\mathrm{Ker}(\chi) \subseteq \mathrm{Z}(\chi)$. Falls $\chi$ irreduzibel ist, hat man zusätzlich $\mathrm{Z}(\chi)/\mathrm{Ker}(\chi) = \mathrm{Z}(G/\mathrm{Ker}(\chi))$. Im Fall $\mathrm{Ker}(\chi) = 1$ bezeichnet man $\chi$ als *treu*.

Offenbar operiert eine endliche Gruppe $G$ auf sich selbst durch Linksmultiplikation. Sei $\alpha : G \to \mathrm{Sym}(|G|)$ der entsprechende Homomorphismus in die Symmetrische Gruppe vom Grad $|G|$. Realisiert man die Elemente in $\mathrm{Sym}(|G|)$ als Permutationsmatrizen in $\mathrm{GL}(|G|, \mathbb{C})$, so erhält man aus $\alpha$ eine Darstellung $\Delta : G \to \mathrm{GL}(|G|, \mathbb{C})$ vom Grad $|G|$. Man nennt $\Delta$ die *reguläre Darstellung* von $G$. Der entsprechende Charakter $\rho_G$ von $\Delta$ heißt *regulärer Charakter* von $G$. Man überlegt sich leicht, dass $\rho_G(1) = |G|$ und $\rho_G(g) = 0$ für $1 \neq g \in G$ gilt.

**Definition 1.12.** Sei $G$ eine Gruppe und $N$ ein Normalteiler von $G$. Ist $\Delta$ eine Darstellung von $G/N$ auf einem endlich-dimensionalen Vektorraum $V$, so ist auch $\Gamma : G \to \mathrm{GL}(V)$, $g \mapsto \Delta(gN)$ eine Darstellung von $G$ auf $V$. Man nennt $\Gamma$ die *Inflation* von $\Delta$. Analog spricht man von der *Inflation* eines Charakters.

Ist $\Delta$ in Definition 1.12 irreduzibel, so ist offenbar auch $\Gamma$ irreduzibel.

**Definition 1.13.** Für eine Gruppe $G$ definiert man

$$\mathbb{Z}G := \Big\{\sum_{g \in G} \alpha_g g : \alpha_g \in \mathbb{Z} \text{ für } g \in G\Big\}$$

als Menge aller ganzzahligen „formalen“ Linearkombinationen von Elementen aus $G$. Man bezeichnet $\mathbb{Z}G$ als *Gruppenring* von $G$.

Man überlegt sich leicht, dass $\mathbb{Z}G$ tatsächlich ein Ring wird, indem man

$$\sum_{g\in G}\alpha_g g + \sum_{h\in G}\beta_h h := \sum_{g\in G}(\alpha_g+\beta_g)g,$$
$$\sum_{g\in G}\alpha_g g \cdot \sum_{h\in G}\beta_h h := \sum_{g,h\in G}\alpha_g\beta_h gh = \sum_{g\in G}\Bigg(\sum_{\substack{h,k\in G,\\ hk=g}}\alpha_h\beta_k\Bigg)g$$

für $\sum_{g\in G}\alpha_g g, \sum_{h\in G}\beta_h h \in \mathbb{Z}G$ definiert. Wie üblich bezeichnen wir mit $\mathrm{Z}(\mathbb{Z}G)$ das Zentrum des Gruppenrings, und für eine Teilmenge $K \subseteq G$ setzen wir

$$K^+ := \sum_{x\in K} x \in \mathbb{Z}G.$$

Insbesondere erhält man für $K \in \mathrm{Cl}(G)$ die *Klassensumme* $K^+$ von $K$, welche stets in $\mathrm{Z}(\mathbb{Z}G)$ liegt. Wie jede abelsche Gruppe kann man auch $\mathrm{Z}(\mathbb{Z}G)$ als $\mathbb{Z}$-Modul auffassen. In diesem Sinne bilden dann die Klassensummen eine $\mathbb{Z}$-Basis von $\mathrm{Z}(\mathbb{Z}G)$. Insbesondere stimmt die Klassenzahl von $G$ mit der Dimension von $\mathrm{Z}(\mathbb{Z}G)$ überein.

Gelegentlich werden wir die Abbildung

$$\nu : \mathbb{Z}G \to \mathbb{Z},\ \sum_{g\in G}\alpha_g g \mapsto \sum_{g\in G}\alpha_g$$

benutzen. Man macht sich schnell klar, dass $\nu$ ein Homomorphismus von Ringen ist; man nennt ihn *Augmentationsabbildung* von $\mathbb{Z}G$.

# 2 Problemstellung für Konjugationsklassen

## 2.1 Formulierung der Probleme

Sei $G$ eine endliche $p$-Gruppe und $K$ eine Konjugationsklasse von $G$. Offenbar ist dann auch $K^{-1} := \{x^{-1} : x \in K\}$ eine Konjugationsklasse von $G$. Wir werden zunächst für Gruppen ungerader Ordnung das Verhältnis zwischen $K$ und $K^{-1}$ klären.

**Lemma 2.1.** *Sei $G$ eine Gruppe ungerader Ordnung und $K \in \mathrm{Cl}(G)$. Im Fall $K = K^{-1}$ gilt dann $K = \{1\}$. Folglich ist $\{1\}$ die einzige „selbstinverse" Konjugationsklasse von $G$.*

*Beweis.* Sei $x \in K$ und $K = K^{-1}$. Dann existiert ein $y \in G$ mit $x^{-1} = yxy^{-1}$. Also ist $x = yx^{-1}y^{-1} = y^2xy^{-2}$ und damit $y^2 \in \mathrm{C}_G(x)$. Da $y$ ungerade Ordnung hat, folgt $y \in \mathrm{C}_G(x)$ und $x = x^{-1}$. Also ist $x^2 = 1$. Da auch $x$ ungerade Ordnung hat, folgt schließlich $x = 1$ und damit die Behauptung. □

Für eine Konjugationsklasse $K$ einer Gruppe $G$ ist $KK^{-1}$ wieder eine Vereinigung von Konjugationsklassen von $G$. Wir wollen mit $\eta(K)$ die Anzahl der Konjugationsklassen in $KK^{-1}$ bezeichnen, d. h.

$$\eta(K) := |\{L \in \mathrm{Cl}(G) : L \subseteq KK^{-1}\}|.$$

Adan-Bante hat in [2] bewiesen, dass für eine endliche $p$-Gruppe $G$ und eine Konjugationsklasse $K$ von $G$ der Länge $p^n$ stets $\eta(K) \geq n(p-1)+1$ gilt. Sie hat auch gezeigt, dass diese Ungleichung optimal ist. Wir werden in dieser Arbeit eine ähnliche Aussage untersuchen:

**Problem 1.** *Sei $G$ eine endliche $p$-Gruppe und $K$ eine Konjugationsklasse von $G$. Gilt dann stets*

$$\eta(K) \equiv 1 \pmod{p-1}? \tag{P1}$$

Da die Länge einer Konjugationsklasse in einer endlichen $p$-Gruppe stets eine Potenz von $p$ ist, erhält man mit $p^n \equiv 1 \pmod{p-1}$ für $n \in \mathbb{N}$ die zu (P1) äquivalente Aussage

$$|KK^{-1}| \equiv 1 \pmod{p-1}. \tag{P2}$$

Bevor wir beginnen, einige Spezialfälle zu diskutieren, werden wir mit Hilfe der Klassenmultiplikationskonstanten eine stärkere Aussage angeben.

Multipliziert man zwei Klassensummen $K^+$ und $L^+$ einer endlichen $p$-Gruppe $G$, so erhält man

$$K^+L^+ = \sum_{M \in \mathrm{Cl}(G)} c_{KLM} M^+ \text{ in } \mathbb{Z}G. \qquad (\star\star)$$

Wendet man nun die Augmentationsabbildung auf beiden Seiten an, ergibt sich

$$1 \equiv |K||L| = \sum_{M \in \mathrm{Cl}(G)} c_{KLM}|M| \equiv \sum_{M \in \mathrm{Cl}(G)} c_{KLM} \pmod{p-1}.$$

Erfüllt die Konjugationsklasse $K$ die Eigenschaft

$$\text{Für alle } L \in \mathrm{Cl}(G) \text{ gilt } c_{KK^{-1}L} = 0 \text{ oder } c_{KK^{-1}L} \equiv 1 \pmod{p-1}, \qquad \text{(P3)}$$

so folgt daher

$$\eta(K) = \sum_{\substack{L \in \mathrm{Cl}(G),\\ L \subseteq KK^{-1}}} 1 = \sum_{\substack{L \in \mathrm{Cl}(G),\\ c_{KK^{-1}L} \neq 0}} 1 \equiv \sum_{L \in \mathrm{Cl}(G)} c_{KK^{-1}L} \equiv 1 \pmod{p-1}.$$

Also folgen die Eigenschaften (P1) und (P2) aus (P3). Wir werden (P3) in vielen Fällen beweisen, indem wir zeigen, dass $c_{KK^{-1}L}$ für $K, L \in \mathrm{Cl}(G)$ entweder 0 oder sogar eine Potenz von $p$ ist.

## 2.2 Resultate

In diesem Abschnitt werden wir Problem 1 (bzw. dessen Modifikationen mittels (P2) und (P3)) für einige Spezialfälle lösen. Hauptsächlich werden wir dabei die Ordnung der zu betrachtenden Gruppen beschränken.

Wir beginnen mit dem Spezialfall $p = 2$. Offenbar sind in diesem Fall (P1), (P2) und (P3) für alle endlichen $p$-Gruppen $G$ und alle Konjugationsklassen $K$ von $G$ erfüllt. Also können wir ab jetzt voraussetzen, dass $p$ ungerade ist. Insbesondere kann man Lemma 2.1 anwenden.

**Satz 2.1.** *Sei $G$ eine endliche $p$-Gruppe für eine ungerade Primzahl $p$ und $K$ eine Konjugationsklasse von $G$. Dann sind $\eta(K)$ und $|KK^{-1}|$ ungerade. Insbesondere sind* (P1) *und* (P2) *im Fall $p = 3$ stets erfüllt.*

*Beweis.* Für $x \in KK^{-1}$ existieren $a \in K$ und $g \in G$ mit $x = aga^{-1}g^{-1}$. Also ist $x^{-1} = gag^{-1}a^{-1} \in KK^{-1}$. Für jede Konjugationsklasse $L \subseteq KK^{-1}$ ist also auch $L^{-1} \subseteq KK^{-1}$. Da offenbar auch $\{1\} \subseteq KK^{-1}$ gilt, folgt aus Lemma 2.1, dass $\eta(K)$ ungerade ist. Offensichtlich ist dann auch $|KK^{-1}|$ ungerade. □

**Lemma 2.2.** *Sei $G$ eine endliche $p$-Gruppe und $K$ eine Konjugationsklasse von $G$. Dann ist $KK^{-1} \cap \mathrm{Z}(G) \leq G$ und $(KK^{-1} \cap \mathrm{Z}(G))K = K$.*

*Beweis.* Wegen $1 \in KK^{-1} \cap \mathrm{Z}(G)$ genügt es, für $KK^{-1} \cap \mathrm{Z}(G) \leq G$ zu zeigen, dass $KK^{-1} \cap \mathrm{Z}(G)$ multiplikativ abgeschlossen ist. Sei also $x, y \in KK^{-1} \cap \mathrm{Z}(G)$. Dann existieren $g, h \in G$ und $a \in K$ mit $x = gag^{-1}a^{-1}$ und $y = aha^{-1}h^{-1}$. Also ist $xy = gag^{-1}ha^{-1}h^{-1} \in KK^{-1} \cap \mathrm{Z}(G)$.

Ist nun $x \in KK^{-1} \cap \mathrm{Z}(G)$ und $a \in K$, so lässt sich $x$ in der Form $x = gag^{-1}a^{-1}$ mit $g \in G$ schreiben. Dann ist $xa = gag^{-1} \in K$. Dies zeigt $(KK^{-1} \cap \mathrm{Z}(G))K \subseteq K$. Umgekehrt ist sicher $K = 1K \subseteq (KK^{-1} \cap \mathrm{Z}(G))K$, und die Behauptung ist gezeigt. □

**Lemma 2.3.** *Sei $G$ eine endliche $p$-Gruppe und $K$ eine Konjugationsklasse von $G$. Dann gilt stets $|K| \leq |KK^{-1}|$. Im Fall $|K| = |KK^{-1}|$ ist $c_{KK^{-1}L} \in \{0, |K|\}$ für $L \in \mathrm{Cl}(G)$. Insbesondere sind dann* (P3)*,* (P2) *und* (P1) *erfüllt.*

*Beweis.* Sei $x \in K$. Da die Elemente $xy \in KK^{-1}$ mit $y \in K^{-1}$ paarweise verschieden sind, folgt $|K| \leq |KK^{-1}|$. Sei nun $|K| = |KK^{-1}|$. Wegen

$$|KK^{-1}| = |K| = |\{gxg^{-1} : g \in G\}| = |\{gxg^{-1}x^{-1} : g \in G\}|$$

ist dann $KK^{-1} = \{xgx^{-1}g^{-1} : g \in G\} = \{gxg^{-1}x^{-1} : g \in G\}$. Wie in Lemma 2.2 zeigt man, dass $N := KK^{-1}$ eine Untergruppe von $G$ ist. Da $N$ eine Vereinigung von Konjugationsklassen von $G$ ist, gilt sogar $N \trianglelefteq G$. Außerdem ist $K = Nx$, und man erhält

$$K^+(K^{-1})^+ = (Nx)^+(x^{-1}N)^+ = (N^+)^2 = |N|N^+ = |K|N^+.$$

Mit Gleichung $(\star\star)$ folgt dann die Behauptung. □

Als Nächstes werden wir die Längen der Konjugationsklassen beschränken. Das folgende Lemma entspricht Lemma 4.1 in [2].

**Lemma 2.4.** *Sei $G$ eine endliche $p$-Gruppe und $K$ eine Konjugationsklasse der Länge $p$ von $G$. Ist dann $a \in K$, so gilt einer der beiden Fälle:*

*(i) Es existiert eine Untergruppe $Z$ von $\mathrm{Z}(G)$ mit $K = aZ$. In diesem Fall ist $KK^{-1} = Z$ und damit $\eta(K) = |KK^{-1}| = p$.*

*(ii) Die Menge $KK^{-1}$ ist die Vereinigung von $p-1$ Konjugationsklassen der Länge $p$ und $\{1\}$. Insbesondere gilt auch in diesem Fall $\eta(K) = p$.*

*Beweis.* Nach Lemma 2.2 ist $Z := KK^{-1} \cap \mathrm{Z}(G) \leq \mathrm{Z}(G)$ und $aZ = Za \subseteq ZK = K$. Im Fall $|Z| = p = |K|$ gilt also (i).

Sei nun $Z = 1$. Offenbar gilt $|KK^{-1}| \leq |K \times K^{-1}| = p^2$, und wegen $1 = xx^{-1} \in KK^{-1}$ für alle $x \in K$ kann man die Ungleichung zu

$$|KK^{-1}| \leq p^2 - p + 1 = p(p-1) + 1$$

verbessern. Also besteht $KK^{-1}$ nur aus $\{1\}$ und Konjugationsklassen der Länge $p$. Andererseits gilt $\eta(K) \geq p$ nach Theorem A in [2], und (ii) ist erfüllt. □

Lemma 2.4 zeigt bereits, dass (P1) und (P2) im Fall $|K| = p$ für eine Konjugationsklasse $K$ einer endlichen $p$-Gruppe $G$ erfüllt sind. Mit etwas mehr Aufwand kann man zeigen, dass auch (P3) erfüllt ist.

**Satz 2.2.** *Sei $G$ eine endliche $p$-Gruppe der Ordnung $p^n$ mit $n \geq 2$ und $K, L \in \mathrm{Cl}(G)$ mit $|K| \in \{1, p, p^{n-2}\}$. Dann ist $c_{KK^{-1}L} \in \{0, 1, |K|\}$. Insbesondere sind* (P3)*,* (P2) *und* (P1) *erfüllt.*

*Beweis.* Der Fall $|K| = 1$ ist trivial. Betrachten wir also zunächst den Fall $|K| = p$. Gilt (i) in Lemma 2.4, so existiert eine Untergruppe $Z \leq \mathrm{Z}(G)$ mit $K = aZ$. Dann ist $KK^{-1} = Zaa^{-1}Z = Z$ und $|K| = |KK^{-1}|$. Mit Lemma 2.3 folgt in diesem Fall die Behauptung.

Nehmen wir nun an, dass (ii) in Lemma 2.4 gilt, d. h., $KK^{-1}$ ist die Vereinigung von $\{1\}$ und Konjugationsklassen $K_1, \ldots, K_{p-1}$ der Länge $p$. Dann erhält man

$$K^+(K^{-1})^+ = p \cdot 1 + K_1^+ + \ldots + K_{p-1}^+,$$

sodass mit Gleichung $(\star\star)$ in diesem Fall die Behauptung folgt.

Schließlich sei $|K| = p^{n-2}$. Für $x \in K$ ist dann

$$p^{n-2} = |K| = |\{gxg^{-1} : g \in G\}| = |\{gxg^{-1}x^{-1} : g \in G\}| \leq |G'|,$$

und wegen $|G : G'| \geq p^2$ gilt $|K| = |KK^{-1}| = |G'|$. Die Behauptung folgt nun mit Lemma 2.3. □

Für jede Konjugationsklasse $K$ einer endlichen $p$-Gruppe $G$ gilt offenbar $KK^{-1} = \{xgx^{-1}g^{-1} = [x, g] : x \in K, g \in G\} \subseteq G'$. Wegen $|K| \leq |KK^{-1}|$ kann daher die Länge einer Konjugationsklasse im Fall $|G| = p^n$ mit $n \geq 2$ nicht größer als $p^{n-2}$ sein. Als Folgerung von Satz 2.2 erhält man dann, dass (P3), (P2) und (P1) für alle Konjugationsklassen $K$ von $G$ erfüllt sind, falls $|G| \leq p^4$ gilt. Satz III.14.23 in [5] besagt, dass die Gruppen der Ordnung $p^n$ mit $n \geq 2$ und einer Konjugationsklasse der Länge $p^{n-2}$ gerade die $p$-Gruppen von maximaler Klasse sind.

Wir werden nun die Nilpotenzklasse der zu betrachtenden Gruppen einschränken.

**Satz 2.3.** *Sei $G$ eine endliche $p$-Gruppe mit Nilpotenzklasse kleiner gleich 2 und $K, L \in \mathrm{Cl}(G)$. Dann gilt $|K| = |KK^{-1}|$ und $c_{KK^{-1}L} \in \{0, |K|\}$. Insbesondere sind* (P3)*,* (P2) *und* (P1) *erfüllt.*

*Beweis.* Aus Lemma 1.2 folgt $KK^{-1} \subseteq G' \subseteq \mathrm{Z}(G)$, und nach Lemma 2.2 ist $|KK^{-1}| = |KK^{-1} \cap \mathrm{Z}(G)| \leq |(KK^{-1} \cap \mathrm{Z}(G))K| = |K|$. Daher ist $|K| = |KK^{-1}|$, und mit Lemma 2.3 folgt die Behauptung. □

Das folgende, etwas technische Lemma verallgemeinert Satz 2.3.

**Lemma 2.5.** *Sei $G$ eine endliche $p$-Gruppe und $x \in K \in \mathrm{Cl}(G)$. Existiert eine Untergruppe $H$ von $G$ mit $G = H\,\mathrm{C}_G(x)$ und $KK^{-1} \subseteq \mathrm{C}_G(H)$, so ist $|K| = |KK^{-1}|$ und $c_{KK^{-1}L} \in \{0, |K|\}$ für $L \in \mathrm{Cl}(G)$. Insbesondere sind* (P3), (P2) *und* (P1) *erfüllt.*

*Beweis.* Unter den angegebenen Voraussetzungen gilt offenbar $K = \{hxh^{-1} : h \in H\}$. Wegen $KK^{-1} \subseteq \mathrm{C}_G(H)$ ist auch $H \subseteq \mathrm{C}_G(KK^{-1})$, und man kann jedes Element in $KK^{-1}$ in der Form $xgx^{-1}g^{-1}$ mit $g \in G$ schreiben. Also ist $|K| = |KK^{-1}|$, und die Behauptung folgt aus Lemma 2.3. □

**Lemma 2.6.** *Sei $G$ eine endliche $p$-Gruppe und $x \in K \in \mathrm{Cl}(G)$. Existiert dann ein abelscher Normalteiler $A$ von $G$ mit $G = A\,\mathrm{C}_G(x)$ und $G' \subseteq A$, so ist $|K| = |KK^{-1}|$ und $c_{KK^{-1}L} \in \{0, |K|\}$ für $L \in \mathrm{Cl}(G)$. Insbesondere sind* (P3), (P2) *und* (P1) *erfüllt.*

*Beweis.* Wegen $KK^{-1} \subseteq G' \subseteq A \subseteq C_G(A)$ folgt die Behauptung aus Lemma 2.5, indem man $H := A$ setzt. □

Damit kann man einen weiteren Spezialfall behandeln.

**Satz 2.4.** *Sei $G$ eine endliche $p$-Gruppe, $A$ ein abelscher Normalteiler von $G$ mit Index $p$ und $K, L \in \mathrm{Cl}(G)$. Dann ist $|K| \leq p$ oder $|K| = |KK^{-1}|$, und $c_{KK^{-1}L}$ ist entweder 0 oder eine Potenz von $p$. Insbesondere sind* (P3), (P2) *und* (P1) *erfüllt.*

*Beweis.* Sei $x \in K$. Im Fall $x \in A$ ist dann $A \subseteq \mathrm{C}_G(x)$ und damit $|K| \leq p$. Also folgt in diesem Fall die Behauptung aus Satz 2.2, und wir können $x \notin A$ annehmen. Dann sind aber die Voraussetzungen von Lemma 2.6 erfüllt. □

**Lemma 2.7.** *Sei $G$ eine endliche $p$-Gruppe und $K$ eine Konjugationsklasse von $G$. Existiert ein Normalteiler $N$ von $G$ mit $K \subseteq N$ und $|N|/|K| = p$, so ist $KK^{-1} = [G, N]$ und $|K| = |KK^{-1}|$. Insbesondere kann man Lemma 2.3 anwenden.*

*Beweis.* Sei $x \in K$. Bekanntlich ist $[G, N] \trianglelefteq G$ und $[G, N] < N$. Wegen

$$KK^{-1} = \{gxg^{-1}hx^{-1}h^{-1} : g, h \in G\} = \{g[x, g^{-1}h]g^{-1} : g, h \in G\} \subseteq [G, N]$$

und $|N|/|K| = p$ folgt dann $KK^{-1} = [G, N]$ und $|K| = |KK^{-1}|$. □

Wir stellen nun zwei Lemmata vor, die es ermöglichen, bei der Untersuchung von (P2) bzw. (P3) zu Faktorgruppen überzugehen.

**Lemma 2.8.** *Sei $G$ eine endliche $p$-Gruppe, $N$ ein Normalteiler von $G$ und $K, L \in \mathrm{Cl}(G)$. Offenbar sind dann $\overline{K} := KN/N$ und $\overline{L} := LN/N$ Konjugationsklassen von $\overline{G} := G/N$. Ist $KLN = KL$, so gilt $|KL| = |\overline{KL}||N| \equiv |\overline{KL}| \pmod{p-1}$.*

*Beweis.* Sei $KL$ die disjunkte Vereinigung der Linksnebenklassen $a_1N, \ldots, a_rN$ mit $a_1, \ldots, a_r \in G$ und $r \in \mathbb{N}$. Dann ist

$$|KL| = r|N| = |\overline{KL}||N| \equiv |\overline{KL}| \pmod{p-1}.$$ □

Nehmen wir nun an, dass $L = K^{-1}$ in der Situation von Lemma 2.8 gilt. Nach Lemma 2.2 ist $KK^{-1} \cap \mathrm{Z}(G) \trianglelefteq G$ und $(KK^{-1} \cap \mathrm{Z}(G))KK^{-1} = KK^{-1}$. Mit $N := KK^{-1} \cap \mathrm{Z}(G)$ sind also die Voraussetzungen von Lemma 2.8 erfüllt. Im Fall $N = KK^{-1} \cap \mathrm{Z}(G) \neq 1$ können wir daher die Gültigkeit von (P2) für $K$ aus der Gültigkeit von (P2) für $\overline{K}$ in der kleineren Gruppe $G/N$ ableiten. Existiert umgekehrt ein nichttrivialer Normalteiler $N$ von $G$ mit $KK^{-1}N = KK^{-1}$, so ist $1 \neq N \cap \mathrm{Z}(G) = 1N \cap \mathrm{Z}(G) \subseteq KK^{-1}N \cap \mathrm{Z}(G) = KK^{-1} \cap \mathrm{Z}(G)$. Daher kann man in der Regel $N = KK^{-1} \cap \mathrm{Z}(G)$ annehmen.

**Lemma 2.9.** *Sei $G$ eine endliche $p$-Gruppe, $N$ ein Normalteiler von $G$ und $K$, $L$ und $M$ Konjugationsklassen von $G$. Wir bezeichnen mit $\overline{K}$, $\overline{L}$ und $\overline{M}$ wieder die Bilder von $K$, $L$ und $M$ in $\overline{G} := G/N$. Ist nun $MN = M$, so unterscheiden sich $c_{KLM}$ und $c_{\overline{KLM}}$ nur durch einen Faktor, welcher eine Potenz von $p$ ist. Insbesondere gilt*

*(i)* $c_{KLM} = 0 \;\Leftrightarrow\; c_{\overline{KLM}} = 0$,

*(ii)* $c_{KLM} \equiv 1 \pmod{p-1} \;\Leftrightarrow\; c_{\overline{KLM}} \equiv 1 \pmod{p-1}$.

*Beweis.* Der natürliche Epimorphismus $G \to \overline{G}$, $g \mapsto gN$ induziert einen Ringepimorphismus $f : \mathbb{Z}G \to \mathbb{Z}\overline{G}$. Wendet man $f$ auf die Gleichung $(\star\star)$ an, so erhält man

$$\frac{|K||L|}{|\overline{K}||\overline{L}|}\overline{K}^{+}\overline{L}^{+} = \sum_{C \in \mathrm{Cl}(G)} c_{KLC}\frac{|C|}{|\overline{C}|}\overline{C}^{+}.$$

Die Voraussetzung $MN = M$ impliziert, dass $M$ die einzige Konjugationsklasse von $G$ mit $f(M) = \overline{M}$ ist. Also ist

$$|K||L||\overline{M}|c_{\overline{KLM}} = |\overline{K}||\overline{L}||M|c_{KLM},$$

und die Behauptung folgt. □

Analog zu Lemma 2.8 kann man Lemma 2.9 mit $L = K^{-1}$ und $N = MM^{-1} \cap \mathrm{Z}(G)$ anwenden. Sind zum Beispiel die Voraussetzungen von Lemma 2.7 für $M$ mit $|M| > 1$ erfüllt, so ist $MM^{-1} \cap \mathrm{Z}(G) \neq 1$, und man kann die Gültigkeit von (P3) für $K$ und $M$ aus der Gültigkeit von (P3) für $\overline{K}$ und $\overline{M}$ in der kleineren Gruppe $G/N$ ableiten. Wie in Lemma 2.8 kann man auch hier in der Regel $N = MM^{-1} \cap \mathrm{Z}(G)$ annehmen.

Als Nächstes wollen wir zeigen, dass (P3) für alle Gruppen der Ordnung $p^5$ gilt. Dazu tragen wir einige elementare Eigenschaften der Klassenmultiplikationskonstanten zusammen.

**Lemma 2.10.** *Sei $G$ eine endliche $p$-Gruppe und $x \in K \in \mathrm{Cl}(G)$. Außerdem sei $L \in \mathrm{Cl}(G)$ mit $L \subseteq KK^{-1}$ und $t \in L \cap xK^{-1}$. Dann gelten folgende Aussagen:*

*(i)* $c_{KK^{-1}L} \leq |K|$,

*(ii)* $c_{KK^{-1}L} = |K| \;\Leftrightarrow\; L \subseteq xK^{-1}$,

*(iii)* $L \subseteq \mathrm{Z}(G) \;\Rightarrow\; c_{KK^{-1}L} = |K|$,

*(iv)* $c_{KK^{-1}L} \geq |\,\mathrm{C}_G(t) : \mathrm{C}_G(t) \cap \mathrm{C}_G(x)| \geq |K|/|L|$,

*(v)* $|KK^{-1} \cap \mathrm{Z}(G)| \leq \eta(K) \leq |K|$,

*(vi)* $\eta(K) = |K| \;\Rightarrow\; c_{KK^{-1}L} = |K|/|L|$,

*(vii)* $|\,\mathrm{C}_G(x) : \mathrm{C}_G(x) \cap \mathrm{C}_G(t)| \leq |L \cap xK^{-1}| \leq |L|$,

*(viii)* $\mathrm{C}_G(x) \subseteq \mathrm{C}_G(t) \trianglelefteq G \;\Rightarrow\; c_{KK^{-1}L} = |L \cap xK^{-1}||K|/|L|$.

*Beweis.*

(i) Für jedes $a \in K$ existiert höchstens ein $b \in K^{-1}$ mit $ab = t$. Also folgt (i).

(ii) Sei zunächst $c_{KK^{-1}L} = |K|$. Dann existiert für jedes $g \in G$ ein $h \in G$ mit $t = g^{-1}xghx^{-1}h^{-1}$. Also ist $gtg^{-1} = xghx^{-1}h^{-1}g^{-1} \in L \cap xK^{-1}$, und es folgt $L \subseteq xK^{-1}$. Ist umgekehrt $L \subseteq xK^{-1}$, so existiert für jedes $g \in G$ ein $h \in G$ mit $g^{-1}tg = xhx^{-1}h^{-1}$. Also ist $t = gxg^{-1}ghx^{-1}h^{-1}g^{-1}$, und $c_{KK^{-1}L} = |K|$ folgt.

(iii) Jedes Element in $KK^{-1} \cap \mathrm{Z}(G)$ lässt sich in der Form $xgx^{-1}g^{-1}$ mit $g \in G$ schreiben. Also folgt (iii) aus (ii).

(iv) Wegen $t \in L \cap xK^{-1}$ existiert ein $g \in G$ mit $t = xgx^{-1}g^{-1}$. Für jedes $c \in \mathrm{C}_G(t)$ ist dann $t = ctc^{-1} = cxc^{-1}cgx^{-1}g^{-1}c^{-1}$. Damit erhält man $|\,\mathrm{C}_G(t) : \mathrm{C}_G(t) \cap \mathrm{C}_G(x)|$ Darstellungen von $t$ der Form $t = ab$ mit $a \in K$ und $b \in K^{-1}$. Also gilt $c_{KK^{-1}L} \geq |\,\mathrm{C}_G(t) : \mathrm{C}_G(t) \cap \mathrm{C}_G(x)| \geq |\,\mathrm{C}_G(t)|/|\,\mathrm{C}_G(x)| = |K|/|L|$, und (iv) ist gezeigt.

(v) Die Ungleichung $|KK^{-1} \cap \mathrm{Z}(G)| \leq \eta(K)$ ist trivial. Offenbar enthält jede Konjugationsklasse in $KK^{-1}$ ein Element der Form $xgx^{-1}g^{-1}$ mit $g \in G$. Damit folgt $\eta(K) \leq |\{xgx^{-1}g^{-1} : g \in G\}| = |K|$ und (v).

(vi) Wir definieren

$$a_i := |\{M \in \mathrm{Cl}(G) : M \subseteq KK^{-1},\ |M| = p^i\}|$$

für $i \in \mathbb{N}_0$. Aus der Voraussetzung $\eta(K) = |K|$ folgt dann $\sum_{i=0}^{\infty} a_i = |K|$. Die Augmentationsabbildung liefert $\nu(K^+(K^{-1})^+) = |K||K^{-1}| = |K|^2$. Andererseits gilt aber

$$\nu(K^+(K^{-1})^+) = \sum_{i=0}^{\infty} \sum_{\substack{M \in \mathrm{Cl}(G),\\ M \subseteq KK^{-1},\\ |M| = p^i}} c_{KK^{-1}M}|M| \geq \sum_{i=0}^{\infty} a_i \frac{|K|}{|M|}|M| = |K|^2$$

nach Gleichung $(\star\star)$ und (iv). Folglich gilt $c_{KK^{-1}L} = |K|/|L|$, und (vi) ist gezeigt.

(vii) Die Ungleichung $|L \cap xK^{-1}| \leq |L|$ ist trivial. Wegen $t \in L \cap xK^{-1}$ existiert ein $g \in G$ mit $t = xgx^{-1}g^{-1}$. Für jedes $c \in \mathrm{C}_G(x)$ ist dann $ctc^{-1} = xcgx^{-1}g^{-1}c^{-1}$. Auf diese Weise erhält man also $|\,\mathrm{C}_G(x) : \mathrm{C}_G(x) \cap \mathrm{C}_G(t)|$ Konjugierte von $t$ der Form $xhx^{-1}h^{-1}$ mit $h \in G$. Also ist $|L \cap xK^{-1}| \geq |\,\mathrm{C}_G(x) : \mathrm{C}_G(x) \cap \mathrm{C}_G(t)|$, und (vii) ist gezeigt.

(viii) Sei $n := |L \cap xK^{-1}|$. Wir wählen $a_1, \ldots, a_n \in G$ mit $L \cap xK^{-1} = \{a_i t a_i^{-1} : i \in \{1, \ldots, n\}\}$. Sei nun $t = gxg^{-1}hx^{-1}h^{-1}$ mit $g, h \in G$. Dann ist $g^{-1}tg \in L \cap xK^{-1}$ und damit $g^{-1} \in \bigcup_{i=1}^{n} a_i \operatorname{C}_G(t)$. Da $\operatorname{C}_G(t)$ normal in $G$ ist, gilt auch $g \in \bigcup_{i=1}^{n} a_i^{-1} \operatorname{C}_G(t)$.

Wir zeigen nun $|\{gxg^{-1} : g \in \bigcup_{i=1}^{n} a_i^{-1} \operatorname{C}_G(t)\}| = n|\operatorname{C}_G(t) : \operatorname{C}_G(x)| = n|K|/|L|$. Dann folgt $c_{KK^{-1}L} \leq n|K|/|L|$. Sei dafür $\tilde{g} = a_i^{-1}c$ und $\tilde{h} = a_j^{-1}d$ mit $i, j \in \{1, \ldots, n\}$, $c, d \in \operatorname{C}_G(t)$ und $\tilde{g}x\tilde{g}^{-1} = \tilde{h}x\tilde{h}^{-1}$. Aus $\tilde{g}\operatorname{C}_G(x) = \tilde{h}\operatorname{C}_G(x)$ und $\operatorname{C}_G(x) \subseteq \operatorname{C}_G(t)$ folgt dann $a_i^{-1}\operatorname{C}_G(t) = \tilde{g}\operatorname{C}_G(t) = \tilde{h}\operatorname{C}_G(t) = a_j^{-1}\operatorname{C}_G(t)$. Wegen $\operatorname{C}_G(t) \trianglelefteq G$ ist dann $i = j$ und $d \equiv c \pmod{\operatorname{C}_G(x)}$.

Um auch $c_{KK^{-1}L} \geq n|K|/|L|$ zu zeigen, konstruieren wir nun zu jedem $g \in \bigcup_{i=1}^{n} a_i^{-1}\operatorname{C}_G(t)$ ein $h \in G$ mit $t = gxg^{-1}hx^{-1}h^{-1}$. Sei also $g \in \bigcup_{i=1}^{n} a_i^{-1}\operatorname{C}_G(t) = \bigcup_{i=1}^{n} \operatorname{C}_G(t)a_i^{-1}$ beliebig vorgegeben. Dann existieren $i \in \{1, \ldots, n\}$ und $c \in \operatorname{C}_G(t)$ mit $g = ca_i^{-1}$. Wir wählen ein $k \in G$ mit $a_i t a_i^{-1} = xkx^{-1}k^{-1}$, und setzen $h := ca_i^{-1}k$. Dann ist

$$\begin{aligned} gxg^{-1}hx^{-1}h^{-1} &= ca_i^{-1}xa_ic^{-1}ca_i^{-1}kx^{-1}k^{-1}a_ic^{-1} \\ &= ca_i^{-1}(xkx^{-1}k^{-1})a_ic^{-1} = ctc^{-1} = t. \end{aligned}$$

Also ist (viii) bewiesen. □

In der Situation von Lemma 2.10 gilt offenbar stets $L \cap xK^{-1} \neq \varnothing$. Also existiert das Element $t$ immer. Im Fall $\eta(K) = |K|$ folgt aus (vi), dass $c_{KK^{-1}L}$ für alle $L \in \operatorname{Cl}(G)$ stets 0 oder eine Potenz von $p$ ist. Insbesondere sind dann (P3), (P2) und (P1) erfüllt. Die Zahl $|L \cap xK^{-1}|$ gibt an, wie viele Konjugierte von $t$ sich in der Form $xhx^{-1}h^{-1}$ mit $h \in G$ schreiben lassen. Wir werden oft zeigen, dass diese Zahl eine Potenz von $p$ ist, und dann mit (viii) argumentieren, dass auch $c_{KK^{-1}L}$ eine Potenz von $p$ ist. Da die Klassenmultiplikationskonstante nicht von der Wahl des Repräsentanten $t \in L$ abhängt, werden wir häufig $t \in L \cap xK^{-1}$ voraussetzen.

**Satz 2.5.** *Sei $G$ eine endliche $p$-Gruppe der Ordnung $p^n$ mit $n \leq 5$ und $K, L \in \operatorname{Cl}(G)$. Dann ist $c_{KK^{-1}L}$ entweder 0 oder eine Potenz von $p$. Insbesondere sind* (P3)*,* (P2) *und* (P1) *erfüllt.*

*Beweis.* Nach Satz 2.2 und Lemma 2.3 können wir $|G| = p^5$, $|K| = p^2$ und $|K| < |KK^{-1}|$ annehmen. Insbesondere ist dann $|G'| = p^3$ und $\Phi(G) = G'$. Sei $x \in K$. Nach Lemma 2.7 ist $x \notin G'$. Da $G/G' = G/\Phi(G)$ elementarabelsch ist, hat $M := G'\langle x\rangle$ die Ordnung $p^4$. Wir berechnen nun die Klassenmultiplikationskonstanten. Für jede Konjugationsklasse $L \nsubseteq KK^{-1}$ gilt offensichtlich $c_{KK^{-1}L} = 0$. Ist $L \subseteq KK^{-1} \cap \operatorname{Z}(G)$, so gilt $c_{KK^{-1}L} = |K|$ nach Lemma 2.10(iii). Sei nun $L \subseteq KK^{-1} \subseteq G'$ eine Konjugationsklasse der Länge $p^2$. Nach Lemma 2.7 ist dann $LL^{-1} = G^3$ und damit $LL^{-1} \cap \operatorname{Z}(G) \neq 1$. Man kann daher Lemma 2.9 mit $N := LL^{-1} \cap \operatorname{Z}(G)$ anwenden, und erhält, dass $c_{KK^{-1}L}$ eine Potenz von $p$ ist.

Sei nun $L \subseteq KK^{-1}$ eine Konjugationsklasse der Länge $p$ und $t \in L$. Dann hat $\operatorname{C}_G(t)$ die Ordung $p^4$. Wir können annehmen, dass $t$ die Form $t = xgx^{-1}g^{-1}$ mit $g \in G$ hat. Im Fall $g \in M$ ist $t \in M'$ und damit $L \subseteq M'$. Wegen $|M'| \leq p^2$ ist

dann $LL^{-1} = [G, M']$ nach Lemma 2.7. Also folgt in diesem Fall die Behauptung aus Lemma 2.9 mit $N := LL^{-1} \cap \mathrm{Z}(G) = [G, M'] \cap \mathrm{Z}(G) \neq 1$. Wir können daher $g \notin M$ annehmen. Dann ist $G = M\langle g\rangle = G'\langle x, g\rangle = \Phi(G)\langle x, g\rangle = \langle x, g\rangle$. Wegen $[x, g] = t \in \mathrm{Z}(\mathrm{C}_G(t))$ ist dann $G/\mathrm{Z}(\mathrm{C}_G(t))$ abelsch und $G' \subseteq \mathrm{Z}(\mathrm{C}_G(t))$. Da $G'$ die Ordnung $p^3$ hat, ist $\mathrm{C}_G(t)/\mathrm{Z}(\mathrm{C}_G(t))$ zyklisch und damit $\mathrm{C}_G(t)$ abelsch. Nach Satz 2.4 ist dies aber ausgeschlossen. □

Im nächsten Abschnitt werden wir Gruppen der Ordnung $p^6$ betrachten.

## 2.3 Gruppen der Ordnung $p^6$

Wir benötigen zunächst einige Hilfssätze.

**Lemma 2.11.** *Die $p$-Sylowgruppen von $\mathrm{GL}(3, p)$ sind nichtabelsch, und haben die Ordnung $p^3$.*

*Beweis.* Wegen $|\mathrm{GL}(3, p)| = (p^3 - 1)(p^3 - p)(p^3 - p^2) = p^3(p^3 - 1)(p^2 - 1)(p - 1)$ hat jede $p$-Sylowgruppe von $\mathrm{GL}(3, p)$ die Ordnung $p^3$. Bekanntlich bilden die oberen Dreiecksmatrizen mit Einsen auf der Hauptdiagonale eine $p$-Sylowgruppe $P$ von $\mathrm{GL}(3, p)$. Wegen

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ in } \mathrm{GL}(3, p)$$

ist $P$ nichtabelsch. □

**Lemma 2.12.** *Sei $G = \langle a\rangle \times \langle b\rangle$ mit $|\langle a\rangle| = p^2$ und $|\langle b\rangle| = p$ für eine Primzahl $p$. Dann hat die Automorphismengruppe von $G$ die Ordnung $p^3(p - 1)^2$ und nur eine $p$-Sylowgruppe. Diese ist nichtabelsch, und hat die Ordnung $p^3$.*

*Beweis.* Offenbar ist jeder Automorphismus von $G$ durch die Bilder von $a$ und $b$ bereits eindeutig bestimmt. Man überlegt sich dann, dass für jeden Automorphismus $\alpha$ gilt:

$$\alpha(a) = a^i b^j,\ \alpha(b) = a^{kp} b^l \text{ mit } j, k, l \in \{0, \ldots, p - 1\},\ l \neq 0,$$
$$i \in \{1, \ldots, p^2 - 1\} \text{ und } \mathrm{ggT}(i, p) = 1.$$

Für verschiedene Wahlen von $i, j, k$ oder $l$ erhält man verschiedene Automorphismen. Da es für die Wahl von $i$ genau $|(\mathbb{Z}/p^2\mathbb{Z})^\times| = p(p-1)$ Möglichkeiten gibt, hat $\mathrm{Aut}(G)$ also die Ordnung $p^3(p - 1)^2$. Wir definieren einen Automorphismus $\alpha$ durch

$$\alpha(a) = a^{1+p} b,\ \alpha(b) = b.$$

Wegen $\alpha^p(a) = \alpha^{p-1}(a^{1+p})b = \ldots = a^{(1+p)^p} b^{1+(1+p)+(1+p)^2+\ldots+(1+p)^{p-1}} = ab^{\frac{(1+p)^p-1}{p}} = a$ hat $\alpha$ die Ordnung $p$. Sei nun $\beta$ ein weiterer Automorphismus von $G$ mit

$$\beta(a) = a,\ \beta(b) = a^p b.$$

Wegen $\beta^p(b) = a^p\beta^{p-1}(b) = \ldots = a^{p^2}b = b$ hat auch $\beta$ die Ordnung $p$. Da $\alpha(\beta(a)) = \alpha(a) = a^cb \neq a^{c+p}b = \beta(a^cb) = \beta(\alpha(a))$ gilt, ist $\beta$ nicht mit $\alpha$ vertauschbar.

Wir zeigen nun, dass $\mathrm{Aut}(G)$ nur eine $p$-Sylowgruppe besitzt. Dazu überlegt man sich zunächst, dass $\Phi(G) = \langle a^p\rangle$ gilt. Da $\Phi(G)$ charakteristisch in $G$ ist, kann man jeden Automorphismus von $G$ auf $\Phi(G)$ einschränken. Die entsprechende Abbildung

$$\pi : \mathrm{Aut}(G) \to \mathrm{Aut}(\Phi(G)),\ \alpha \mapsto \alpha|_{\Phi(G)}$$

ist ein Homomorphismus. Da jeder Automorphismus $\varphi$ von $\Phi(G)$ die Form $\varphi(a^p) = a^{ip}$ mit $i \in \{1, \ldots, p-1\}$ hat, ist $\pi$ surjektiv. Also ist $\mathrm{Ker}(\pi)$ ein Normalteiler der Ordnung $p^3(p-1)$ in $\mathrm{Aut}(G)$. Jede $p$-Sylowgruppe von $\mathrm{Ker}(\pi)$ ist offenbar normal in $\mathrm{Ker}(\pi)$ und damit auch normal in $\mathrm{Aut}(G)$. Dies zeigt, dass $\mathrm{Aut}(G)$ nur eine $p$-Sylowgruppe $P$ besitzen kann. Insbesondere ist $\alpha, \beta \in P$, und $P$ ist nichtabelsch. □

**Definition 2.1.** Sei $G$ eine endliche Gruppe und $A$ ein abelscher Normalteiler von $G$. Man nennt $A$ einen *maximal abelschen Normalteiler* von $G$, falls kein abelscher Normalteiler $B$ von $G$ mit $A < B$ existiert.

Bekanntlich gilt für einen maximal abelschen Normalteiler $A$ einer endlichen $p$-Gruppe $G$ stets $\mathrm{C}_G(A) = A$ (siehe Satz III.7.3 in [5]).

**Lemma 2.13.** *Sei $G$ eine endliche $p$-Gruppe der Ordnung $p^6$ und $|G'| = p^3$. Dann ist $G'$ abelsch, aber kein maximal abelscher Normalteiler von $G$. Insbesondere existiert ein abelscher Normalteiler $A$ von $G$ mit $G' < A \leq \mathrm{C}_G(G')$.*

*Beweis.* Aus Satz III.7.8(b) in [5] folgt, dass $G'$ abelsch ist. Nehmen wir $G' = \mathrm{C}_G(G')$ an. Bekanntlich ist dann $G/\mathrm{C}_G(G')$ isomorph zu einer Untergruppe von $\mathrm{Aut}(G')$. Ist $G'$ zyklisch, so ist $|\mathrm{Aut}(G')| = p^2(p-1)$. Wegen $|G/\mathrm{C}_G(G')| = p^3$ ist dieser Fall ausgeschlossen.

Sei nun $G'$ elementarabelsch. Dann ist $\mathrm{Aut}(G') \cong \mathrm{GL}(3,p)$, und nach Lemma 2.11 wäre $G/\mathrm{C}_G(G')$ isomorph zu einer $p$-Sylowgruppe von $\mathrm{GL}(3,p)$. Da $G/\mathrm{C}_G(G') = G/G'$ abelsch ist, kann dieser Fall auch ausgeschlossen werden.

Sei schließlich $G' = \langle a\rangle \times \langle b\rangle$ mit $|\langle a\rangle| = p^2$ und $|\langle b\rangle| = p$. Dann kann man Lemma 2.12 anwenden, und erhält wie eben einen Widerspruch. □

**Lemma 2.14.** *Sei $G$ eine endliche $p$-Gruppe und $g, h \in G$. Sind die Elemente $[h, g^i]$ und $[h, g^j]$ mit $i, j \in \mathbb{Z}$ und $i \not\equiv j \pmod p$ konjugiert, so ist $[h, g^i] = [h, g^j]$.*

*Beweis.* Sei $G$ ein Gegenbeispiel minimaler Ordnung. Dann erfüllen auch $\overline{G} := G/\mathrm{Z}(G)$, $\overline{g} := g\,\mathrm{Z}(G)$ und $\overline{h} := h\,\mathrm{Z}(G)$ die Voraussetzung des Satzes, und da $G$ minimal gewählt war, folgt $[\overline{h}, \overline{g}^i] = [\overline{h}, \overline{g}^j]$. Also ist $\overline{g}^{i-j} \in \mathrm{C}_{\overline{G}}(\overline{h})$. Wegen $i - j \not\equiv 0 \pmod p$ ist $\langle g\rangle = \langle g^{i-j}\rangle$ und $\overline{g}^i \in \langle \overline{g}^{i-j}\rangle \subseteq \mathrm{C}_{\overline{G}}(\overline{h})$. Also ist $[\overline{h}, \overline{g}^i] = 1$ und $[h, g^i] \in \mathrm{Z}(G)$. Damit erhalten wir einen Widerspruch. □

Das nächste Lemma verallgemeinert Satz 2.3.

**Lemma 2.15.** *Sei $G$ eine endliche $p$-Gruppe, $K$ eine Konjugationsklasse von $G$ und $n \in \mathbb{N}_0$. Gilt $|KK^{-1} \cap Z_n(G)| = 1$ und $KK^{-1} \subseteq Z_{n+1}(G)$, so ist $\eta(K) = |K|$. Nach Lemma 2.10*(vi) *ist also $c_{KK^{-1}L}$ für $L \in \mathrm{Cl}(G)$ entweder 0 oder eine Potenz von $p$. Insbesondere sind* (P3), (P2) *und* (P1) *erfüllt.*

*Beweis.* Sei $x \in K$. Nehmen wir an, dass $[x, g]$ und $[x, h]$ mit $g, h \in G$ konjugiert sind. Mit den Bezeichnungen $\overline{G} := G/Z_n(G)$, $\overline{x} := xZ_n(G)$ usw. sind dann auch $[\overline{x}, \overline{g}]$ und $[\overline{x}, \overline{h}]$ in $\overline{G}$ konjugiert. Wegen

$$[\overline{x}, \overline{g}] \in KK^{-1}Z_n(G)/Z_n(G) \subseteq Z_{n+1}(G)/Z_n(G) = \mathrm{Z}(\overline{G})$$

ist dann sogar $[\overline{x}, \overline{g}] = [\overline{x}, \overline{h}]$, und wir erhalten $[x, g^{-1}h] \in KK^{-1} \cap Z_n(G) = 1$. Also ist $[x, g] = [x, h]$. Dies zeigt, dass die Elemente in $xK^{-1} \subseteq KK^{-1}$ paarweise nichtkonjugiert sind. Also ist $\eta(K) \geq |xK^{-1}| = |K|$, und aus Lemma 2.10(v) folgt die Behauptung. □

Die folgenden zwei Lemmata zeigen, dass (P3) für spezielle Gruppen der Ordnung $p^6$ gilt.

**Lemma 2.16.** *Sei $G$ eine endliche $p$-Gruppe der Ordnung $p^6$ und $K$ eine Konjugationsklasse von $G$ der Länge $p^2$ mit $x \in K$. Gilt dann $|KK^{-1} \cap \mathrm{Z}(G)| = p$ und $\mathrm{C}_G(x) \trianglelefteq G$, so ist $c_{KK^{-1}L}$ für $L \in \mathrm{Cl}(G)$ entweder 0 oder eine Potenz von $p$.*

Unter den angegebenen Voraussetzungen folgt aus Lemma 2.8 und Satz 2.5 bereits, dass (P1) und (P2) erfüllt sind.

*Beweis.* Wir wählen ein $g \in G$ mit $1 \neq [x, g] \in KK^{-1} \cap \mathrm{Z}(G)$. Offensichtlich ist dann auch $[x, g^i] = ([x, g]g)^i g^{-i} = [x, g]^i \in KK^{-1} \cap \mathrm{Z}(G)$ für $i \in \mathbb{Z}$. Im Fall $g^p \notin \mathrm{C}_G(x)$ wäre $|KK^{-1} \cap \mathrm{Z}(G)| = p^2$. Also ist $g^p \in \mathrm{C}_G(x)$ und $\mathrm{C}_G(x)\langle g\rangle < G$. Wir wählen nun ein $h \in G$ mit $G = \mathrm{C}_G(x)\langle g, h\rangle$. Jede Konjugationsklasse in $KK^{-1}$ besitzt dann ein Element der Form $[x, h^i g^j]$ mit $i, j \in \{0, \ldots, p-1\}$. Offenbar ist $[x, h] \notin \mathrm{Z}(G)$. Wir analysieren nun, wie viele Elemente der Form $[x, h^i g^j]$ zueinander konjugiert sind. Für $i = 0$ erhält man genau die Elemente in $KK^{-1} \cap \mathrm{Z}(G)$. Für $j = 0$ sind nach Lemma 2.14 die Elemente der Form $[x, h^i]$ mit $i \in \{1, \ldots, p-1\}$ paarweise nichtkonjugiert. Wir werden nun zeigen, dass auch zwei Elemente $[x, h^i g^j]$ und $[x, h^k g^l]$ mit $i, j, k, l \in \{0, \ldots, p-1\}$ und $0 \neq i \neq k \neq 0$ nicht konjugiert sein können. Ersetzt man $h$ durch $h^i g^j$, so kann man $i = 1$ und $j = 0$ annehmen. Wegen $[x, g^l] \in \mathrm{Z}(G)$ kann man $[x, h^k g^l]$ in der Form

$$[x, h^k g^l] = [x, h^k]h^k[x, g^l]h^{-k} = [x, h^k][x, g]^l$$

schreiben. Sind nun $[x, h]$ und $[x, h^k g^l]$ konjugiert, so existiert ein $y \in G$ mit

$$y[x, h]y^{-1} = [x, h^k g^l] = [x, h^k][x, g]^l.$$

Insbesondere ist $y[x, h]y^{-1} \equiv [x, h^k] \pmod{\mathrm{Z}(G)}$. Mit den Bezeichnungen $\overline{G} := G/\mathrm{Z}(G)$, $\overline{x} := x\,\mathrm{Z}(G)$ und $\overline{h} := h\,\mathrm{Z}(G)$ sind also $[\overline{x}, \overline{h}]$ und $[\overline{x}, \overline{h}^k]$ in $\overline{G}$ konjugiert.

Nach Lemma 2.14 ist daher $[\overline{x},\overline{h}] = [\overline{x},\overline{h}^k]$ und $[x,h^{k-1}] \in \mathrm{Z}(G)$. Wegen $1 = i \neq k$ ist dies ein Widerspruch. Daraus folgt, dass $[x,h]$ nicht zu $[x,h^kg^l]$ konjugiert sein kann. Schließlich zeigen wir, dass für ein festes $i \in \{1,\ldots,p-1\}$ die Elemente der Form $[x,h^ig^j]$ mit $j \in \{0,\ldots,p-1\}$ entweder alle konjugiert oder paarweise nichtkonjugiert sind. Sei dazu $[x,h^ig^j]$ zu $[x,h^ig^k]$ konjugiert und $j \neq k$. Wie eben können wir $i = 1$ und $j = 0$ annehmen. Dann existiert ein $y \in G$ mit $y[x,h]y^{-1} = [x,h][x,g]^k$. Für $l \in \{0,\ldots,p-1\}$ erhält man damit

$$y^l[x,h]y^{-l} = y^{l-1}[x,h]y^{1-l}[x,g]^k = \ldots = [x,h][x,g]^{kl} = [x,hg^{kl}].$$

Wegen $k \not\equiv 0 \pmod p$ sind in diesem Fall alle Elemente der angegebenen Form konjugiert. Ist $L$ eine Konjugationsklasse in $KK^{-1}$, so gilt also $|L \cap xK^{-1}| \in \{1,p\}$. Wegen $\mathrm{C}_G(x) \trianglelefteq G$ ist $\mathrm{C}_G(x) \subseteq \mathrm{C}_G(KK^{-1})$. Für $t \in L$ ist daher $\mathrm{C}_G(x) \subseteq \mathrm{C}_G(t) \trianglelefteq G$. Die Behauptung folgt nun aus Lemma 2.10(viii). □

**Lemma 2.17.** *Sei $G$ eine endliche $p$-Gruppe der Ordnung $p^6$ und $K$ eine Konjugationsklasse von $G$ der Länge $p^2$ mit $x \in K$. Gelten dann die folgenden Bedingungen*

*(i)* $KK^{-1} \cap \mathrm{Z}(G) = 1$,

*(ii)* $1 \neq y \in KK^{-1} \cap Z_2(G) \;\Rightarrow\; |\mathrm{C}_G(y)| = p^5$,

*(iii)* $G' \subseteq \mathrm{C}_G(x)$,

*(iv)* $\exists N \trianglelefteq G : KK^{-1} \subseteq N,\ |N| = p^3$,

*so ist $c_{KK^{-1}L}$ für $L \in \mathrm{Cl}(G)$ entweder 0 oder eine Potenz von $p$.*

*Beweis.* Im Fall $KK^{-1} \subseteq Z_2(G)$ folgt die Behauptung aus Lemma 2.15 mit $n := 1$. Wir werden daher $KK^{-1} \nsubseteq Z_2(G)$ voraussetzen. Aus $x \in \mathrm{Z}(\mathrm{C}_G(x)) \trianglelefteq G$ folgt $\langle K\rangle \subseteq \mathrm{Z}(\mathrm{C}_G(x))$. Wegen $|\langle K\rangle| > |K| = p^2$ ist daher $\mathrm{C}_G(x)/\mathrm{Z}(\mathrm{C}_G(x))$ zyklisch und $\mathrm{C}_G(x)$ abelsch. Für ein $t \in KK^{-1}$ gilt stets $\mathrm{C}_G(x) \subseteq \mathrm{C}_G(G') \subseteq \mathrm{C}_G(t) \trianglelefteq G$. Wir können also Lemma 2.10(viii) anwenden.

Wir betrachten nun $KK^{-1} \cap Z_2(G)$. Hat $G$ Nilpotenzklasse kleiner gleich 4, so ist $KK^{-1} \subseteq G' \subseteq Z_3(G)$. Hat $G$ maximale Klasse, so ist $KK^{-1} \subseteq N = Z_3(G)$ nach Hilfssatz III.14.2(b) in [5]. Nach Lemma 2.15 können wir also $KK^{-1} \cap Z_2(G) \neq 1$ annehmen. Sei also $g \in G$ mit $1 \neq [x,g] \in KK^{-1} \cap Z_2(G)$. Dann gilt auch $[x,g^2] = [x,g]g[x,g]g^{-1} \in Z_2(G)$ und induktiv $[x,g^i] \in KK^{-1} \cap Z_2(G)$ für $i \in \mathbb{Z}$. Im Fall $g^p \notin \mathrm{C}_G(x)$ hätte jede Konjugationsklasse in $KK^{-1}$ ein Element der Form $[x,g^i] \in Z_2(G)$ mit $i \in \mathbb{Z}$. Dann wäre aber $KK^{-1} \subseteq Z_2(G)$. Also ist $g^p \in \mathrm{C}_G(x)$ und $\mathrm{C}_G(x)\langle g\rangle < G$. Wählt man nun ein $h \in G$ mit $G = \mathrm{C}_G(x)\langle g,h\rangle$, so enthält jede Konjugationsklasse in $KK^{-1}$ ein Element der Form $[x,h^ig^j]$ mit $i,j \in \{0,\ldots,p-1\}$. Im Fall $[x,h] \in Z_2(G)$ wäre $[x,h^ig^j] = [x,h^i]h^i[x,g^j]h^{-i} \in Z_2(G)$ für alle $i,j \in \{0,\ldots,p-1\}$ und damit $KK^{-1} \subseteq Z_2(G)$. Also enthält $KK^{-1} \cap Z_2(G)$ entsprechend den Elementen $[x,g^j]$ genau $p$ Konjugationsklassen. Ist $L$ eine von diesen, so gilt $|L \cap xK^{-1}| = 1$. Also folgt $c_{KK^{-1}L} = |K|/|L|$ aus Lemma 2.10(viii).

Wir untersuchen nun die Konjugationsklassen in $KK^{-1} \setminus Z_2(G)$. Nach Lemma 2.14 sind die Elemente $[x,h^i]$ mit $i \in \{1,\ldots,p-1\}$ paarweise nichtkonjugiert. Nehmen

wir nun an, dass $[x, h^i g^j]$ und $[x, h^k g^l]$ mit $i, j, k, l \in \{0, \ldots, p-1\}$ und $0 \neq i \neq k \neq 0$ konjugiert sind. Ersetzt man $h$ durch $h^i g^j$, so kann man $i = 1$ und $j = 0$ annehmen. Mit den Bezeichnungen $\overline{G} := G/Z_2(G)$, $\overline{x} := xZ_2(G)$ usw. sind dann auch $[\overline{x}, \overline{h}]$ und $[\overline{x}, \overline{h}^k \overline{g}^l]$ in $\overline{G}$ konjugiert. Wegen

$$[\overline{x}, \overline{h}] \in KK^{-1}Z_2(G)/Z_2(G) \subseteq Z_3(G)/Z_2(G) = \mathrm{Z}(\overline{G})$$

ist dann sogar $[\overline{x}, \overline{h}] = [\overline{x}, \overline{h}^k \overline{g}^l]$, und man erhält $[x, h^{k-1} g^l] \in Z_2(G)$. Wegen $1 = i \neq k$ ist das ausgeschlossen. Wir zeigen schließlich, dass für ein festes $i \in \{1, \ldots, p-1\}$ die Elemente $[x, h^i g^j]$ mit $j \in \{0, \ldots, p-1\}$ entweder alle konjugiert oder paarweise nichtkonjugiert sind. Die Behauptung folgt dann wieder mit Lemma 2.10(viii).

Nach (ii) hat die Konjugationsklasse von $[x, g]$ genau $p$ Elemente. Wegen $[x, g] \in Z_2(G)$ kann man jedes Konjugierte von $[x, g]$ in der Form $y[x, g]y^{-1} = [x, g]z$ mit $y \in G$ und $z \in \mathrm{Z}(G)$ schreiben. Außerdem ist $[x, g^i] = ([x, g]g)^i g^{-i} \equiv [x, g]^i \pmod{\mathrm{Z}(G)}$ für $i \in \{0, \ldots, p-1\}$. Wir unterscheiden nun zwei Fälle.

Sei $g \in \mathrm{C}_G([x, g])$.
Betrachten wir zunächst den Fall, dass $i, j \in \{0, \ldots, p-1\}$ mit $i \neq 0$ existieren, sodass die Konjugationsklasse von $[x, h^i g^j]$ aus $p$ Elementen besteht. Ersetzt man $h$ durch $h^i g^j$, so kann man $i = 1$ und $j = 0$ annehmen. Sei $s \in G$ mit $\mathrm{C}_G([x, h]) = \mathrm{C}_G(x)\langle s \rangle$. Im Fall $s \in \mathrm{C}_G([x, g])$ wäre $g \in \mathrm{C}_G([x, h])$. Da $\mathrm{C}_G(x)$ und $G/\mathrm{C}_G(x)$ abelsch sind, gilt dann

$$\begin{aligned} h[x, g]h^{-1} &= hxh^{-1}hgx^{-1}g^{-1}h^{-1} = (hxh^{-1})(ghx^{-1}h^{-1}g^{-1}) \\ &= (ghx^{-1}h^{-1}g^{-1})(hxh^{-1})x^{-1}x = ghx^{-1}h^{-1}g^{-1}[x, h]^{-1}x \\ &= (gx^{-1}g^{-1})x = x(gx^{-1}g^{-1}) = [x, g]. \end{aligned} \tag{A}$$

Also ist $h \in \mathrm{C}_G([x, g])$, und wir erhalten den Widerspruch $[x, g] \in \mathrm{Z}(G)$. Dies zeigt $s \notin \mathrm{C}_G([x, g])$. Sind nun $[x, hg^i]$ und $[x, hg^j]$ mit $i, j \in \{0, \ldots, p-1\}$ und $i \neq j$ konjugiert, so existieren $y \in G$ und $z \in \mathrm{Z}(G)$ mit

$$\begin{aligned} y[x, h]y^{-1}yh[x, g^i]h^{-1}y^{-1} = y[x, hg^i]y^{-1} = [x, hg^j] = [x, h]h[x, g^j]h^{-1}, \\ y[x, h]y^{-1}[x, g]^i = [x, h][x, g]^j z. \end{aligned} \tag{B}$$

Also ist $y[x, h]y^{-1} = [x, h][x, g]^{j-i}z$, und wegen $i \neq j$ erhalten wir den Widerspruch $s \notin \mathrm{C}_G(y[x, h]y^{-1}) = \mathrm{C}_G([x, h])$. Folglich sind die Elemente $[x, hg^j]$ mit $j \in \{0, \ldots, p-1\}$ paarweise nichtkonjugiert. Aus $[x, h^i] = [x, h]h[x, h^{i-1}]h^{-1}$ und $\mathrm{C}_G([x, h]) \trianglelefteq G$ folgt induktiv $\mathrm{C}_G([x, h]) = \mathrm{C}_G([x, h^i])$ für $i \in \{1, \ldots, p-1\}$. Analog zeigt man daher, dass für ein festes $i \in \{1, \ldots, p-1\}$ die Elemente $[x, h^i g^j]$ mit $j \in \{0, \ldots, p-1\}$ auch paarweise nichtkonjugiert sind.

Nehmen wir nun an, dass für alle $i, j \in \{0, \ldots, p-1\}$ mit $i \neq 0$ die Konjugationsklasse von $[x, h^i g^j]$ die Länge $p^2$ hat. Wegen $|KK^{-1}| \leq |N| = p^3$ kann es dann höchstens $p-1$ derartige Konjugationsklassen geben, und wir erhalten, dass für ein festes $i \in \{1, \ldots, p-1\}$ die Elemente $[x, h^i g^j]$ mit $j \in \{0, \ldots, p-1\}$ konjugiert sein müssen.

Sei nun $g \notin \mathrm{C}_G([x, g])$.
Durch eine geeignete Wahl von $h$ kann man dann $\mathrm{C}_G([x, g]) = \mathrm{C}_G(x)\langle h \rangle$ annehmen.

Vertauscht man nun $g$ und $h$ in Rechnung (A), so sieht man, dass $g \in \mathrm{C}_G([x,h])$ gilt. Nehmen wir an, dass $[x,hg^i]$ und $[x,hg^j]$ mit $i,j \in \{0,\dots,p-1\}$ und $i \neq j$ konjugiert sind. Dann existiert ein $y \in G$ mit $y[x,hg^i]y^{-1} = [x,hg^j]$. Wie in Rechnung (B) folgt dann der Widerspruch $g \notin \mathrm{C}_G(y[x,h]y^{-1}) = \mathrm{C}_G([x,h])$. Also sind die Elemente $[x,hg^j]$ mit $j \in \{0,\dots,p-1\}$ paarweise nichtkonjugiert. Wie im Fall $g \in \mathrm{C}_G([x,g])$ sieht man nun, dass für ein festes $i \in \{1,\dots,p-1\}$ die Elemente $[x,h^ig^j]$ mit $j \in \{0,\dots,p-1\}$ auch paarweise nichtkonjugiert sind. Damit ist das Lemma bewiesen. □

Wir sind nun in der Lage, (P3) für Gruppen der Ordnung $p^6$ zu beweisen.

**Satz 2.6.** *Sei $G$ eine endliche $p$-Gruppe der Ordnung $p^6$ und $K$ eine Konjugationsklasse von $G$. Für $L \in \mathrm{Cl}(G)$ ist dann $c_{KK^{-1}L}$ entweder 0 oder eine Potenz von $p$. Insbesondere sind* (P3)*,* (P2) *und* (P1) *erfüllt.*

*Beweis.* Nach Satz 2.2 genügt es, die Fälle $|K| = p^2$ und $|K| = p^3$ zu betrachten. Außerdem können wir nach Lemma 2.3 stets $|K| < |KK^{-1}|$ voraussetzen. Wegen $KK^{-1} \subseteq G'$ gilt also $|G'| \in \{p^3, p^4\}$. Daher wird der Beweis aus zwei Teilen bestehen: Im ersten Teil untersuchen wir den Fall $|G'| = p^3$ und im zweiten den Fall $|G'| = p^4$. Beide Teile werden in weitere Fallunterscheidungen unterteilt. Es gilt stets $x \in K$.

**Fall 1:** $|G'| = p^3$.
Im Fall $|K| = p^3$ wäre $|K| = |KK^{-1}|$. Also können wir uns auf den Fall $|K| = p^2$ beschränken. Nach Lemma 2.13 existiert ein abelscher Normalteiler $A$ von $G$ mit $G' < A$, und nach Satz 2.4 hat $A$ die Ordnung $p^4$. Es gilt $|\,\mathrm{C}_G(x)| = p^4$, und aus Lemma 2.6 folgt $A\,\mathrm{C}_G(x) < G$. Nach Lemma 2.7 ist $x \notin G'$. Wegen $KK^{-1} \subseteq G'$ hat jede Konjugationsklasse in $KK^{-1}$ höchstens die Länge $p^2$. Wir werden nun weitere Fallunterscheidungen machen.

**Fall 1.1:** $G' \nsubseteq \mathrm{C}_G(x)$.
Es gilt $x \notin A$, denn im Fall $x \in A \subseteq \mathrm{C}_G(G')$ wäre $G' \subseteq \mathrm{C}_G(x)$. Also ist $p^4 = |A| < |A\langle x\rangle| \leq |A\,\mathrm{C}_G(x)| \leq p^5$ und damit $M := A\langle x\rangle = A\,\mathrm{C}_G(x)$. Wegen $|\,\mathrm{C}_A(x)| = |A \cap \mathrm{C}_G(x)| = p^3$ gibt es daher genau $|A : \mathrm{C}_A(x)| = p$ Konjugierte von $x$ unter $A$. Definiert man $H := \{xax^{-1}a^{-1} : a \in A\} \subseteq KK^{-1} \subseteq G' \subseteq A$, so kann man wie in Lemma 2.2 zeigen, dass $H$ eine Untergruppe von $G$ ist. Außerdem ist $|H| = |A : \mathrm{C}_A(x)| = p$. Wegen $xHx^{-1} = H$ ist $H$ ein Normalteiler von $M$. Da $M/H$ abelsch ist, folgt $M' \subseteq H$. Wegen $|H| = p$ ist dann $M' \subseteq \mathrm{Z}(G)$. Wir berechnen nun die Klassenmultiplikationskonstanten. Für jede Konjugationsklasse $L \nsubseteq KK^{-1}$ gilt offensichtlich $c_{KK^{-1}L} = 0$. Ist $L \subseteq KK^{-1} \cap \mathrm{Z}(G)$, so gilt $c_{KK^{-1}L} = |K|$ nach Lemma 2.10(iii). Sei nun $L \subseteq KK^{-1} \subseteq G'$ eine Konjugationsklasse der Länge $p^2$. Nach Lemma 2.7 ist dann $LL^{-1} = G^3$ und damit $LL^{-1} \cap \mathrm{Z}(G) \neq 1$. Man kann daher Lemma 2.9 mit $N := LL^{-1} \cap \mathrm{Z}(G)$ anwenden, und erhält auf diese Weise, dass $c_{KK^{-1}L}$ eine Potenz von $p$ ist.

Sei nun $L \subseteq KK^{-1}$ eine Konjugationsklasse der Länge $p$ und $t \in L$.
Annahme: $\mathrm{C}_G(x) \subseteq \mathrm{C}_G(t)$.
Wegen $A \subseteq \mathrm{C}_G(G') \subseteq \mathrm{C}_G(t)$ ist dann $M = A\,\mathrm{C}_G(x) = \mathrm{C}_G(t)$. Wegen $\mathrm{C}_G(t) \trianglelefteq G$ kann man $t$ durch jedes zu $t$ konjugierte Element ersetzen, und daher annehmen,

dass $t$ die Form $t = xgx^{-1}g^{-1}$ mit $g \in G$ hat. Im Fall $g \in M$ wäre $t \in M' \subseteq \mathrm{Z}(G)$. Also ist $g \notin M$ und $G = M\langle g\rangle = \mathrm{C}_G(t)\langle g\rangle$. Für jedes $c \in \mathrm{C}_G(x) \subseteq \mathrm{C}_G(t)$ ist

$$xgx^{-1}g^{-1} = t = ctc^{-1} = xcgx^{-1}g^{-1}c^{-1},$$

d. h. $c \in \mathrm{C}_G(gx^{-1}g^{-1}) = g\,\mathrm{C}_G(x)g^{-1}$. Also ist $\mathrm{C}_G(x) = g\,\mathrm{C}_G(x)g^{-1}$ und $g \in \mathrm{N}_G(\mathrm{C}_G(x))$. Wegen $|\,\mathrm{C}_G(t) : \mathrm{C}_G(x)| = p$ ist auch $\mathrm{C}_G(t) \subseteq \mathrm{N}_G(\mathrm{C}_G(x))$. Insgesamt erhält man $G = \mathrm{C}_G(t)\langle g\rangle \subseteq \mathrm{N}_G(\mathrm{C}_G(x))$. Also ist $\mathrm{C}_G(x)$ ein Normalteiler mit abelscher Faktorgruppe, und wir erhalten den Widerspruch $G' \subseteq \mathrm{C}_G(x)$.
Folglich können wir $\mathrm{C}_G(x) \nsubseteq \mathrm{C}_G(t)$ annehmen. Wegen $\mathrm{C}_G(t)\,\mathrm{C}_G(x) = G$ ist dann $|\,\mathrm{C}_G(t) \cap \mathrm{C}_G(x)| = p^3$ und damit $|\,\mathrm{C}_G(t) : \mathrm{C}_G(t) \cap \mathrm{C}_G(x)| = p^2$. Also folgt aus Lemma 2.10(i), (iv) schließlich $c_{KK^{-1}L} = |K|$. Damit ist die Behauptung in diesem Fall gezeigt.

**Fall 1.2:** $G' \subseteq \mathrm{C}_G(x)$.
Gilt $|KK^{-1} \cap \mathrm{Z}(G)| = p^2$, so erhalten wir den Widerspruch $|K| = |KK^{-1}|$ aus Lemma 2.10(v). Im Fall $|KK^{-1} \cap \mathrm{Z}(G)| = p$ folgt die Behauptung aus Lemma 2.16. Also können wir $KK^{-1} \cap \mathrm{Z}(G) = 1$ annehmen. Wir zeigen nun, dass dann die Voraussetzungen von Lemma 2.17 erfüllt sind.

Wie im Beweis von Lemma 2.17 können wir $KK^{-1} \nsubseteq Z_2(G)$ und $KK^{-1} \cap Z_2(G) \neq 1$ voraussetzen. Insbesondere ist $|G' \cap Z_2(G)| \in \{p, p^2\}$. Da $G/\,\mathrm{C}_G(G' \cap Z_2(G))$ isomorph zu einer $p$-Untergruppe von $\mathrm{Aut}(G' \cap Z_2(G))$ ist, folgt dann $|G/\,\mathrm{C}_G(G' \cap Z_2(G))| = p$. Für $1 \neq y \in KK^{-1} \cap Z_2(G)$ ist daher $|\,\mathrm{C}_G(y)| = |\,\mathrm{C}_G(G' \cap Z_2(G))| = p^5$. Also folgt nun die Behauptung aus Lemma 2.17 mit $N := G'$.

Damit ist die Aussage im Fall $|G'| = p^3$ bewiesen, und wir kommen nun zum zweiten Teil des Beweises.

**Fall 2:** $|G'| = p^4$.
In diesem Fall ist $G'$ nicht notwendig abelsch, und wir müssen auch beachten, dass $K$ neben $p^2$ auch die Länge $p^3$ haben kann. Da $G$ nichtzyklisch ist, folgt $G' = \Phi(G)$. Insbesondere ist $G/G' = G/\Phi(G)$ elementarabelsch, und hat die Ordnung $p^2$. Wir unterscheiden nun, ob $G'$ abelsch ist oder nicht.

**Fall 2.1:** $G'$ ist abelsch.
Nach Satz 2.4 ist $G'$ ein maximal abelscher Normalteiler von $G$. Insbesondere gilt $G' = \mathrm{C}_G(G')$. Für alle $t \in KK^{-1} \subseteq G'$ ist $\mathrm{C}_G(G') \subseteq \mathrm{C}_G(t)$. Insbesondere hat jede Konjugationsklasse in $KK^{-1}$ höchstens die Länge $p^2$. Wir unterscheiden die Fälle $|K| = p^2$ und $|K| = p^3$.

**Fall 2.1.1:** $|K| = p^2$.
In diesem Fall kann sowohl $x \notin G'$ als auch $x \in G'$ auftreten. Wir unterscheiden diese beiden Fälle.

**Fall 2.1.1.1:** $x \notin G'$.
Die Situation ist hier ähnlich wie im Beweis von Satz 2.5. Nach Lemma 2.6 hat $M := G'\langle x\rangle = G'\,\mathrm{C}_G(x)$ die Ordnung $p^5$. Sei $H := \{xyx^{-1}y^{-1} : y \in G'\} \subseteq KK^{-1} \subseteq G'$. Da $G'$ abelsch ist, kann man wie bisher zeigen, dass $H$ eine Untergruppe von $G$ ist. Außerdem ist $|H| = |G' : \mathrm{C}_{G'}(x)| = p$ und $H \subseteq M'$. Wegen $xHx^{-1} = H$ ist $H \trianglelefteq M$.

Offenbar ist $M/H$ abelsch, und es folgt $M' \subseteq H$. Damit haben wir $H = M'$ gezeigt. Insbesondere ist $H \trianglelefteq G$ und $H \subseteq KK^{-1} \cap \mathrm{Z}(G)$. Im Fall $|KK^{-1} \cap \mathrm{Z}(G)| = p^2$ folgt der Widerspruch $|K| = |KK^{-1}|$ aus Lemma 2.10(v). Also ist $H = KK^{-1} \cap \mathrm{Z}(G)$, und $KK^{-1}$ enthält genau $p$ Konjugationsklassen der Länge 1. Ist $L$ eine von diesen, so gilt $c_{KK^{-1}L} = |K|$ nach Lemma 2.10(iii).

Nehmen wir nun an, dass $KK^{-1}$ eine Konjugationsklasse der Länge $p$ enthält. Dann existiert ein $t \in KK^{-1}$ mit $|\mathrm{C}_G(t)| = p^5$. Nach Satz 2.4 ist $\mathrm{C}_G(t)$ nichtabelsch. Wir können annehmen an, dass $t$ die Form $t = xgx^{-1}g^{-1}$ mit $g \in G$ hat. Im Fall $g \in M$ wäre $t \in M' = H \subseteq \mathrm{Z}(G)$. Also ist $g \notin M$ und $G = M\langle g\rangle = G'\langle x, g\rangle = \Phi(G)\langle x, g\rangle = \langle x, g\rangle$. Wegen $[x, g] = t \in \mathrm{Z}(\mathrm{C}_G(t))$ ist dann $G/\mathrm{Z}(\mathrm{C}_G(t))$ abelsch und $G' \subseteq \mathrm{Z}(\mathrm{C}_G(t))$. Da $G'$ die Ordnung $p^4$ hat, ist $\mathrm{C}_G(t)/\mathrm{Z}(\mathrm{C}_G(t))$ zyklisch. Da $\mathrm{C}_G(t)$ aber nichtabelsch ist, ist dies ausgeschlossen. Folglich enthält $KK^{-1}$ keine Konjugationsklasse der Länge $p$.

Wenn $l$ nun die Anzahl der Konjugationsklassen der Länge $p^2$ in $KK^{-1}$ bezeichnet, so gilt

$$p + l = \eta(K) \geq 2(p-1) + 1 = 2p - 1$$

nach Theorem A in [2]. Also ist $l \geq p - 1$. Sei nun $L$ eine Konjugationsklasse der Länge $p^2$ in $KK^{-1}$ und $t \in L$. Dann ist $\mathrm{C}_G(t) = G'$, und aus Lemma 2.10(iv) folgt $c_{KK^{-1}L} \geq |G' : \mathrm{C}_{G'}(x)| = p$. Die Augmentationsabbildung liefert $\nu(K^+(K^{-1})^+) = |K||K^{-1}| = p^4$. Andererseits folgt aus Gleichung $(\star\star)$ schließlich

$$\nu(K^+(K^{-1})^+) = \sum_{M \in \mathrm{Cl}(G)} c_{KK^{-1}M}|M| \geq |K||KK^{-1} \cap \mathrm{Z}(G)| + pl|L| \geq p^4.$$

Daher ist $l = p - 1$ und $c_{KK^{-1}L} = p$. In diesem Fall ist die Behauptung also gezeigt.

**Fall 2.1.1.2:** $x \in G'$.
Dann ist $G' = \mathrm{C}_G(x)$ und

$$KK^{-1} = \{gxg^{-1}hx^{-1}h^{-1} : g, h \in G\} = \{g[x, g^{-1}h]g^{-1} : g, h \in G\} \subseteq G^3 < G'.$$

Wegen $|K| < |KK^{-1}|$ hat $G^3$ die Ordnung $p^3$. Im Fall $|KK^{-1} \cap \mathrm{Z}(G)| = p^2$ erhalten wir den Widerspruch $|K| = |KK^{-1}|$ aus Lemma 2.10(v). Ist $|KK^{-1} \cap \mathrm{Z}(G)| = p$, so folgt die Behauptung aus Lemma 2.16. Also können wir $KK^{-1} \cap \mathrm{Z}(G) = 1$ annehmen. Wir zeigen nun, dass dann die Voraussetzungen von Lemma 2.17 erfüllt sind.

Hat $G$ Nilpotenzklasse kleiner gleich 4, so ist $G' \subseteq Z_3(G)$ und $KK^{-1} \subseteq G^3 \subseteq Z_2(G)$. Also folgt in diesem Fall die Behauptung aus Lemma 2.15 mit $n := 1$. Wir können daher annehmen, dass $G$ maximale Klasse hat. Dann ist $|\mathrm{Z}(G)| = p$. Für jedes $y \in KK^{-1} \cap Z_2(G)$ und $h \in G$ gilt $hyh^{-1} \in y\,\mathrm{Z}(G)$. Im Fall $y \neq 1$ hat daher die Konjugationsklasse von $y$ genau $p$ Elemente, und es folgt $|\mathrm{C}_G(y)| = p^5$. Die Behauptung folgt nun aus Lemma 2.17 mit $N := G^3$.

**Fall 2.1.2:** $|K| = p^3$.
Nach Lemma 2.7 ist $x \notin G'$, und nach Lemma 2.6 hat $M := G'\langle x\rangle = G'\,\mathrm{C}_G(x)$ die Ordnung $p^5$. Definiert man $H := \{xyx^{-1}y^{-1} : y \in G'\} \subseteq KK^{-1} \subseteq G'$, so gilt $|H| = |G' : \mathrm{C}_{G'}(x)| = p^2$. Da $G'$ abelsch ist, kann man wie bisher zeigen, dass $H$

eine Untergruppe von $G$ ist. Offenbar ist $H \subseteq M'$. Wegen $xHx^{-1} = H$ ist $H \trianglelefteq M$. Da $M/H$ abelsch ist, gilt auch $M' \subseteq H$, und es folgt $H = M'$. Insbesondere ist $H \trianglelefteq G$ und $1 \neq H \cap \mathrm{Z}(G) \subseteq KK^{-1} \cap \mathrm{Z}(G)$. Sei nun $y := xgx^{-1}g^{-1} \in KK^{-1} \cap \mathrm{Z}(G)$ mit $g \in G$. Wir nehmen zunächst $g \notin M$ an. Dann ist $G = M\langle g\rangle = G'\langle x, g\rangle = \Phi(G)\langle x, g\rangle = \langle x, g\rangle$. Wegen $[x, g] = y \in \mathrm{Z}(G)$ wäre dann aber $G/\mathrm{Z}(G)$ abelsch, und $G$ hätte Nilpotenzklasse kleiner gleich 2. Nach Satz 2.3 ist das ausgeschlossen. Also ist $g \in M$ und damit $y \in M' \cap \mathrm{Z}(G) = H \cap \mathrm{Z}(G)$. Dies zeigt schließlich $H \cap \mathrm{Z}(G) = KK^{-1} \cap \mathrm{Z}(G)$. Wir unterscheiden zwei Fälle.

**Fall 2.1.2.1:** $|KK^{-1} \cap \mathrm{Z}(G)| = p^2$.
In diesem Fall ist $KK^{-1} \cap \mathrm{Z}(G) = H$, und $KK^{-1}$ enthält genau $p^2$ Konjugationsklassen der Länge 1. Nehmen wir nun an, dass $KK^{-1}$ eine Konjugationsklasse der Länge $p$ enthält. Dann existiert ein $t \in KK^{-1}$ mit $|\mathrm{C}_G(t)| = p^5$. Nach Satz 2.4 ist $\mathrm{C}_G(t)$ nichtabelsch. Wir können annehmen, dass $t$ die Form $t = xgx^{-1}g^{-1}$ mit $g \in G$ hat. Im Fall $g \in M$ wäre $t \in M' = H \subseteq \mathrm{Z}(G)$. Also ist $g \notin M$ und $G = M\langle g\rangle = G'\langle x, g\rangle = \Phi(G)\langle x, g\rangle = \langle x, g\rangle$. Wegen $[x, g] = t \in \mathrm{Z}(\mathrm{C}_G(t)) \trianglelefteq G$ ist dann $G/\mathrm{Z}(\mathrm{C}_G(t))$ abelsch und $G' \subseteq \mathrm{Z}(\mathrm{C}_G(t))$. Da $G'$ die Ordnung $p^4$ hat, ist $\mathrm{C}_G(t)/\mathrm{Z}(\mathrm{C}_G(t))$ zyklisch. Da $\mathrm{C}_G(t)$ aber nichtabelsch ist, ist dies ausgeschlossen. Folglich enthält $KK^{-1}$ keine Konjugationsklasse der Länge $p$.

Sei nun $t \in KK^{-1}$ mit $|\mathrm{C}_G(t)| = p^4$. Dann ist $G' = \mathrm{C}_G(t)$. Wie bisher können wir annehmen, dass $t$ die Form $t = [x, g]$ mit $g \in G$ hat. Dann ist $g \notin M$. Wir analysieren nun, wie viele Elemente der Form $[x, h]$ mit $h \in G$ zu $t$ konjugiert sind. Wegen $M' \subseteq \mathrm{Z}(G) \subseteq \mathrm{C}_G(x)$ ist $\mathrm{C}_G(x) \trianglelefteq M$. Außerdem ist $x \notin G' = \mathrm{C}_G(t) = \mathrm{C}_G([x, g])$, und es folgt $\mathrm{C}_G(x) \neq \mathrm{C}_G(gxg^{-1})$ und $\mathrm{C}_G(x) \cap \mathrm{C}_G(gxg^{-1}) = \mathrm{Z}(G)$. Also ist $\mathrm{C}_G(x)\,\mathrm{C}_G(gxg^{-1})$ eine Untergruppe der Ordnung $p^4$ in $M$. Wir wählen $a \in \mathrm{C}_G(x)$ mit $\mathrm{C}_G(x)\,\mathrm{C}_G(gxg^{-1}) = \mathrm{C}_G(gxg^{-1})\langle a\rangle$ und $b \in G'$ mit $M = \mathrm{C}_G(x)\,\mathrm{C}_G(gxg^{-1})\langle b\rangle$. Wegen $g \notin M$ ist außerdem $G = M\langle g\rangle$. Man überlegt sich dann leicht, dass die Konjugationsklasse von $gxg^{-1}$ genau aus den Elementen $g^ib^ja^k(gxg^{-1})a^{-k}b^{-j}g^{-i}$ mit $i, j, k \in \{0, \ldots, p-1\}$ besteht. Offenbar sind alle Elemente der Form $[x, a^ig] = a^i[x, g]a^{-i} = a^ita^{-i}$ mit $i \in \{0, \ldots, p-1\}$ zu $t$ konjugiert. Betrachten wir nun den Fall, dass $t$ auch zu $[x, b^ia^jg]$ mit $i, j \in \{0, \ldots, p-1\}$ und $i \neq 0$ konjugiert ist. Ersetzt man $b$ durch $b^i$, so kann man $i = 1$ annehmen. Wegen $\mathrm{C}_G(x) \trianglelefteq M$ existiert ein $c \in \mathrm{C}_G(x)$ mit $ba^j = cb$. Dann ist $t$ auch zu $[x, bg]$ konjugiert. Sei nun $y \in G$ mit

$$yty^{-1} = y[x, g]y^{-1} = [x, bg] = [x, b]b[x, g]b^{-1} = [x, b][x, g].$$

Wegen $[x, b] \in H \subseteq \mathrm{Z}(G)$ folgt dann

$$y^lty^{-l} = [x, b]y^{l-1}[x, g]y^{1-l} = \ldots = [x, b]^l[x, g] = [x, b^lg]$$

für $l \in \{0, \ldots, p-1\}$. Also ist $t$ dann zu allen Elementen der Form $[x, a^ib^jg]$ mit $i, j \in \{0, \ldots, p-1\}$ konjugiert. Wegen $\mathrm{C}_G(gxg^{-1}) \trianglelefteq M$ sind das genau die $p^2$ Elemente der Form $[x, b^ia^jg]$ mit $i, j \in \{0, \ldots, p-1\}$. Diese Elemente bilden dann die ganze Konjugationsklasse von $t$. Nehmen wir nun an, dass $t$ zu $[x, g^ib^ja^kg]$ mit $i, j, k \in \{0, \ldots, p-1\}$ und $i \neq 0$ konjugiert ist. Wegen $M \trianglelefteq G$ existiert ein $y \in M$ mit $g^ib^ja^k = yg^i$. Dann ist $t$ zu $[x, yg^{i+1}]$ konjugiert, und es existiert ein $z \in G$ mit

$$ztz^{-1} = z[x, g]z^{-1} = [x, yg^{i+1}] = [x, y]y[x, g^{i+1}]y^{-1}.$$

Wegen $[x,y] \in H \subseteq \mathrm{Z}(G)$ ist also $z[x,g]z^{-1} \equiv y[x,g^{i+1}]y^{-1} \pmod{\mathrm{Z}(G)}$. Mit den Bezeichnungen $\overline{G} := G/\mathrm{Z}(G)$, $\overline{g} := g\,\mathrm{Z}(G)$ und $\overline{x} := x\,\mathrm{Z}(G)$ sind also $[\overline{x},\overline{g}]$ und $[\overline{x},\overline{g}^{i+1}]$ in $\overline{G}$ konjugiert. Nach Lemma 2.14 ist $[\overline{x},\overline{g}] = [\overline{x},\overline{g}^{i+1}]$ und damit $[x,g^i] \in \mathrm{Z}(G)$. Wegen $i \neq 0$ ist dies ein Widerspruch. Folglich kann $t$ zu keinem Element der Form $[x,g^ib^ja^kg]$ mit $i,j,k \in \{0,\ldots,p-1\}$ und $i \neq 0$ konjugiert sein.

Insgesamt haben wir also gesehen, dass $t$ entweder zu $p$ oder zu $p^2$ Elementen der Form $[x,h]$ mit $h \in G$ konjugiert ist. Wegen $\mathrm{C}_G(x) \nsubseteq G' = \mathrm{C}_G(t)$ können wir aber nicht Lemma 2.10(viii) anwenden. Wir werden daher auf andere Weise argumentieren. Bezeichnet man mit $L$ die Konjugationsklasse von $t$, so ist $c_{KK^{-1}L} \geq |G' : \mathrm{C}_{G'}(x)| = p^2$ nach Lemma 2.10(iv). Im Fall $|L \cap xK^{-1}| = p^2 = |L|$ folgt $c_{KK^{-1}L} = |K|$ aus Lemma 2.10(ii). Sei also $|L \cap xK^{-1}| = p$ und $t = hxh^{-1}kx^{-1}k^{-1}$ mit $h,k \in G$. Dann existiert ein $i \in \{0,\ldots,p-1\}$ mit $h^{-1}th = xh^{-1}kx^{-1}k^{-1}h = a^ita^{-i}$. Also ist $ha^i \in \mathrm{C}_G(t) = G'$, und es folgt $h \in M$. Wegen $|M : \mathrm{C}_G(x)| = p^2$ ist dann $c_{KK^{-1}L} \leq p^2$. Also ist $c_{KK^{-1}L} = p^2$, und die Behauptung ist in diesem Fall bewiesen.

**Fall 2.1.2.2:** $|KK^{-1} \cap \mathrm{Z}(G)| = p$.
In diesem Fall enthält $KK^{-1}$ genau $p$ Konjugationsklassen der Länge 1. Sei $t \in KK^{-1}$ mit $|\mathrm{C}_G(t)| = p^5$. Nach Satz 2.4 ist $\mathrm{C}_G(t)$ nichtabelsch. Wir können wieder annehmen, dass $t$ die Form $t = [x,g]$ mit $g \in G$ hat. Im Fall $g \notin M$ ist $G = M\langle g\rangle = G'\langle x,g\rangle = \Phi(G)\langle x,g\rangle = \langle x,g\rangle$. Wegen $t = [x,g] \in \mathrm{Z}(\mathrm{C}_G(t)) \trianglelefteq G$ wäre dann $G/\mathrm{Z}(\mathrm{C}_G(t))$ abelsch und $G' \subseteq \mathrm{Z}(\mathrm{C}_G(t))$. Dann wäre aber $\mathrm{C}_G(t)/\mathrm{Z}(\mathrm{C}_G(t))$ zyklisch und $\mathrm{C}_G(t)$ abelsch. Also ist $g \in M$ und $t \in H$. Offensichtlich enthält $H$ genau $p-1$ Konjugationsklassen der Länge $p$. Also enthält auch $KK^{-1}$ genau $p-1$ Konjugationsklassen der Länge $p$. Ist $L$ eine von diesen, so gilt $L \subseteq xK^{-1}$, und aus Lemma 2.10(ii) folgt $c_{KK^{-1}L} = |K|$.

Sei nun $L \subseteq KK^{-1}$ eine Konjugationsklasse der Länge $p^2$ und $t \in L$. Wie bisher können wir annehmen, dass $t$ die Form $t = [x,g]$ mit $g \in G$ hat. Offenbar gilt jetzt $g \notin M$ und $\mathrm{C}_G(t) = G'$. Wir definieren

$$B := \{h \in G' : [x,h] \in \mathrm{Z}(G)\}.$$

Wegen $1 \in B$ und $[x,hk] = [x,h]h[x,k]h^{-1} = [x,h][x,k] \in \mathrm{Z}(G)$ für $h,k \in B$ ist $B$ eine Untergruppe von $G'$. Es gilt $|B \cap \mathrm{C}_G(x)| = |G' \cap \mathrm{C}_G(x)| = p^2$ und $|B| = p^3$. Wir zeigen nun, dass $B$ sogar ein Normalteiler von $G$ ist. Sei dazu $y \in B$ und $z \in G$. Es gilt

$$\begin{aligned}[x,zyz^{-1}] &= [x,z]z[x,yz^{-1}]z^{-1} = [x,z][x,y]z[x,z^{-1}]z^{-1}\\ &= [x,z]z[x,z^{-1}]z^{-1}[x,y] = [x,y] \in \mathrm{Z}(G).\end{aligned}$$

Also ist $zyz^{-1} \in B$ und $B \trianglelefteq G$. Insbesondere ist $B\,\mathrm{C}_G(gxg^{-1})$ eine Untergruppe der Ordnung $p^4$ von $M$.
Annahme: $\mathrm{C}_G(x) \subseteq B\,\mathrm{C}_G(gxg^{-1})$.
Dann ist $B\,\mathrm{C}_G(gxg^{-1}) = B\,\mathrm{C}_G(x)$ und $g \in \mathrm{N}_G(B\,\mathrm{C}_G(x))$. Außerdem ist auch $M \subseteq \mathrm{N}_G(B\,\mathrm{C}_G(x))$, und es folgt $B\,\mathrm{C}_G(x) \trianglelefteq G$. Dann ist aber $G' = B\,\mathrm{C}_G(x)$, und wir erhalten den Widerspruch $x \in G'$.
Also ist $\mathrm{C}_G(x) \nsubseteq B\,\mathrm{C}_G(gxg^{-1})$ und $M = \mathrm{C}_G(x)B\,\mathrm{C}_G(gxg^{-1})$. Wir wählen $b \in B$ mit $B\,\mathrm{C}_G(gxg^{-1}) = \mathrm{C}_G(gxg^{-1})\langle b\rangle$ und $a \in \mathrm{C}_G(x)$ mit $M = B\,\mathrm{C}_G(gxg^{-1})\langle a\rangle$.

Offenbar besteht dann die Konjugationsklasse von $gxg^{-1}$ genau aus den Elementen $g^i a^j b^k (gxg^{-1}) b^{-k} a^{-j} g^{-i}$ mit $i, j, k \in \{0, \ldots, p-1\}$. Offenbar ist $t$ zu den $p$ Elementen der Form $[x, a^i g] = a^i [x, g] a^{-i} = a^i t a^{-i}$ mit $i \in \{0, \ldots, p-1\}$ konjugiert. Sei nun $t$ zu $[x, a^i b^j g]$ mit $i, j \in \{0, \ldots, p-1\}$ und $j \neq 0$ konjugiert. Ersetzt man $b$ durch $b^j$, so kann man $j = 1$ annehmen. Offenbar ist dann $t$ auch zu $[x, bg]$ konjugiert. Sei nun $y \in G$ mit

$$yty^{-1} = y[x, g]y^{-1} = [x, bg] = [x, b]b[x, g]b^{-1} = [x, b][x, g].$$

Wegen $[x, b] \in \mathrm{Z}(G)$ folgt dann

$$y^l t y^{-l} = [x, b]y^{l-1}[x, g]y^{1-l} = \ldots = [x, b]^l [x, g] = [x, b^l g]$$

für $l \in \{0, \ldots, p-1\}$. Also ist $t$ dann zu allen Elementen der Form $[x, a^i b^j g]$ mit $i, j \in \{0, \ldots, p-1\}$ konjugiert. Diese Elemente bilden dann die ganze Konjugationsklasse von $t$. Nehmen wir nun an, dass $t$ zu $[x, g^i a^j b^k g]$ mit $i, j, k \in \{0, \ldots, p-1\}$ und $i \neq 0$ konjugiert ist. Wegen $M \trianglelefteq G$ existiert ein $y \in M$ mit $g^i a^j b^k = y g^i$. Dann ist $t$ zu $[x, y g^{i+1}]$ konjugiert, und es existiert ein $z \in G$ mit

$$ztz^{-1} = z[x, g]z^{-1} = [x, yg^{i+1}] = [x, y]y[x, g^{i+1}]y^{-1}.$$

Wegen $[x, y] \in H$ ist also $z[x, g]z^{-1} \equiv y[x, g^{i+1}]y^{-1} \pmod{H}$. Mit den Bezeichnungen $\overline{G} := G/H$, $\overline{g} := gH$ und $\overline{x} := xH$ sind also $[\overline{x}, \overline{g}]$ und $[\overline{x}, \overline{g}^{i+1}]$ in $\overline{G}$ konjugiert. Nach Lemma 2.14 ist $[\overline{x}, \overline{g}] = [\overline{x}, \overline{g}^{i+1}]$ und damit $[x, g^i] \in H$. Wegen $i \neq 0$ ist dies ein Widerspruch. Folglich kann $t$ zu keinem Element der Form $[x, g^i a^j b^k g]$ mit $i, j, k \in \{0, \ldots, p-1\}$ und $i \neq 0$ konjugiert sein.

Insgesamt haben wir also gesehen, dass $t$ entweder zu $p$ oder zu $p^2$ Elementen der Form $[x, h]$ mit $h \in G$ konjugiert ist. Aus Lemma 2.10(iv) folgt $c_{KK^{-1}L} \geq |G' : \mathrm{C}_{G'}(x)| = p^2$. Im Fall $|L \cap xK^{-1}| = p^2 = |L|$ folgt $c_{KK^{-1}L} = |K|$ aus Lemma 2.10(ii). Sei also $|L \cap xK^{-1}| = p$ und $t = hxh^{-1}kx^{-1}k^{-1}$ mit $h, k \in G$. Dann existiert ein $i \in \{0, \ldots, p-1\}$ mit $h^{-1}th = xh^{-1}kx^{-1}k^{-1}h = a^i t a^{-i}$. Also ist $ha^i \in \mathrm{C}_G(t) = G'$, und es folgt $h \in M$. Wegen $|M : \mathrm{C}_G(x)| = p^2$ ist dann $c_{KK^{-1}L} \leq p^2$. Also ist $c_{KK^{-1}L} = p^2$, und die Behauptung ist in diesem Fall bewiesen.

**Fall 2.2:** $G'$ ist nichtabelsch.
Überraschenderweise ist dieser Fall einfacher als Fall 2.1. Trotzdem müssen wir unter anderem beachten, dass $KK^{-1}$ jetzt auch Konjugationsklassen der Länge $p^3$ enthalten kann. Wegen $KK^{-1} \subseteq G'$ und $|G'| = p^4$ kann die Länge einer Konjugationsklasse in $KK^{-1}$ allerdings nicht größer als $p^3$ sein.

Wir untersuchen nun die Struktur von $G'$. Nach Satz III.7.8(b) in [5] ist $\mathrm{Z}(G')$ nichtzyklisch. Es folgt, dass $\mathrm{Z}(G')$ und $G'/\mathrm{Z}(G')$ elementarabelsch sind, und dass $\mathrm{Z}(G')$ die Ordnung $p^2$ hat. Aus Hilfssatz III.7.10 in [5] folgt $|G''| = p$. Insbesondere ist $G'' \subseteq \mathrm{Z}(G)$.

Für eine Konjugationsklasse $L \subseteq KK^{-1} \cap \mathrm{Z}(G)$ ist $c_{KK^{-1}L} = |K|$ nach Lemma 2.10(iii). Wir zeigen nun, dass für jede Konjugationsklasse $L \subseteq KK^{-1}$ mit $|L| > 1$ stets $LL^{-1} \cap \mathrm{Z}(G) \neq 1$ gilt. Die Behauptung folgt dann mit Lemma 2.9 und Satz 2.5. Sei $t \in L$. Hat $L$ die Länge $p$, so ist $|\mathrm{C}_G(t)| = p^5$ und $G' \subseteq \mathrm{C}_G(t)$. Damit

folgt $t \in \mathrm{Z}(G')$ und $LL^{-1} = [G, \mathrm{Z}(G')]$ nach Lemma 2.7. Also ist $LL^{-1} \cap \mathrm{Z}(G) = [G, \mathrm{Z}(G')] \cap \mathrm{Z}(G) \neq 1$. Nehmen wir nun an, dass $L$ die Länge $p^2$ hat. Im Fall $G' = \mathrm{C}_G(t)$ wäre wieder $t \in \mathrm{Z}(G')$. Wegen $|\mathrm{Z}(G')| = p^2$ ist dies ausgeschlossen. Also ist $G' \neq \mathrm{C}_G(t)$ und $1 \neq \{[t, y] : y \in G'\} \subseteq LL^{-1} \cap G'' \subseteq LL^{-1} \cap \mathrm{Z}(G)$. Sei nun $|L| = p^3$. Dann ist $LL^{-1} = G^3$ und $LL^{-1} \cap \mathrm{Z}(G) = G^3 \cap \mathrm{Z}(G) \neq 1$ nach Lemma 2.7.

Damit ist der Beweis vollständig. □

In gewisser Hinsicht bildet Satz 2.6 eine Grenze für die Gültigkeit von (P3), denn wir haben mit Hilfe von GAP eine Gruppe $G$ der Ordnung $3^7$ gefunden, in der (P3) nicht mehr für alle Konjugationsklassen gültig ist. Genauer existieren Konjugationsklassen $K$ und $L$ in $G$ mit $|K| = 3^3$, $|L| = 3$ und $c_{KK^{-1}L} = 18 \not\equiv 1 \pmod 2$. Mit dem folgenden Quellcode kann man dies verifizieren.

```
G:=PcGroupCode(3216233062478022961865738644473 6,3^7);
CC:=ConjugacyClasses(G);
K:=CC[24];
L:=CC[6];
x:=Representative(L);
product:=function(x,y) return x*y^-1; end;
Size(Filtered(ListX(K,K,product),y->y=x)); # = c_{KK^{-1}L}
```

Selbst für $p = 2$ kann man im Allgemeinen nicht mehr davon ausgehen, dass die Klassenmultiplikationskonstanten der Form $c_{KK^{-1}L}$ mit Konjugationsklassen $K$ und $L$ einer endlichen $p$-Gruppe entweder 0 oder Potenzen von $p$ sind. Die Gruppe mit der Bezeichnung `SmallGroup(2^8,503)` der Ordnung $2^8$ aus der „Small Group Library“ liefert hierfür ein Beispiel.

## 2.4 Metazyklische $p$-Gruppen

In diesem Abschnitt werden wir zeigen, dass (P3) für jede Konjugationsklasse einer metazyklischen $p$-Gruppe erfüllt ist.

**Lemma 2.18.** *Sei $G$ eine metazyklische $p$-Gruppe für eine ungerade Primzahl $p$. Außerdem sei $A = \langle a \rangle \trianglelefteq G$ und $B = \langle b \rangle \leq G$ mit $G = AB$. Dann ist $G' = \{[a^i, b] : i \in \mathbb{Z}\} = \{[a, b^i] : i \in \mathbb{Z}\}$.*

*Beweis.* Da $G/A$ zyklisch ist, folgt $G' \subseteq A$. Wir betrachten nun $N := \{[a^i, b] : i \in \mathbb{Z}\} \subseteq G' \subseteq A$. Für $i \in \mathbb{Z}$ ist $[a^i, b] = a^i(a^{-1}[a, b])^i = [a, b]^i$, und es folgt $N = \langle [a, b] \rangle \leq G$. Da $N$ charakteristisch in $A$ ist, gilt auch $N \trianglelefteq G$. Offenbar ist $G/N$ abelsch, und es folgt $G' \subseteq N \subseteq G'$ und damit $N = G'$.

Für den zweiten Teil der Aussage betrachten wir $M := \{[a, b^i] : i \in \mathbb{Z}\}$. Offenbar ist dann $M \subseteq G' = N$. Sei nun $|M| = |B : \mathrm{C}_B(A)| = p^s$ mit $s \in \mathbb{N}_0$. Dann genügt es, $|N| \leq p^s$ zu zeigen. Sicherlich können wir $A \neq 1$ annehmen. Hat dann $A$ die

Ordnung $p^n$ mit $n \in \mathbb{N}$, so hat $\mathrm{Aut}(A)$ die Ordnung $p^{n-1}(p-1)$. Da $p$ ungerade ist, ist $\mathrm{Aut}(A)$ zyklisch, und die $p$-Sylowgruppe von $\mathrm{Aut}(A)$ wird von $\alpha$ mit $\alpha(a) = a^{1+p}$ erzeugt. Offenbar operiert $B$ auf $A$ durch Konjugation, und es existiert ein $m \in \mathbb{N}$ mit

$$bab^{-1} = a^{(1+p)^m}.$$

Durch eine geeignete Wahl von $b$ kann man $m = p^t$ mit $t \in \mathbb{N}_0$ annehmen. Aus $|B : \mathrm{C}_B(A)| = p^s$ folgt dann

$$a = b^{p^s} a b^{-p^s} = a^{(1+p)^{p^{s+t}}}.$$

Also ist $(1+p)^{p^{s+t}} \equiv 1 \pmod{p^n}$. Bekanntlich gilt dann $s + t \geq n - 1$. Außerdem ist $(1+p)^{p^t} \equiv 1 \pmod{p^{t+1}}$, und es existiert ein $k \in \mathbb{Z}$ mit $(1+p)^{p^t} = 1 + kp^{t+1}$. Dann ist

$$ba^{p^s}b^{-1} = a^{p^s(1+p)^{p^t}} = a^{p^s + kp^{s+t+1}} = a^{p^s},$$

und es folgt $|N| = |A : \mathrm{C}_A(B)| \leq p^s$. □

Die Diedergruppe der Ordnung 16 zeigt, dass die Aussage in Lemma 2.18 für $p = 2$ falsch wäre.

**Satz 2.7.** *Sei $G$ eine metazyklische $p$-Gruppe für eine ungerade Primzahl $p$ und $K, L \in \mathrm{Cl}(G)$. Dann ist $c_{KK^{-1}L} \in \{0, |K|\}$. Insbesondere sind* (P3)*,* (P2) *und* (P1) *erfüllt.*

*Beweis.* Wie in Lemma 2.18 wählen wir $A = \langle a \rangle \trianglelefteq G$ und $B = \langle b \rangle \leq G$ mit $G = AB$. Sei außerdem $x \in K$. Dann existieren $s, t \in \mathbb{Z}$ mit $x = b^s a^t$. Jedes Element in $K$ hat dann die Form

$$\begin{aligned} a^i b^j x b^{-j} a^{-i} &= x(a^{-t}b^{-s}a^i b^j b^s a^t b^{-j} a^{-i}) = x(a^{-t}(b^{-s}a^i b^s)(b^j a^t b^{-j})a^{-i}) \\ &= x(a^{-t}(b^j a^t b^{-j})(b^{-s}a^i b^s)a^{-i}) = x[a^{-t}, b^j][b^{-s}, a^i] \end{aligned}$$

mit $i, j \in \mathbb{Z}$. Also ist $K = x \cdot \{[a^{-t}, b^j] : j \in \mathbb{Z}\} \cdot \{[b^{-s}, a^i] = [a^{-i}, b^{-s}] : i \in \mathbb{Z}\}$. Da $\langle a^t \rangle B$ und $A\langle b^s \rangle$ auch metazyklische $p$-Gruppen sind, folgt

$$(\langle a^t \rangle B)' = \{[a^{-t}, b^j] : j \in \mathbb{Z}\} \text{ und } (A\langle b^s \rangle)' = \{[a^{-i}, b^{-s}] : i \in \mathbb{Z}\}$$

aus Lemma 2.18. Wegen $(\langle a^t \rangle B)' \leq A$ und $(A\langle b^s \rangle)' \leq A$ sind $(\langle a^t \rangle B)'$ und $(A\langle b^s \rangle)'$ Normalteiler von $G$. Insbesondere ist auch $(\langle a^t \rangle B)'(A\langle b^s \rangle)' =: N \trianglelefteq G$. Also ist $K = xN$ und damit $KK^{-1} = Nxx^{-1}N = N$. Schließlich erhalten wir $|K| = |N| = |KK^{-1}|$, und die Behauptung folgt aus Lemma 2.3. □

Auch hier zeigt die Diedergruppe der Ordnung 16, dass die Aussage in Satz 2.7 für $p = 2$ falsch wäre. Es sei außerdem angemerkt, dass nach Satz III.11.5 in [5] eine endliche $p$-Gruppe $G$ für $p > 2$ bereits dann metazyklisch ist, wenn $a, b \in G$ mit $G = \langle a \rangle \langle b \rangle$ existieren.

Zum Schluss dieses Kapitels möchten wir bemerken, dass wir bisher kein Gegenbeispiel für (P1) bzw. (P2) gefunden haben.

# 3 Problemstellung für Charaktere

## 3.1 Formulierung des Problems

Sei $G$ eine endliche $p$-Gruppe und $\chi$ ein irreduzibler Charakter von $G$. Wie in Abschnitt 1.3 bemerkt wurde, ist dann auch $\chi\overline{\chi}$ ein Charakter von $G$. Da $\chi$ irreduzibel ist, existiert ein $n \in \mathbb{N}_0$ mit $\chi(1) = p^n$. Adan-Bante hat in [1] gezeigt, dass dann

$$|\operatorname{Irr}(\chi\overline{\chi})| \geq 2n(p-1)+1$$

gilt. Sie hat auch gezeigt, dass diese Ungleichung optimal ist. Wir werden in diesem Kapitel das folgende Problem studieren.

**Problem 2.** *Sei $G$ eine endliche $p$-Gruppe und $\chi$ ein irreduzibler Charakter von $G$. Gilt dann stets*

$$|\operatorname{Irr}(\chi\overline{\chi})| \equiv 1 \pmod{p-1}? \tag{P4}$$

## 3.2 Resultate

Wir werden zeigen, dass (P4) für einige spezielle Klassen von endlichen $p$-Gruppen erfüllt ist. Dabei treten viele Ähnlichkeiten mit den Sätzen aus Abschnitt 2.2 auf. Im Fall $p = 2$ ist (P4) offenbar für alle endlichen $p$-Gruppen $G$ und alle irreduziblen Charaktere $\chi$ von $G$ erfüllt. Wir betrachten nun den Fall $p = 3$.

**Satz 3.1.** *Sei $G$ eine endliche $p$-Gruppe für eine ungerade Primzahl $p$ und $\chi \in \operatorname{Irr}(G)$. Dann ist $|\operatorname{Irr}(\chi\overline{\chi})|$ ungerade. Insbesondere ist* (P4) *im Fall $p = 3$ stets erfüllt.*

*Beweis.* Offenbar operiert die Gruppe $\langle -1 \rangle \leq \mathbb{C}$ durch ${}^{-1}K = K^{-1}$ für $K \in \operatorname{Cl}(G)$ und ${}^{-1}\chi = \overline{\chi}$ für $\chi \in \operatorname{Irr}(G)$ auf $\operatorname{Cl}(G)$ und $\operatorname{Irr}(G)$. Aus Lemma 2.1 und Satz 1.8 folgt dann, dass $1_G$ der einzige reellwertige irreduzible Charakter von $G$ ist. Wegen $(\chi\overline{\chi}|1_G)_G = (\chi|\chi)_G = 1$ ist $1_G \in \operatorname{Irr}(\chi\overline{\chi})$. Für $\psi \in \operatorname{Irr}(G)$ ist

$$(\chi\overline{\chi}|\psi)_G = \overline{(\chi\overline{\chi}|\psi)_G} = (\overline{\chi\overline{\chi}}|\overline{\psi})_G = (\chi\overline{\chi}|\overline{\psi})_G.$$

Also kann man die Elemente in $\operatorname{Irr}(\chi\overline{\chi}) \setminus \{1_G\}$ in Paare der Form $(\psi, \overline{\psi})$ einteilen, und die Behauptung folgt. □

Wir beschränken nun die Grade der irreduziblen Charaktere. Sei dafür $G$ eine endliche $p$-Gruppe und $\chi \in \mathrm{Irr}(G)$. Hat $\chi$ den Grad 1, so kann man $\chi$ offenbar auch als Gruppenhomomorphismus von $G$ nach $\mathbb{C}^\times$ auffassen. Insbesondere gilt daher $(\chi\overline{\chi})(g) = \chi(g)\overline{\chi}(g) = \chi(g)\chi(g^{-1}) = \chi(g)\chi(g)^{-1} = 1$ für alle $g \in G$, und wir erhalten $\chi\overline{\chi} = 1_G$. Also ist in diesem Fall (P4) erfüllt. Auch wenn $\chi$ den Grad $p$ hat, kann man die Gültigkeit von (P4) beweisen. Der folgende Satz, welcher ein Spezialfall von Theorem B in [1] ist, zeigt dies.

**Satz 3.2.** *Sei $G$ eine endliche $p$-Gruppe und $\chi \in \mathrm{Irr}(G)$ mit $\chi(1) = p$. Dann ist $|\mathrm{Irr}(\chi\overline{\chi})| \in \{2p-1, p^2\}$. Insbesondere ist* (P4) *erfüllt.*

*Beweis.* Siehe [1]. □

Ist nun $G$ eine endliche $p$-Gruppe mit $|G| \leq p^4$, so folgt $\chi(1) \leq p$ für alle $\chi \in \mathrm{Irr}(G)$ aus Gleichung $(\star)$. Also ist (P4) für jeden irreduziblen Charakter $\chi$ erfüllt. Eine weitere Folgerung aus Satz 3.2 ist das Analogon zu Satz 2.4.

**Satz 3.3.** *Sei $G$ eine endliche $p$-Gruppe und $\chi$ ein irreduzibler Charakter von $G$. Existiert dann ein abelscher Normalteiler $A$ von $G$ mit Index $p$, so ist* (P4) *erfüllt.*

*Beweis.* Nach Problem 2.9(b) in [6] ist $\chi(1) \leq |G : A| = p$. Also folgt die Behauptung aus Satz 3.2. □

Wir werden nun die Argumentation aus dem Beweis von Satz 3.1 verallgemeinern. Sei dazu $G$ eine endliche $p$-Gruppe der Ordnung $p^n > 1$. Wir wählen eine primitive $p^n$-te Einheitswurzel $\zeta \in \mathbb{C}$. Bekanntlich ist dann $\mathbb{Q}(\zeta)|\mathbb{Q}$ eine Galoiserweiterung mit Galoisgruppe $\mathcal{G} := \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$. Ist $p$ ungerade, so ist $\mathcal{G}$ zyklisch der Ordnung $p^{n-1}(p-1)$, und man kann ein Element $\sigma \in \mathcal{G}$ der Ordnung $p-1$ wählen. Es existiert dann ein $m \in \mathbb{Z}$ mit $\sigma(\zeta) = \zeta^m$ und $m^{p-1} \equiv 1 \pmod{p^n}$. In der Darstellungstheorie zeigt man, dass für jeden irreduziblen Charakter $\chi$ von $G$ stets $\chi(g) \in \mathbb{Q}(\zeta)$ für $g \in G$ gilt. Außerdem ist auch ${}^\sigma\chi$ mit

$$ {}^\sigma\chi(g) := \sigma(\chi(g)) = \chi(g^m) \text{ für } g \in G$$

ein irreduzibler Charakter von $G$. Auf diese Weise operiert $\langle\sigma\rangle$ auf $\mathrm{Irr}(G)$. Man überlegt sich leicht, dass $\langle\sigma\rangle$ auch auf $\mathrm{Cl}(G)$ durch

$$ {}^\sigma K := \{g^m : g \in K\} \text{ für } K \in \mathrm{Cl}(G)$$

operiert.

**Lemma 3.1.** *Mit den obigen Bezeichnungen gilt:*

*(i) Die Operation von $\langle\sigma\rangle$ auf $\mathrm{Cl}(G) \setminus \{\{1\}\}$ ist* fixpunktfrei, *d. h. $\{K \in \mathrm{Cl}(G) : {}^\tau K = K\} = \{\{1\}\}$ für alle $1 \neq \tau \in \langle\sigma\rangle$.*

*(ii) Die Operation von $\langle\sigma\rangle$ auf $\mathrm{Irr}(G) \setminus \{1_G\}$ ist fixpunktfrei.*

*Beweis.*

(i) Nehmen wir indirekt an, dass $1 \neq \tau \in \langle\sigma\rangle$ und $1 \neq K \in \mathrm{Cl}(G)$ mit ${}^{\tau}K = K$ existieren. Offenbar wird dann $K$ auch von jeder Potenz von $\tau$ fixiert, und wir können annehmen, dass $\tau$ die Ordnung $q$ für eine Primzahl $q \neq p$ hat. Sei $k \in \mathbb{Z}$ mit $\tau(\zeta) = \zeta^k$. Da $\langle\tau\rangle$ auch auf $K$ operiert, und $|K|$ eine Potenz von $p$ ist, liefert die Bahnengleichung ein $x \in K$ mit $x^k = x$. Insbesondere ist $k \equiv 1 \pmod{p}$, und es existiert ein $l \in \mathbb{Z}$ mit $k = 1 + pl$. Dann ist aber $k^{p^n} = (1+pl)^{p^n} \equiv 1 \pmod{p^n}$, und mit $k^q \equiv 1 \pmod{p^n}$ folgt $k \equiv 1 \pmod{p^n}$. Damit erhalten wir den Widerspruch $\tau = 1$.

(ii) Sei $a \in K \in \mathrm{Cl}(G)$ und $\chi \in \mathrm{Irr}(G)$. Dann ist $a^m \in {}^{\sigma}K$ und $\chi(a^m) = {}^{\sigma}\chi(a)$. Also sind die Voraussetzungen von Satz 1.8 erfüllt, und die Behauptung folgt. □

Aus Lemma 3.1 folgt $|\mathrm{Cl}(G)| = |\mathrm{Irr}(G)| \equiv 1 \pmod{p-1}$ für jede endliche $p$-Gruppe $G$. Außerdem kann man die Operation von $\langle\sigma\rangle$ auch auf $\{K \in \mathrm{Cl}(G) : K \subseteq N\}$ für $N \trianglelefteq G$ einschränken, und erhält so zum Beispiel

$$|\{K \in \mathrm{Cl}(G) : K \subseteq G'\}| \equiv 1 \pmod{p-1}.$$

Die 5-Sylowgruppen der Symmetrischen Gruppe vom Grad 25 zeigen allerdings, dass $\langle\sigma\rangle$ im Allgemeinen weder auf $\{L \in \mathrm{Cl}(G) : L \subseteq KK^{-1}\}$ für eine Konjugationsklasse $K$ von $G$ noch auf $\mathrm{Irr}(\chi\overline{\chi})$ für einen irreduziblen Charakter $\chi$ von $G$ operiert, sodass man auf diese Weise nicht direkt (P1) bzw. (P4) zeigen kann.

Wir werden nun sehen, dass die Situation für endliche $p$-Gruppen mit Nilpotenzklasse kleiner gleich 2 besser ist. Dazu betrachten wir die Operation von $\langle\sigma\rangle$ nun auf allen Charakteren von $G$.

**Lemma 3.2.** *Sei $G$ eine endliche $p$-Gruppe mit Nilpotenzklasse kleiner gleich 2 und $\chi \in \mathrm{Irr}(G)$. Mit den obigen Bezeichnungen gilt dann ${}^{\sigma}(\chi\overline{\chi}) = \chi\overline{\chi}$.*

*Beweis.* Sei $g \in G$. Aus Problem 3.12 in [6] folgt dann

$$\chi(g)\overline{\chi}(g) = \frac{\chi(1)}{|G|}\sum_{h\in G}\chi([g,h]).$$

Wegen $G' \subseteq \mathrm{Z}(G)$ ist $[g,h^m] = ([g,h]h)^m h^{-m} = [g,h]^m$ für alle $h \in G$. Außerdem ist die Abbildung $x \mapsto x^m$ für $x \in G$ offenbar eine Bijektion auf $G$. Also folgt

$$\begin{aligned}\sigma(\chi(g)\overline{\chi}(g)) &= \frac{\chi(1)}{|G|}\sum_{h\in G}\sigma(\chi([g,h])) = \frac{\chi(1)}{|G|}\sum_{h\in G}\chi([g,h]^m)\\ &= \frac{\chi(1)}{|G|}\sum_{h\in G}\chi([g,h^m]) = \frac{\chi(1)}{|G|}\sum_{k\in G}\chi([g,k]) = \chi(g)\overline{\chi}(g)\end{aligned}$$

und damit die Behauptung. □

**Satz 3.4.** *Sei $G$ eine endliche $p$-Gruppe mit Nilpotenzklasse kleiner gleich 2 und $\chi \in \mathrm{Irr}(G)$. Dann ist* (P4) *erfüllt.*

*Beweis.* Für $\psi \in \mathrm{Irr}(G)$ gilt

$$(\chi\overline{\chi}|^\sigma\psi)_G = ({}^\sigma(\chi\overline{\chi})|^\sigma\psi)_G = \sigma((\chi\overline{\chi}|\psi)_G) = (\chi\overline{\chi}|\psi)_G$$

nach Lemma 3.2. Also operiert $\langle\sigma\rangle$ auch auf $\mathrm{Irr}(\chi\overline{\chi})$. Wegen $(\chi\overline{\chi}|1_G)_G = (\chi|\chi)_G = 1$ ist $1_G \in \mathrm{Irr}(\chi\overline{\chi})$, und die Behauptung folgt aus Lemma 3.1. □

Man kann leicht zeigen, dass in der Situation von Satz 3.4 die Gruppe $\langle\sigma\rangle$ auch auf $\{L \in \mathrm{Cl}(G) : L \subseteq KK^{-1}\}$ für jede Konjugationsklasse $K$ von $G$ operiert. Wir zeigen nun, dass (P4) auch für Gruppen der Ordnung $p^5$ erfüllt ist.

**Lemma 3.3.** *Sei $G$ eine endliche $p$-Gruppe und $\chi$ ein irreduzibler Charakter von $G$. Gilt dann $\chi(1)^2 = |G : \mathrm{Z}(\chi)|$, so ist* (P4) *erfüllt. Insbesondere ist* (P4) *bereits dann erfüllt, wenn ein $n \in \mathbb{N}$ mit $|G| = p^{2n+1}$ und $\chi(1) = p^n$ existiert.*

*Beweis.* Aus Corollary 2.30 in [6] folgt, dass unter den angegebenen Voraussetzungen $\chi$ auf $G \setminus \mathrm{Z}(\chi)$ verschwindet. Nach Lemma 2.27(c) in [6] existiert außerdem ein Charakter $\psi \in \mathrm{Irr}(\mathrm{Z}(\chi))$ vom Grad 1 mit $\chi|_{\mathrm{Z}(\chi)} = \chi(1)\psi$. Also ist

$$(\chi\overline{\chi})(g) = \begin{cases} \chi(1)^2 & \text{für } g \in \mathrm{Z}(\chi) \\ 0 & \text{für } g \notin \mathrm{Z}(\chi) \end{cases}.$$

Daher ist $\chi\overline{\chi}$ gerade die Inflation des regulären Charakters $\rho_{G/\mathrm{Z}(\chi)}$ von $G/\mathrm{Z}(\chi)$. Bekanntlich ist jedes $\psi \in \mathrm{Irr}(G/\mathrm{Z}(\chi))$ ein irreduzibler Bestandteil von $\rho_{G/\mathrm{Z}(\chi)}$. Die Inflation eines $\psi \in \mathrm{Irr}(G/\mathrm{Z}(\chi))$ ist daher auch stets ein irreduzibler Bestandteil von $\chi\overline{\chi}$. Andererseits sind dies sicherlich die einzigen irreduziblen Bestandteile von $\chi\overline{\chi}$, und es folgt

$$|\mathrm{Irr}(\chi\overline{\chi})| = |\mathrm{Irr}(G/\mathrm{Z}(\chi))| \equiv 1 \pmod{p-1}$$

aus Lemma 3.1.

Für die zweite Behauptung wissen wir aus Corollary 2.30 in [6] bereits, dass $p^{2n} = \chi(1)^2 \leq |G : \mathrm{Z}(\chi)|$ gilt. Im Fall $\mathrm{Z}(\chi) = 1$ wäre $1 = \mathrm{Z}(\chi)/\ker(\chi) = \mathrm{Z}(G/\ker(\chi)) \cong \mathrm{Z}(G)$. Also ist $|\mathrm{Z}(\chi)| = p$ und $\chi(1)^2 = |G : \mathrm{Z}(\chi)|$. □

**Satz 3.5.** *Sei $G$ eine endliche $p$-Gruppe mit $|G| \leq p^5$ und $\chi$ ein irreduzibler Charakter von $G$. Dann ist* (P4) *erfüllt.*

*Beweis.* Nach Satz 3.2 können wir $\chi(1) = p^2$ und $|G| = p^5$ annehmen. Dann sind aber die Voraussetzungen von Lemma 3.3 für $n = 2$ erfüllt, und die Behauptung folgt. □

Aus Lemma 3.3 kann man noch eine weitere Folgerung ableiten.

**Satz 3.6.** *Sei $G$ eine endliche $p$-Gruppe und $\chi$ ein irreduzibler Charakter von $G$ mit $G' \subseteq \mathrm{Z}(\chi)$. Dann ist* (P4) *erfüllt.*

*Beweis.* Die Aussage folgt unmittelbar aus Theorem 2.31 in [6] und Lemma 3.3. □

Wegen $\mathrm{Z}(G)\,\mathrm{Ker}(\chi)/\,\mathrm{Ker}(\chi) \subseteq \mathrm{Z}(G/\,\mathrm{Ker}(\chi)) = \mathrm{Z}(\chi)/\,\mathrm{Ker}(\chi)$ gilt $\mathrm{Z}(G) \subseteq \mathrm{Z}(\chi)$ für alle endlichen Gruppen $G$ und alle irreduziblen Charaktere $\chi$ von $G$. Daher ist Satz 3.6 eine Verallgemeinerung von Satz 3.4.

Mit GAP haben wir gezeigt, dass (P4) auch für alle Gruppen der Ordnung $5^6$ erfüllt ist. Wie bei (P1) und (P2) möchten wir auch hier anmerken, dass bisher kein Gegenbeispiel für (P4) bekannt ist.

# Literaturverzeichnis


[1] E. Adan-Bante, *Products of characters and finite p-groups. II*, Arch. Math. (Basel) **82** (2004), 289–297.

[2] E. Adan-Bante, *Conjugacy classes and finite p-groups*, Arch. Math. (Basel) **85** (2005), 297–303.

[3] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.10*; 2007, (`http://www.gap-system.org`).

[4] L. Héthelyi und B. Külshammer, *Classes and characters of finite p-groups*, unveröffentlicht.

[5] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967.

[6] I. M. Isaacs, *Character theory of finite groups*, AMS Chelsea Publishing, Providence, RI, 2006.

[7] J. Schmidt, persönliche Mitteilung.

# Selbstständigkeitserklärung

Ich erkläre, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Jena, den 19. November 2008