# Einige verallgemeinerte Charaktere von Thompson

Diplomarbeit

von

Thorsten Rey

zur Erlangung des akademischen Grades eines
Diplom-Mathematikers

angefertigt bei
Universitätsprofessor Dr. Gerhard Hiß

Fakultät für Mathematik, Informatik und Naturwissenschaften
Rheinisch-Westfälische Technische Hochschule Aachen

# Inhaltsverzeichnis

# Symbolverzeichnis

| | |
|---|---|
| $G$ | eine endliche Gruppe |
| $\mathbb{N}$ | die Menge der natürlichen Zahlen mit Null |
| $\mathbb{P}$ | die Menge Primzahlen in den natürlichen Zahlen |
| $x^y$ | Konjugation eines Elementes $x$ mit einem Element $y$; in dieser Arbeit stets als $x^y = y^{-1}xy$ definiert |
| $Z(G)$ | das Zentrum von $G$ |
| $N_G(U)$ | der Normalisator einer Untergruppe $U$ von $G$ |
| $C_G(U)$ | der Zentralisator einer Untergruppe $U$ von $G$ |
| $(\chi, \psi)_G$ | Skalarprodukt in $G$ zweier Klassenfunktionen $\chi$ und $\psi$ von $G$ |
| $\mathbb{1}_G$ | der Eins-Charakter von $G$ |
| $\chi \boxtimes \psi$ | das Produkt zweier Charaktere $\chi$ einer Gruppe $U$ und $\psi$ einer Gruppe $V$, aufgefasst als Charakter des direkten Produktes $U \times V$ |
| $D_n$ | die Diedergruppe von Ordnung $n$ |
| $S_n$ | die symmetrische Gruppe auf $n$ Punkten |
| $\mathbb{F}_p$ | der endliche Körper mit $p$ Elementen |

# Einleitung

Diese Arbeit beschäftigt sich mit Klassenfunktionen einer endlichen Gruppe $G$, die von John G. Thompson in [Tho96] vorgestellt wurden. Ebendort beweist er, dass es sich darüberhinaus um verallgemeinerte Charaktere, also $\mathbb{Z}$-Linearkombinationen von irreduziblen Charakteren von $G$, handelt. Thompson vermutet überdies, dass die vorgestellten Klassenfunktionen sogar Charaktere der Gruppe sind. Diese Vermutung trifft nicht zu, wie wir im Laufe dieser Arbeit sehen werden.
Dennoch besteht die Hauptfragestellung dieser Arbeit darin, Kriterien dafür zu finden, unter welchen Voraussetzungen doch Charaktere vorliegen. Für die Klassenfunktion $\chi_p$ können wir Nilpotenz als hinreichende Bedingung anführen (2.15). Dagegen deutet sich für die Funktion $\chi_{\text{solv}}$ eine Charakterisierung an (3.3).

### Inhalt

In Kapitel 1 stellen wir eine Klasse von verallgemeinerten Charakteren vor, die auch Thompsons Klassenfunktionen abdeckt. Betrachtet werden dabei Klassen von Untergruppen, die zwei Bedingungen genügen, insbesondere der Abgeschlossenheit unter Konjugation. Die Idee dieses allgemeineren Konzepts geht auf Stephen Gagola Jr. und Mark L. Lewis zurück, die ihre Ergebnisse jedoch nicht veröffentlicht haben. Dieser allgemeinere Zugang wird im ersten Abschnitt mit Hilfe der Techniken, die Thompson in [Tho96] für seine Klassenfunktionen benutzt, vorgestellt. Anschließend werden im zweiten Abschnitt Thompsons Klassenfunktionen in das allgemeine Konzept eingebettet.

In Kapitel 2 beleuchten wir für die Klassenfunktion $\chi_p$ die Frage, wann diese sogar ein Charakter ist. Wir werden relativ schnell sehen, dass der weniger interessante Fall $\chi_p = |G| \cdot \mathbb{1}_G$ leicht charakterisierbar ist.
Weiter werden wir feststellen, dass bei $p$-Gruppen der verallgemeinerte Charakter $\chi_p$ bereits mit dem Permutationscharakter der Gruppe bei Konjugation auf sich selbst übereinstimmt. Dennoch können wir dies benutzen, um die Situation bei $p$-nilpotenten und nilpotenten Gruppen vollständig - und mit positivem

Ergebnis - abzuhandeln. Dabei nutzen wir Resultate, die bei geeigneten Normalteilern der Gruppe die Funktionswerte von $\chi_p$, definiert auf dem Normalteiler, und der Werte bei Definition auf der zugehörigen Faktorgruppe in Beziehung bringen.
Bereits zu Beginn des Kapitels geben wir mit der symmetrischen Gruppe $S_4$ ein Beispiel für eine Gruppe, für die $\chi_p$ nicht für alle Primzahlen ein Charakter ist. Wegen der Auflösbarkeit von $S_4$ zeigt dies, dass sich das Ergebnis über die nilpotenten Gruppen nicht noch auf die auflösbaren Gruppen ausweiten lässt.
Mit Gegenbeispielen - also Gruppen, für die eine Primzahl $p$ existiert, so dass $\chi_p$ kein Charakter ist - beschäftigen sich die letzten beiden Abschnitte des zweiten Kapitels. Dabei geben wir eine generische Serie von Gegenbeispielen für jede ungerade Primzahl $p$ an. Dies wurde motiviert durch ein Gegenbeispiel in [Mor04] von Alexander Moreto für $p = 3$ und einen Vorschlag von Roderick Gow, dass sich dieses Gegenbeispiel für beliebige ungerade Primzahlen verallgemeinern lässt.
Abschließend wenden wir uns den symmetrischen Gruppen zu, da sich in diesen durch GAP-Rechnungen - siehe Anhang B - eine Serie von Gegenbeispielen andeutet. Die große Schwierigkeit dieser Gruppen liegt in den nicht allgemein berechenbaren Funktionswerten von $\chi_p$ für diese Gruppen. Dennoch können wir für einen Spezialfall eine Aussage machen.

In Kapitel 3 steht die Klassenfunktion $\chi_{\text{solv}}$ im Mittelpunkt. Ähnlich zum vorigen Kapitel können wir auch hier den Fall $\chi_{\text{solv}} = |G| \cdot \mathbb{1}_G$ leicht abhandeln. Zentral ist in diesem Kapitel aber die Vermutung, dass $\chi_{\text{solv}}$ genau für die auflösbaren Gruppen ein Charakter ist. Um sich dem Beweis dieser Vermutung zu nähern, werden analog zum Kapitel 2 Aussagen über Normalteiler und Faktorgruppen gemacht, die in der Beschreibeung eines minimalen Gegenbeispiels zur Vermutung Verwendung finden.
Untermauert wird die Vermutung von einer Serie nicht-auflösbarer Gruppen, für die $\chi_{\text{solv}}$ kein Charakter ist. Diese Serie - die Gruppen $\mathrm{PSL}(2, p)$ für geeignete Primzahlen $p$ - wird im letzten Abschnitt des Kapitels umfassend behandelt. Dabei stützen wir uns auf eine Arbeit von John Thompson, die die spezielle, für unsere Belange sehr günstige Struktur dieser Gruppen garantiert [Tho68]. Entscheidend ist in der dortigen Situation die Frage, wann ein Untergruppenerzeugnis $\langle x, y \rangle$ in $\mathrm{PSL}(2, p)$ echt ist, denn dann ist es bereits auflösbar. Wir werden jeweils in Abhängigkeit von der Ordnung eines festen $x$ die Anzahl der

$y$ bestimmen, so dass $\langle x, y \rangle$ eine echte Untergruppe erzeugt. Die Klassifikation der maximalen Untergruppen von $\mathrm{PSL}(2, p)$ wird dabei sehr hilfreich sein.

**Danksagung**

Bedanken möchte ich mich zu allererst bei Herrn Prof. Dr. Hiß. Ihm vedanke ich das interessante Thema dieser Arbeit. Stets nahm er sich die Zeit, über Probleme zu diskutieren und zeigte mir durch Anregungen und Kritik neue Wege auf. Seine ausgezeichnete Betreuung trug wesentlich zum Gelingen dieser Arbeit bei. Weiter danke ich Dr. Frank Lübeck, an den ich mich ebenfalls jederzeit mit Fragen wenden konnte. Insbesondere seine Erklärungen zur projektiven speziellen linearen Gruppe und dem CHEVIE-Paket haben mir entscheidend weitergeholfen. Für das eine oder andere helfende Gespräch über Inhaltliches und LaTeX-Fragen sei auch Michael Bodewig gedankt. Ich danke meinen Eltern, die mir dieses Studium überhaupt ermöglicht und mich stets unterstützt haben. Zu guter Letzt, aber vor allem danke ich Julia. An Glaube in mich hat es dir nie gemangelt. Damit war alles ganz leicht.

# Kapitel 1

# Thompsons Ergebnis und eine Verallgemeinerung

Es sei $G$ eine endliche Gruppe. In diesem Kapitel stellen wir Thompsons Ergebnis vor, was Ausgangspunkt und Motivation dieser Arbeit ist. Stephen Gagola Jr. und Mark L. Lewis haben sich bereits vor der vorliegenden Arbeit mit den Klassenfunktionen von Thompson beschäftigt und dabei ein allgemeineres Konzept entwickelt, dieses aber nach Wissen des Autors nicht publiziert. Im ersten Abschnitt wird diese Idee, bei der Verbände von Untergruppen betrachtet werden, die gewissen (schwachen) Bedingungen genügen, vorgestellt. Danach werden im zweiten Abschnitt Thompsons Klassenfunktionen in das allgemeinere Konzept von Gagola und Lewis eingebettet.

## 1.1 Eine Klasse von verallgemeinerten Charakteren

**(1.1) Definition**
Es sei $\wp$ ein Verband von Untergruppen von $G$, für den folgende Eigenschaften gelten:

(1) Der Verband $\wp$ sei unter Konjugation abgeschlossen, d.h aus $H \in \wp$ folge stets $H^g \in \wp$ für alle $g \in G$.

(2) Es sei $U \leq G$ und $g, h \in N_G(U)$ mit $gh^{-1} \in C_G(U)$.
Dann gilt:
$$\langle U, g\rangle \in \wp \;\Leftrightarrow\; \langle U, h\rangle \in \wp.$$

Nun definieren wir das zentrale Untersuchungsobjekt.

**(1.2) Definition**
Wir definieren für $g \in G$ die Menge

$$P(g) := \{h \in G \mid \langle g, h \rangle \in \wp\}$$

und darauf aufbauend die Funktion

$$\vartheta_\wp : \; G \to \mathbb{Z}, \; g \mapsto |P(g)|.$$

**(1.3) Bemerkung**
$\vartheta_\wp$ ist eine Klassenfunktion auf $G$.

**Beweis**
Es sei $g \in G$. Dann gilt

$$\begin{aligned} P(u^{-1}gu) &= \left\{h \in G \mid \langle u^{-1}gu, h \rangle \in \wp\right\} \\ &= \left\{h \in G \;\middle|\; u^{-1}\langle g, uhu^{-1} \rangle u \in \wp\right\} \\ &= \left\{h \in G \;\middle|\; \langle g, uhu^{-1} \rangle \in \wp\right\} \\ &= u^{-1}P(g)u \end{aligned}$$

für alle $u \in G$, wobei im vorletzten Schritt Eigenschaft (1) aus (1.1) angewandt wurde. Also ist

$$\vartheta_\wp(u^{-1}gu) = \left|P(u^{-1}gu)\right| = \left|u^{-1}P(g)u\right| = |P(g)| = \vartheta_\wp(g),$$

für alle $u \in G$. □

Wir werden im Folgenden zeigen, dass $\vartheta_\wp$ sogar ein verallgemeinerter Charakter von $G$ ist. Dazu benutzen wir Thompsons Beweisideen aus [Tho96], der dies dort für konkrete Varianten von $\vartheta_\wp$ gezeigt hat. Der folgende Satz deutet an, wie unsere Beweisstrategie aussieht.

**(1.4) Satz**
Für alle $\psi \in \mathrm{Irr}(G)$ ist $(\vartheta_\wp, \psi)_G$ eine rationale Zahl.

**Beweis**
Es sei $\psi \in \mathrm{Irr}(G)$ beliebig, $\epsilon$ eine $|G|$-te Einheitswurzel und $K$ der Körper aus Anhang (C.2), sowie $\mathfrak{X}$ eine $K$-Darstellung von $\psi$ vom Grad $n$. Wähle $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ beliebig und $g \in G$. Es ist $\sigma(\epsilon) = \epsilon^k$ für ein $k \in \mathbb{N}$ mit $\mathrm{ggT}(k, |G|) = 1$. Nach (C.1) im Anhang ist $\mathfrak{X}(g)$ ähnlich zu einer Diagonalmatrix aus Einheitswurzeln. Es existieren also $m_1, \ldots, m_n \in \mathbb{N}$ so dass

$$\mathfrak{X}(g) \text{ ähnlich zu } \begin{pmatrix} \epsilon^{m_1} & & \\ & \ddots & \\ & & \epsilon^{m_n} \end{pmatrix}$$

ist, woraus dann

$$\mathfrak{X}(g^k) = \mathfrak{X}(g)^k \text{ ähnlich zu } \begin{pmatrix} \epsilon^{km_1} & & \\ & \ddots & \\ & & \epsilon^{km_n} \end{pmatrix}$$

folgt. Somit ist

$$\sigma\left(\psi(g)\right) = \sum_{i=1}^{n} \sigma\left(\epsilon^{m_i}\right) = \sum_{i=1}^{n} \epsilon^{km_i} = \psi\left(g^k\right).$$

Wegen $\mathrm{ggT}\,(k, |G|) = 1$ gilt $\langle g^k \rangle = \langle g \rangle$. Außerdem sieht man leicht an der Definition von $\vartheta_\wp$, dass $\vartheta_\wp(g) = \vartheta_\wp(g')$ für alle $g, g' \in G$ mit $\langle g \rangle = \langle g' \rangle$ gilt. Da $\vartheta_\wp$ nur ganzzahlige Werte annimt, ist $\vartheta_\wp$ invariant unter $\sigma$. Also ist

$$\begin{aligned}
\sigma\left((\vartheta_\wp, \psi)_G\right) &= \frac{1}{|G|} \sum_{g\in G} \vartheta_\wp(g) \cdot \sigma\left(\overline{\psi(g)}\right) = \frac{1}{|G|} \sum_{g\in G} \vartheta_\wp(g) \cdot \sigma\left(\psi(g^{-1})\right) \\
&= \frac{1}{|G|} \sum_{g\in G} \vartheta_\wp(g) \cdot \psi(g^{-k}) \quad = \frac{1}{|G|} \sum_{g\in G} \vartheta_\wp(g^k) \cdot \psi(g^{-k}) \\
&= \frac{1}{|G|} \sum_{g\in G} \vartheta_\wp(g^k) \cdot \overline{\psi(g^k)} \quad = (\vartheta_\wp, \psi)_G\,,
\end{aligned}$$

da $g^k$ wegen $\mathrm{ggT}\,(k, |G|) = 1$ die ganze Gruppe durchläuft. Das heißt, $(\vartheta_\wp, \psi)_G$ ist invariant unter allen Galois-Automorphismen und liegt somit im Fixkörper $\mathbb{Q}$. $\square$

Um nun zu beweisen, dass $\vartheta_\wp$ ein verallgemeinerter Charakter ist, genügt es also zu zeigen, dass das Skalarprodukt mit einem irreduziblen Charakter von $G$ eine ganz-algebraische Zahl ist. Denn dann läge das Skalarprodukt nach dem vorangegangenen Satz sogar in $\mathbb{Z}$. Als Zwischenschritt arbeiten wir im Folgenden darauf hin, dass für jedes $g \in G$ der Funktionswert $\vartheta_\wp(g)$ durch die Zentralisatorordnung $|C_G(g)|$ teilbar ist. Mit diesem Wissen lässt sich dann leicht zeigen, dass die relevanten Skalarprodukte ganz-algebraisch sind. Um diese Teilbarkeitseigenschaft zu zeigen, betrachten wir die im Folgenden definierten Mengen, die, wie wir sehen werden, Partitionen von $G$ und von $P(g)$ liefern.

**(1.5) Definition**

Für eine Untergruppe $C \leq G$ und $x \in G$ setzen wir

$$D(x) := D(x,\ C,\ G) := \bigcap_{n \in \mathbb{Z}} C^{x^n},$$

$$E(x) := E(x,\ C,\ G) := \left\{ h \in G \;\middle|\; \exists\, u \in C,\ d \in D(x) : h = u^{-1}xdu \in D(x) \right\}.$$

**(1.6) Lemma**

Es gilt $|E(x)| = |C|$ für alle $x \in G,\ C \leq G$.

**Beweis**

Aufgrund der endlichen Ordnung von $x$ ist $D(x)$ als endlicher Schnitt von Untegruppen eine Untergruppe von $G$. Insbesondere gilt $D(x) \leq C$. Es sei $e = [C : D(x)]$ und wir wählen eine Transversale $c_1, \ldots, c_e$ für $D(x)\backslash C$ mit $c_1 = 1$. Für $u \in C$ ist dann $u = vc_i$ mit $v \in D(x)$ und einem $1 \leq i \leq e$. Also gilt

$$u^{-1}xD(x)u = c_i^{-1}v^{-1}xD(c)vc_i. \tag{$*$}$$

Wegen $x \in N_G(D(x))$ und $v \in D(x)$ gilt nun

$$v^{-1}xD(x)v = v^{-1}xD(x) = v^{-1}D(x)x = D(x)x = xD(x),$$

so dass zusammen mit der Gleichung $(*)$

$$u^{-1}xD(x)u = c_i^{-1}xD(x)c_i \tag{$**$}$$

folgt.

Als zweiten Schritt zeigen wir

$$c_i^{-1}xD(x)c_i \ \cap \ c_j^{-1}xD(x)c_j = \emptyset$$

für alle $1 \leq i \neq j \leq e$.
Wir nehmen das Gegenteil an: Es sei für ein Paar $(i, j)$, $i \neq j$, der obige Schnitt nicht-leer. Es ist $u := c_i c_j^{-1} = vc_k$ für ein $v \in D(x)$ und ein $1 \leq k \leq e$. Da $i \neq j$ und $c_1, \cdots, c_e$ eine Transversale ist, kann nicht $c_k = 1 = c_1$ gelten, also folgt $2 \leq k \leq e$. Weiter gilt:

$$\begin{aligned} c_j \left( c_i^{-1}xD(x)c_i \ \cap \ c_j^{-1}xD(x)c_j \right) c_j^{-1} &= c_j c_i^{-1}xD(x)c_i c_j^{-1} \ \cap \ xD(x) \\ &= u^{-1}xD(x)u \ \cap \ xD(x) \\ &\underset{(**)}{=} c_k^{-1}xD(x)c_k \ \cap \ xD(x). \end{aligned}$$

Daher existieren $d_1, \ d_2 \in D(x)$ mit $c_k^{-1}xd_1c_k = xd_2$. Diese Gleichung lässt sich äquivalent umschreiben zu $x^{-1}c_kx = d_1c_kd_2^{-1}$. Da $D(x)$ von $x$ normalisiert wird, gilt nun sogar $x \in N_G(\langle D(x), \ c_k \rangle)$. Dann ist aber

$$\langle D(x), \ c_k \rangle \ \subseteq \ \bigcap_{n \in \mathbb{Z}} C^{x^n} = D(x),$$

was insbesondere $c_k \in D(x)$ bedeutet. Es folgt $k = 1$, was aber ein Widerspruch ist.

Also sind die obigen Schnitte alle disjunkt, so dass sich nun mit

$$|c_i^{-1}xD(x)c_i| = |D(x)|$$

für alle $1 \leq i \leq e$ die Gleichung

$$|E(x)| = \sum_{i=1}^{e} \left| c_i^{-1}xD(x)c_i \right| = e \cdot |D(x)| = |C|$$

ergibt. □

**(1.7) Lemma**
Es gilt $E(x) = E(x_0)$ für alle $x_0 \in E(x)$.

**Beweis**
Es sei $x_0 \in E(x)$ und $u \in C,\ d \in D(x)$ mit $x_0 = u^{-1}xdu$.

**1. Fall:** $d = 1$, d.h. $x_0 = u^{-1}xu$
Dann gilt

$$D(x_0) = \bigcap_{n\in\mathbb{Z}} C^{x_0^n} = \bigcap_{n\in\mathbb{Z}} C^{u^{-1}x^n u} \underset{u\in C}{=} \bigcap_{n\in\mathbb{Z}} C^{x^n u} = \left(\bigcap_{n\in\mathbb{Z}} C^{x^n}\right)^u = D(x)^u,$$

also

$$\begin{aligned} E(x_0) = \bigcup_{v\in C} v^{-1}x_0 D(x_0)v \qquad &= \bigcup_{v\in C} v^{-1}u^{-1}xuu^{-1}D(x)uv \\ = \bigcup_{v\in C} (uv)^{-1}xD(x)(uv) = &\ E(x). \end{aligned}$$

**2. Fall:** $u = 1$, d.h. $x_0 = xd$
Für beliebiges $n \in \mathbb{N} \setminus \{0\}$ setzen wir

$$d_n := \left(x^{-(n-1)}dx^{n-1}\right)\left(x^{-(n-2)}dx^{n-2}\right)\ldots\left(x^{-1}dx\right)d, \quad d_0 := 1.$$

Wegen $d \in D(x)$ und $x \in N_G(D(x))$ ist $d_n \in D(x)$. Damit liegt

$$x_0^n = (xd)^n = x^n d_n$$

in $N_G(D(x))$. Daraus ergibt sich:

$$D(x_0) = \bigcap_{n\in\mathbb{Z}} C^{x_0^n} = \bigcap_{n\in\mathbb{Z}} C^{x^n d_n} = D(x)^{d_n} = D(x).$$

Wir können also

$$x_0 D(x_0) = xdD(x) = xD(x)$$

schreiben, woraus nach Definition direkt

$$E(x) = E(x_0)$$

folgt.

**3. Fall:** $u \neq 1,\ d \neq 1$
Lassen wir im 1. Fall $xd$ die Rolle von $x$ einnehmen, folgt dort

$$D(x_0) = D(xd)^u$$

sowie

$$E(x_0) = E(xd).$$

Andererseits liefert der 2. Fall $D(x) = D(xd)$, so dass über

$$xdD(xd) = xdD(x) = xD(x)$$

nun

$$E(xd) = E(x)$$

folgt. Insgesamt haben wir also das gewünschte $E(x) = E(x_0)$. □

Das Lemma zeigt, dass die Mengen $E(x)$ die Gruppe $G$ partitionieren, d.h. es existieren $x_1, \ldots, x_m \in G$, so dass

$$G = E(x_1) \dot{\cup} \ \ldots \ \dot{\cup}\ E(x_m).$$

Bisher war die Untergruppe $C \leq G$ allgemein gewählt. Ab jetzt sei $C = C_G(g)$ für ein beliebiges, aber festes $g \in G$. Nun können wir sogar zeigen, dass sogar $P(g)$ durch geeignete Mengen $E(x)$ partitioniert werden kann.

**(1.8) Lemma**
Es sei $i \in \{1, \ldots, m\}$ mit $P(g) \cap E(x_i) \neq \emptyset$. Dann gilt

$$E(x_i) \subseteq P(g).$$

**Beweis**
Es sei $i \in \{1, \ldots, m\}$ mit $P(g) \cap E(x_i) \neq \emptyset$. Zur einfacheren Notation setzen wir $x = x_i$ und wir wählen ein $x' \in P(g) \cap E(x)$. Nach (1.7) ist $E(x) = E(x')$, also können wir ohne Einschränkung annehmen, dass $x \in P(g) \cap E(x)$. Somit gilt $\langle g, x \rangle \in \wp$. Wir setzen weiter

$$U = \langle g^{x^n} \mid n \in \mathbb{Z} \rangle.$$

Dass $U$ von $x$ normalisiert wird, ist offensichtlich. Außerdem gilt für $n \in \mathbb{N}$:

$$\begin{aligned}\left(g^{x^n}\right)^g &= g^{-1}x^{-n}gx^ng = x^{-n}\left(x^ng^{-1}x^{-n}\right)gx^ng\\ &= x^{-n}\left(g^{-1}\right)^{x^{-n}}gx^ng = x^{-n}\left(g^{x^{-n}}\right)^{-1}gx^ng\\ &= x^{-n}\left(\left(g^{x^{-n}}\right)^{-1}g\right)x^ng.\end{aligned}$$

Da $x \in N_G(U)$ und sowohl $g$ als auch $\left(g^{x^{-n}}\right)^{-1}g$ in $U$ liegen, gilt nach obiger Rechnung also auch $\left(g^{x^n}\right)^g \in U$. Wir haben damit also

$$U \trianglelefteq \langle g, x\rangle$$

gezeigt und erhalten außerdem die Identität

$$\langle g, x\rangle = U\langle x\rangle = \langle U, x\rangle.$$

Nach Definition ist $D(x) = \bigcap_{n\in\mathbb{Z}} C^{x^n} \leq C$, also gilt $[D(x), g] = 1$ aufgrund der speziellen Wahl von $C$. Mit $D(x) = D(x)^{x^n}$ folgt dann sofort $[D(x), g^{x^n}] = 1$ für alle $n \in \mathbb{Z}$. Wir haben also $[D(x), U] = 1$. Ist $d \in D(x)$ und setzen wir $x_0 = xd$, so erhalten wir

$$U = \langle g^{x_0^n} \mid n \in \mathbb{Z}\rangle.$$

Das bedeutet wie oben $\langle g, x_0\rangle = U\langle x_0\rangle,\ U \trianglelefteq \langle g, x_0\rangle$.

Es sei nun $u \in U$ beliebig. Aus $x^{-1}ux \in U$, $d \in D(x)$ und $[D(x), g^{x^n}] = 1$ folgt offensichtlich

$$d^{-1}x^{-1}uxd = x^{-1}ux,$$

was sich auch als

$$x_0^{-1}ux_0 = x^{-1}ux$$

schreiben lässt. Dies lässt sich aber leicht zur Aussage $xx_0^{-1} \in C_G(U)$ umformen. Außerdem gilt offensichtlich $x,\ x_0 \in N_G(U)$. Wegen

$$\begin{aligned}\langle g, x\rangle\ &= U\langle x\rangle\ = \langle U, x\rangle,\\ \langle g, x_0\rangle &= U\langle x_0\rangle = \langle U, x_0\rangle\end{aligned}$$

folgt nun mit der Eigenschaft (2) von $\wp$, dass $\langle g, x_0\rangle \in \wp$. Es sei $u \in C$. Dann gilt:

$$\langle g, u^{-1}x_0u\rangle = \langle u^{-1}gu, u^{-1}x_0u\rangle = \langle g, x_0\rangle^u.$$

Wir haben damit gezeigt:

$$\langle g, u^{-1}xdu\rangle \in \wp.$$

Da $d \in D(x),\ u \in C$ beliebig waren, folgt $E(x) \subseteq P(g)$. □

Damit haben wir nun alle Hilfsmittel, um zu zeigen, dass $\vartheta_\wp$ ein verallgemeinerter Charakter von $G$ ist.

**(1.9) Definition**
Für $g \in G$ setzen wir

$$c(g) := |C_G(g)| \quad \text{und} \quad m_\wp(g) := \frac{\vartheta_\wp(g)}{c(g)}.$$

**(1.10) Satz**
$\vartheta_\wp$ ist ein verallgemeinerter Charakter von $G$.

**Beweis**
Nach (1.7) partitionieren die Mengen $E(x)$ die Gruppe $G$. Also existieren $x_1, \ldots, x_m \in G$, so dass $G$ die disjunkte Vereinigung der $E(x_i)$ ist. Nach (1.6) ist $|E(x_i)| = |C| = |C_G(g)|$ für alle $1 \leq i \leq m$, also ist $m = [G : C]$.
Außerdem gilt nach (1.8):

$$|P(g)| = t \cdot |E(x_i)| \quad \text{für ein} \ \ t \in \mathbb{N}.$$

Damit haben wir nun:

$$m_\wp(g) = \frac{\vartheta_\wp(g)}{c(g)} = \frac{|P(g)|}{|C_G(g)|} = \frac{t \cdot |E(x_1)|}{|E(x_1)|} = t \in \mathbb{Z}.$$

Die Koeffizienten $m_\wp(g)$ sind also ganze Zahlen. Es seien $C_1, \ldots, C_k$ die Konjugiertenklassen von $G$ und $g_i \in C_i$ für $1 \leq i \leq k$.

Weiter sei $\psi \in \operatorname{Irr}(G)$. Es gilt:

$$\begin{aligned}(\vartheta_\wp, \psi)_G = \frac{1}{|G|}\sum_{g\in G}\vartheta_\wp(g)\overline{\psi(g)} &= \frac{1}{|G|}\sum_{i=1}^{k}|C_i|\vartheta_\wp(g_i)\overline{\psi(g_i)}\\ = \sum_{i=1}^{k}\frac{1}{|C_G(g_i)|}\vartheta_\wp(g_i)\overline{\psi(g_i)} &= \sum_{i=1}^{k} m_\wp(g_i)\overline{\psi(g_i)}\end{aligned}$$

Die Menge der ganz-algebraischen Zahlen über $\mathbb{Q}$ bildet einen Ring, somit ist mit den $m_\wp(g_i)$ und $\overline{\psi(g_i)}$ auch $(\vartheta_\wp, \psi)_G$ ganz-algebraisch. Nach (1.4) ist $(\vartheta_\wp, \psi)_G \in \mathbb{Q}$, woraus nun sogar $(\vartheta_\wp, \psi)_G \in \mathbb{Z}$ folgt. $\vartheta_\wp$ ist also eine $\mathbb{Z}$-Linearkombination von irreduziblen Charakteren von G, d.h. ein verallgemeinerter Charakter. □

## 1.2 Thompsons Klassenfunktionen

Sei $G$ eine endliche Gruppe und $p$ eine Primzahl.

In [Tho96] hat Thompson die Funktionen

$$\begin{aligned}\chi_p(g) &= |\{h \in G \mid \text{die } p\text{-Sylow-Gruppen von } \langle g, h\rangle \text{ sind abelsch}\}|,\\ \chi_{\mathrm{solv}}(g) &= |\{h \in G \mid \langle g, h\rangle \text{ ist auflösbar}\}|,\\ \chi_{\mathrm{nilp}}(g) &= |\{h \in G \mid \langle g, h\rangle \text{ ist nilpotent}\}|,\end{aligned}$$

$g \in G$, vorgestellt und (zumindest für die erste) explizit gezeigt, dass es sich jeweils um verallgemeinerte Charaktere von $G$ handelt. Dies werden wir im Folgenden ebenfalls zeigen, jedoch verwenden wir das allgemeinere Konzept aus dem vorigen Abschnitt.

**(1.11) Lemma**
Es sei $U \leq G$, $x \in N_G(U)$ und $H = \langle U, x\rangle = U\langle x\rangle$.
Dann wird jedes $l \in \mathbb{N}$ vom Index

$$\left[\langle U, x\rangle : \langle U, x^l\rangle\right]$$

geteilt.

**Beweis**
Zunächst ist $\langle U, x^l \rangle$ normal in $H = \langle U, x \rangle$, denn $x$ normalisiert $U$. Außerdem ist

$$H / \langle U, x^l \rangle = \langle U, x^l \rangle \langle x \rangle / \langle U, x^l \rangle \cong \langle x \rangle / \Big( \langle U, x^l \rangle \cap \langle x \rangle \Big)$$

zyklisch. Da weiter $x^l$ in $\langle U, x^l \rangle \cap \langle x \rangle$ enthalten ist, folgt

$$a^l = 1 \;\text{ für alle }\; a \in \langle x \rangle / \Big( \langle U, x^l \rangle \cap \langle x \rangle \Big).$$

Daraus erhalten wir wegen

$$\Big[ H : \langle U, x^l \rangle \Big] = \Big[ \langle x \rangle : \Big( \langle U, x^l \rangle \cap \langle x \rangle \Big) \Big]$$

die Behauptung. □

**(1.12) Lemma**
Es sei $U \leq G$, $x \in N_G(U)$ und $d \in C_G(U)$.
Dann sind die $p$-Sylow-Gruppen von $\langle U, x \rangle$ genau dann abelsch, wenn die $p$-Sylow-Gruppen von $\langle U, xd \rangle$ abelsch sind.
**Beweis**
Es genügt anzunehmen, dass $\langle U, x \rangle$ abelsche $p$-Sylow-Gruppen besitzt, und unter dieser Voraussetzung zu zeigen, dass die $p$-Sylow-Gruppen von $\langle U, xd \rangle$ ebenfalls abelsch sind. Denn die umgekehrte Schlussrichtung kann wegen $xd \in N_G(U)$ und $d^{-1} \in C_G(U)$ auf die gezeigte Implikation zurückgeführt werden.
Es sei $l \in N$ mit $p \nmid l$, so dass $x^l = x_p$ ist (vgl. Anhang (C.3)). Nach (1.11) sind wegen $p \nmid l$ alle $p$-Sylow-Gruppen von $\langle U, x \rangle$ in $\langle U, x_p \rangle$ enthalten. Demnach sind auch die $p$-Sylow-Gruppen von $\langle U, x_p \rangle$ abelsch. Es bezeichne $Q$ eine $p$-Sylow-Gruppe von $\langle U, x_p \rangle$, die $x_p$ enthält. Dann ist

$$\overline{Q} := Q \cap U$$

eine $p$-Sylow-Gruppe von $U$ und $x_p$ zentralisiert diese. Dann wird $\overline{Q}$ auch von $x_p d'$ für alle $d' \in C_G(U)$ zentralisiert. Und wegen $(x_p d')_p \in \langle x_p d' \rangle$ vertauscht schließlich auch $(x_p d')_p$ mit jedem Element von $\overline{Q}$ für alle $d' \in C_G(U)$, so dass die $p$-Sylow-Gruppen von $\langle U, (x_p d')_p \rangle$ abelsch sind.
Mit einem $m \in N,\ p \nmid m$, können wir

$$(x_p d')_p = (x_p d')^m$$

schreiben. Wieder folgt mit (1.11) und $p \nmid m$, dass alle $p$-Sylow-Gruppen von $\langle U, x_p d' \rangle$ in $\langle U, (x_p d')_p \rangle$ enthalten sind. Daraus schließen wir, dass auch die $p$-Sylow-Gruppen von $\langle U, x_p d' \rangle$ abelsch sind.

Es gilt $C_G(U) \trianglelefteq N_G(U)$. Insbesondere ist $xC_G(U) = C_G(U)x$. Zu jedem $d_1 \in C_G(U)$ existiert also ein $d_2 \in C_G(U)$ mit $d_1 x = x d_2$. Daraus schließen wir

$$(xd)^2 = xdxd = x^2 d\tilde{d} \text{ für ein geeignetes } \tilde{d} \in C_G(U)$$

und induktiv

$$(xd)^l = x^l \overline{d} \text{ für ein geeignetes } \overline{d} \in C_G(U).$$

Somit gilt:

$$\left\langle U, (xd)^l \right\rangle = \left\langle U, x_p \overline{d} \right\rangle \text{ hat abelsche } p\text{-Sylow-Gruppen,}$$

weswegen mittels erneuter Anwendung von (1.11) auch die $p$-Sylow-Gruppen von $\langle U, xd \rangle$ abelsch sind. □

**(1.13) Satz**
$\chi_p$ ist ein verallgemeinerter Charakter von $G$.

**Beweis**
Wir zeigen, dass der Verband

$$\wp = \{U \leq G \mid \text{die } p\text{-Sylow-Gruppen von } U \text{ sind abelsch}\}$$

den Eigenschaften aus (1.1) genügt. Dann folgt die Behauptung mit (1.10). Dabei ist Abgeschlossenheit unter Konjugation trivial, d.h. Eigenschaft (1) ist erfüllt. Für die zweite Eigenschaft sei $U \leq G$ und $x, y \in N_G(U)$, so dass $xy^{-1} \in C_G(U)$ und wir nehmen an, dass

$$\langle U, x \rangle \in \wp$$

ist, das heißt, die $p$-Sylow-Gruppen von $\langle U, x \rangle$ sind abelsch. Wir müssen zeigen, dass die $p$-Sylow-Gruppen von $\langle U, y \rangle$ ebenfalls abelsch sind. Wir wählen $d := yx^{-1} = \left(xy^{-1}\right)^{-1} \in C_G(U)$. Nach (1.12) sind dann die $p$-Sylow-Gruppen von $\langle U, xyx^{-1} \rangle$ abelsch. Aber wegen

$$\langle U, xyx^{-1} \rangle = \langle U, y^{x^{-1}} \rangle = \langle U^x, y \rangle^{x^{-1}} = \langle U, y \rangle^{x^{-1}}$$

sind dann auch die $p$-Sylow-Gruppen von $\langle U, y \rangle$ abelsch, und das war zu zeigen. $\square$

Die beiden anderen Klassenfunktionen benötigen keine Hilfssätze und können leichter als verallgemeinerte Charaktere identifiziert werden.

**(1.14) Satz**
$\chi_{\mathrm{solv}}$ ist ein verallgemeinerter Charakter von $G$.

**Beweis**
Es sei $\wp$ der Verband der auflösbaren Untergruppen von $G$. Wir zeigen wieder, dass $\wp$ die Eigenschaften von (1.1) erfüllt. Offensichtlich ist $\wp$ invariant unter Konjugation. Es seien nun $H \leq G$ und $g, h \in N_G(H)$, so dass $gh^{-1} \in C_G(H)$ ist. Es sei weiter $\langle H, g \rangle$ auflösbar. Dann ist auch $H$ als Untergruppe von $\langle H, g \rangle$ auflösbar. Da $H$ von $h$ normalisiert wird, gilt weiter:

$$\langle H, h \rangle / H = H \langle h \rangle / H \cong \langle h \rangle / \left( H \cap \langle h \rangle \right).$$

Damit ist $\langle H, h \rangle / H$ isomorph zu einer Faktorgruppe der abelschen Gruppe $\langle h \rangle$ und somit auflösbar. Zusammen folgt nun, dass auch $\langle H, h \rangle$ auflösbar ist. Aus Symmetriegründen haben wir damit auch die zweite Eigenschaft aus (1.1) gezeigt, die Behauptung folgt nun mit (1.10). $\square$

**(1.15) Satz**
$\chi_{\mathrm{nilp}}$ ist ein verallgemeinerter Charakter von $G$.

**Beweis**
Es sei $\wp$ der Verband der nilpotenten Untergruppen von $G$. Da Nilpotenz eine Eigenschaft ist, die sich via Konjugation vererbt, ist Eigenschaft (1) aus (1.1) erfüllt. Es seien nun $H \leq G$ und $g, h \in N_G(H)$, so dass $gh^{-1} \in C_G(H)$ ist, und wir nehmen an, dass $\langle H, g \rangle$ nilpotent ist. Insbesondere ist also $H$ nilpotent. Setze $d := \left(gh^{-1}\right)^{-1}$. Es sei $l \in \mathbb{Z}$, so dass $g^l \in Z(U)$ ist. Wegen $C_G(U) \trianglelefteq N_G(U)$ existiert ein $d' \in C_G(U)$ mit $(gd)^l = g^l d'$. Dann gilt die Isomorphie

$$\langle U, gd \rangle / \langle (gd)^l \rangle = U \langle gd \rangle / \langle g^l d' \rangle = U \langle g^l d' \rangle / \langle g^l d' \rangle \cong U / \left( U \cap \langle g^l d' \rangle \right).$$

Also ist $\langle U, gd\rangle / \langle (gd)^l \rangle$ als homomorphes Bild von $U$ nilpotent. Weiter ist $(gd)^l = g^l d' \in C_G(U)$, und daher ist $\langle (gd)^l \rangle$ eine Untergruppe des Zentrums von $\langle U, gd\rangle$. Daraus folgt nun die Nilpotenz von $\langle U, gd\rangle$. Abschließend betrachten wir

$$\langle U, gd\rangle = \langle U, ghg^{-1}\rangle = \langle U^g, h\rangle^{g^{-1}} = \langle U, h\rangle^{g^{-1}}$$

und stellen aufgrund der Konjugiertheit fest, dass auch $\langle U, h\rangle$ nilpotent ist. Dies zeigt Eigenschaft (2) von (1.1) und die Behauptung folgt mit (1.10). $\square$

Alle von Thompson definierten Klassenfunktionen werden also von unserem allgemeineren Konzept, das auf die Ideen von Gagola und Lewis zurückgeht, abgedeckt.

# Kapitel 2

# Die Klassenfunktion $\chi_p$

Sei $G$ eine endliche Gruppe und $p$ eine Primzahl. Die im vorigen Kapitel eingeführte Klassenfunktion

$$\chi_p(g) = |\{h \in G \mid \text{die } p\text{-Sylow-Gruppen von } \langle g, h \rangle \text{ sind abelsch}\}|, \quad g \in G,$$

wollen wir in diesem Kapitel eingehender untersuchen. Da wir bereits gesehen haben, dass $\chi_p$ ein verallgemeinerter Charakter ist, interessiert nun insbesondere, unter welchen Bedingungen $\chi_p$ ein Charakter von $G$ ist.

## 2.1 Erste Eigenschaften

Wir beginnen mit einem Spezialfall.

**(2.1) Bemerkung**
Ist G abelsch, so ist $\chi_p$ Charakter von $G$ für alle $p \in \mathbb{P}$, denn offensichtlich ist in diesem Fall $\chi_p = |G| \cdot \mathbb{1}_G$.

Abelsche Gruppen liefern also Positivbeispiele, d.h. für diese Gruppen ist $\chi_p$ stets ein Charakter. Jedoch ist $\chi_p$ dann als Vielfaches des Einscharakters eher uninteressant. Diesen trivialen Fall $\chi_p = |G| \cdot \mathbb{1}_G$ können wir vollständig charakterisieren:

**(2.2) Bemerkung**

(a) Es gilt $\chi_p = |G| \cdot \mathbb{1}_G$ genau dann, wenn die $p$-Sylow-Gruppen von $G$ abelsch sind.

(b) Gilt $p^3 \nmid |G|$ für $p \in \mathbb{P}$, so folgt $\chi_p = |G| \cdot \mathbb{1}_G$.

**Beweis**

(a) Es seien die $p$-Sylow-Gruppen von $G$ abelsch und $x \in G$. Für beliebiges $y \in G$ liegt dann eine $p$-Sylow-Gruppe von $\langle x, y \rangle$ in einer $p$-Sylow-Gruppe von $G$ und ist deswegen abelsch. Somit gilt $\chi_p(x) = |G|$.
Nun seien die $p$-Sylow-Gruppen von $G$ nicht abelsch. Aus einer dieser Sylowgruppen wähle man dann zwei nicht-kommutierende Elemente $a$, $b$. Die davon erzeugte Untergruppe $\langle a, b \rangle$ ist eine $p$-Gruppe, deswegen gleich ihrer Sylow-Gruppe, und nicht abelsch. Also ist $\chi_p(a) < |G|$ gelten, was $\chi_p \neq |G| \cdot \mathbb{1}_G$ bedeutet.

(b) Folgt aus (a). □

Die Aussage (b) der Bemerkung ist sehr nützlich für Beispielrechnungen, da sie eine einfache Bedingung liefert, wann überhaupt nicht-triviale Fälle auftreten können.

Wir werden im nächsten Abschnitt sehen, dass für $p$-Gruppen die Klassenfunktion $\chi_p$ stets ein Charakter ist. Das bedeutet, dass eine Gruppe, für die $\chi_p$ kein Charakter ist, von zusammengesetzer Ordnung ist, wobei $p$ mindestens in dritter Potenz als Primteiler vorkommt. Die kleinste in Frage kommende Gruppenordnung für solch einen Fall ist also $2^3 \cdot 3 = 24$ mit $p = 2$. Tatsächlich liefert diese Gruppenordnung das erste Negativbeispiel, wie man leicht mit GAP nachrechnet.

**(2.3) Bemerkung**
Für $p = 2$ und $G = S_4$ ist $\chi_p$ kein Charakter.

Im Laufe dieser Arbeit werden wir uns den symmetrischen Gruppen noch einmal kurz widmen.

## 2.2 $p$-Gruppen

Für diesen Abschnitt sei $G$ eine Gruppe der Ordnung $p^n$ für eine Primzahl $p$ und ein $n \in \mathbb{N}$. Da die Definition von $\chi_p$ bereits eine Primzahl mitbringt, liegt es nahe, $\chi_p$ als Klassenfunktion einer $p$-Gruppe genauer zu untersuchen. Wir werden in diesem Abschnitt sehen, dass $\chi_p$ dann mit einem bekannten Permutationscharakter zusammenfällt.

**(2.4) Bemerkung**

Es sei $k$ die Anzahl der Konjugiertenklassen von $G$. Dann gilt:

(a) $\chi_p(g) = |C_G(g)|$ für alle $g \in G$.

(b) $\left(\chi_p, \mathbb{1}_G\right)_G = k$.

**Beweis**

(a) Da $G$ eine $p$-Gruppe ist, gilt:

$$\begin{aligned}
\chi_p(g) &= |\{h \in G \mid \text{die } p\text{-Sylow-Gruppen von } \langle g, h\rangle \text{ sind abelsch}\}| \\
&= |\{h \in G \mid \langle g, h\rangle \text{ abelsch}\}| \\
&= |\{h \in G \mid gh = hg\}| \\
&= |C_G(g)|\,.
\end{aligned}$$

(b) $G$ operiert auf sich selbst durch Konjugation; die Bahnen dieser Operation sind die Konjugiertenklassen von $G$. Nach dem Beweis von $(a)$ entspricht $\chi_p(g)$ gerade der Anzahl der Fixpunkte von $g$ auf $G$. Somit gilt mit dem Cauchy-Frobenius-Lemma:

$$\left(\chi_p, \mathbb{1}_G\right)_G = \frac{1}{|G|}\sum_{g \in G}\chi_p(g) = k.$$

□

**(2.5) Satz**

Es sei $G$ eine $p$-Gruppe, $\psi$ ein irreduzibler Charakter von $G$. Dann gilt:

(a) $\chi_p$ ist ein Charakter von $G$.

(b) $\left(\chi_p, \psi\right)$ ist gleich der Zeilensumme von $\psi$ in der Charaktertafel von $G$.

**Beweis**

(a) $G$ operiere auf sich selbst per Konjugation und wir betrachten die zugehörige Permutationsdarstellung. Für $g \in G$ sei also die Matrix $\Pi(g)$ definiert durch

$$(\Pi(g))_{i,j} = \begin{cases} 1, & \text{falls } g^{-1}g_j g = g_i \\ 0, & \text{sonst} \end{cases}, \quad 1 \leq i, j \leq n.$$

Dann ist $(\Pi(g))_{i,i} = 1$ äquivalent dazu, dass $g^{-1}g_i g = g_i$ ist, oder kurz zu $g_i \in C_G(g)$. Also ist $\operatorname{Spur}(\Pi(g)) = |C_G(g)|$ für alle $g \in G$ und mit (2.4)(a) ist $\chi_p$ ein Charakter von $G$.

(b) Es seien $g_1, \ldots, g_k \in G$ Vertreter der Konjugiertenklassen $C_1, \ldots, C_k$ von $G$. Damit gilt:

$$\begin{aligned}(\chi_p, \psi) &= \frac{1}{|G|}\sum_{g\in G}\chi_p(g)\overline{\psi(g)} = \frac{1}{|G|}\sum_{i=1}^{k}|C_i|\cdot\chi_p(g_i)\overline{\psi(g_i)} \\ &= \frac{1}{|G|}\sum_{i=1}^{k}|C_i|\cdot|C_G(g_i)|\cdot\overline{\psi(g_i)} = \frac{1}{|G|}\sum_{i=1}^{k}|C_i|\cdot\frac{|G|}{|C_i|}\cdot\overline{\psi(g_i)} \\ &= \sum_{i=1}^{k}\overline{\psi(g_i)}.\end{aligned}$$

Nach $(a)$ ist $\chi_p$ ein Charakter von $G$, deshalb gilt

$$(\chi_p, \psi) = \sum_{i=1}^{k}\overline{\psi(g_i)} \in \mathbb{N},$$

weshalb wir auf die komplexe Konjugation verzichten können und schließlich gezeigt haben:

$$(\chi_p, \psi) = \sum_{i=1}^{k}\psi(g_i).$$

□

Der verallgemeinerte Charakter $\chi_p$ ist für $p$-Gruppen also genau der Permutationscharakter, der zur Konjugationsoperation der Gruppe auf sich selbst gehört. Somit kann man die Situation bei $p$-Gruppen als vollständig beschrieben betrachten. Jedoch untersuchen wir zum Abschluss dieses Abschnitts noch eine explizite $p$-Potenz genauer, da Gruppen dieses Typs später Rolle spielen.

**(2.6) Lemma (vgl. [JL93, S. 301f])**
Es sei $G$ eine nicht-abelsche Gruppe der Ordnung $p^3$. Dann hat $G$ ein nichttriviales Zentrum der Ordnung $p$, das von einem Element $z$ erzeugt wird, und die zentrale Faktorgruppe ist von der Form $G/Z \cong C_p \times C_p$, also $G/Z = \langle aZ, bZ\rangle$ für zwei Elemente $a, b \in G$. Man kann also schreiben:

$$G = \left\{a^r b^s z^t \mid 0 \leq r,\ s,\ t \leq p-1\right\}.$$

**(2.7) Satz (vgl. [JL93, Chapter 26, Theorem 26.6])**
Es sei

$$G = \left\{a^r b^s z^t \mid 0 \leq r,\ s,\ t \leq p-1\right\}$$

eine nicht-abelsche Gruppe der Ordnung $p^3$ mit der Notation aus (2.6) und

$$\epsilon = e^{2i\pi/p}$$

eine primitive $p$-te Einheitswurzel. Dann sind die irreduziblen Charaktere von $G$ gegeben durch

$$\begin{aligned} &\chi_{u,v}\ , \quad 0 \leq u, v \leq p-1, \\ &\phi_u\ , \quad 1 \leq u \leq p-1, \end{aligned}$$

wobei

$$\begin{aligned} \chi_{u,v}(a^r b^s z^t) &= \epsilon^{ru+sv}, \\ \phi_u(a^r b^s z^t) &= \begin{cases} p\epsilon^{ut}, & \text{falls } r = s = 0 \\ 0, & \text{sonst.} \end{cases} \end{aligned}$$

**(2.8) Satz**
Es sei $G$ eine nicht-abelsche Gruppe der Ordnung $p^3$. Dann gilt

$$(\chi_p, \psi)_G = \begin{cases} p^2 + p - 1, & \text{falls } \psi = \mathbb{1}_G \\ p - 1, & \text{falls } \psi(1) = 1, \psi \neq \mathbb{1}_G \\ 0, & \text{falls } \psi(1) > 1. \end{cases}$$

**Beweis**
Zunächst gilt $(\chi_p, \mathbb{1}_G)_G = |\mathrm{Irr}(G)|$ nach (2.4)(b). Da $G$ nicht-abelsch ist mit Zentrum von Ordnung $p$, hat $G/G'$ Ordnung $p^2$. Demnach existieren genau $p^2$ lineare, irreduzible Charaktere. Aus der Formel für die Gruppenordnung

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

und der Teilbarkeit der Gruppenordnung durch alle irreduziblen Charaktergrade leitet man nun leicht her, dass nur noch irreduzible Charaktere vom Grad $p$ existieren können. Es sei mit $x$ die Anzahl der irreduziblen Charaktere vom Grad $p$ bezeichnet. Es gilt also

$$p^3 = p^2 \cdot 1^2 + x \cdot p^2.$$

Hieraus ergibt sich $x = p - 1$, und insgesamt besitzt $G$ damit genau $p^2 + p - 1$

| | $z^t$ | $a^r b^s$ |
|---|---|---|
| $\chi_{u,v}$ | $1$ | $\epsilon^{ru+sv}$ |
| $\phi_u$ | $p\epsilon^{ut}$ | $0$ |

Tabelle 2.1: Charaktertafel einer nicht-abelschen Gruppe der Ordnung $p^3$

irreduzible Charaktere. Um die übrigen Skalarprodukte zu berechnen, genügt es nach (2.5)(b), die entsprechenden Zeilensummen der Charaktertafel zu bilden. Mit den Aussagen und Notationen aus (2.7) kann die Charaktertafel von $G$ leicht konstruiert werden, siehe Tabelle 2.1. Dabei gilt

$$0 \leq r, s, t \leq p-1, \ (r,s) \neq (0,0).$$

Die Konjugiertenklassenvertreter entnimmt man dem Beweis von (2.29)(b). Nun bearbeiten wir die restlichen Fälle:
Aus $\psi(1) = 1, \psi \neq \mathbb{1}_G$ folgt $\psi = \chi_{u,v}$ mit $u + v > 0$. Damit gilt dann

$$\begin{aligned}
(\chi_p, \chi_{u,v})_G &= \sum_{t=0}^{p-1} 1 + \sum_{r,s=0,\ r+s>0}^{p-1} \epsilon^{ru}\epsilon^{sv} \\
&= p + \sum_{r,s=0}^{p-1} \epsilon^{ru}\epsilon^{sv} - 1 \\
&= p + \left(\sum_{r=0}^{p-1} \epsilon^{ru}\right) \cdot \left(\sum_{s=0}^{p-1} \epsilon^{sv}\right) - 1.
\end{aligned}$$

Wegen $u + v > 0$ ist mindestens eine der beiden Summen gleich 0, was genau

$$(\chi_p, \chi_{u,v})_G = p - 1$$

bedeutet. Schließlich noch der letzte Fall:

$$(\chi_p, \phi_u)_G = \sum_{t=0}^{p-1} p\epsilon^{ut} = p \cdot 0 = 0.$$

□

## 2.3 Faktorgruppen und direkte Produkte

Es sei $G$ eine beliebige endliche Gruppe und $N$ ein Normalteiler von $G$. Um Missverständnisse mit der Induktion von Charakteren zu vermeiden, schreiben wir $\chi_p^{(H)}$, damit verdeutlicht wird, dass $\chi_p$ auf einer Gruppe $H$ definiert ist. Das heißt, es gilt

$$\chi_p^{(H)}(x) := |\{h \in H \mid \text{die } p\text{-Sylow-Gruppen von } \langle x, h\rangle \text{ sind abelsch}\}|$$

für $x \in H$. Wir wollen in diesem Abschnitt untersuchen, wie $\chi_p^{(G)}$ und $\chi_p^{(G/N)}$ in Beziehung stehen. Dazu stellen wir zunächst eine Beziehung zwischen den Funktionswerten her:

**(2.9) Lemma**
Es sei $N \trianglelefteq G$ mit $p \nmid |N|$. Dann gilt

$$\chi_p^{(G)}(g) = |N| \cdot \chi_p^{(G/N)}(gN)$$

für alle $g \in G$.
Insbesondere ist $\chi_p^{(G)}$ konstant auf Nebenklassen von $N$.

**Beweis**
Es seien $g, h \in G$ beliebig, aber fest und $P$ eine $p$-Sylow-Gruppe von $G$, so dass $Q := \langle g, h\rangle \cap P$ eine $p$-Sylow-Gruppe von $\langle g, h\rangle$ ist. Dann gilt $QN/N \cong Q$, und $QN/N$ ist aus Ordnungsgründen eine $p$-Sylow-Gruppe von $\langle gN, hN\rangle = \langle g, h\rangle N/N$. Also sind die $p$-Sylow-Gruppen von $\langle g, h\rangle$ genau dann abelsch, wenn die $p$-Sylow-Gruppen von $\langle gN, hN\rangle$ abelsch sind. Für unseren verallgemeinerten Charakter bedeutet das

$$\begin{aligned}
\chi_p^{(G/N)}(gN) &= |\{hN \in G/N \mid \langle gN, hN\rangle \text{ hat abelsche } p\text{-Sylow-Gruppen}\}| \\
&= |\{hN \in G/N \mid \langle g, h\rangle \text{ hat abelsche } p\text{-Sylow-Gruppen}\}| \\
&= |\{h \in G \mid \langle g, h\rangle \text{ hat abelsche } p\text{-Sylow-Gruppen}\}| \cdot \frac{1}{|N|} \\
&= \chi_p^{(G)}(g) \cdot \frac{1}{|N|}
\end{aligned}$$

für alle $g \in G$. Dies ist gleichbedeutend mit

$$|N| \cdot \chi_p^{(G/N)}(gN) = \chi_p^{(G)}(g)$$

für alle $g \in G$. $\square$

Im nächsten Satz nutzen wir die obige Identität aus, um Skalarprodukt der Gruppe $G$ und der Faktorgruppe nach $N$ auszurechnen.

**(2.10) Satz**
Es sei $N \trianglelefteq G$ mit $p \nmid |N|$.
Dann ist $\chi_p^{(G)}$ genau dann ein Charakter von $G$, wenn $\chi_p^{(G/N)}$ ein Charakter von $G/N$ ist.

**Beweis**
Es sei $n := |G/N|$. Wähle eine Transversale $g_1, \ldots, g_n$ für $G/N$. Für einen irreduziblen Charakter $\psi^{(G/N)}$ von $G/N$ betrachten wir das Skalarprodukt mit $\chi_p^{(G/N)}$:

$$\begin{aligned}\left(\psi^{(G/N)}, \chi_p^{(G/N)}\right)_{G/N} &= \frac{1}{|G/N|} \sum_{gN \in G/N} \psi^{(G/N)}(gN)\chi_p^{(G/N)}(gN) \\ &= \frac{|N|}{|G|} \sum_{i=1}^{n} \psi^{(G/N)}(g_iN)\chi_p^{(G/N)}(g_iN).\end{aligned}$$

Da $\chi_p^{(G)}$ nach (2.9) konstant auf Nebenklassen von $N$ ist, lässt sich obige Gleichungskette mit der Identität aus (2.9) fortsetzen durch

$$\frac{|N|}{|G|} \sum_{i=1}^{n} \psi^{(G/N)}(g_iN) \frac{1}{|N|} \chi_p^{(G)}(g_i) = \frac{1}{|G|} \sum_{i=1}^{n} \psi^{(G/N)}(g_iN)\chi_p^{(G)}(g_i).$$

Nach (C.4)(b)(c) ist

$$\phi : G \to \mathbb{C},\ g \mapsto \psi^{(G/N)}(gN)$$

ein irreduzibler Charakter von $G$ mit $\phi(g) = \psi^{(G/N)}(gN)$. Damit können wir mit der Konstanz von $\phi$ und $\chi_p$ auf Nebenklassen von $N$ weiter folgern:

$$\frac{1}{|G|} \sum_{i=1}^{n} \psi^{(G/N)}(g_iN)\chi_p^{(G)}(g_i) = \frac{1}{|G|} \sum_{i=1}^{n} \phi(g_i)\chi_p^{(G)}(g_i)$$

$$
\begin{aligned}
&= \frac{|N|}{|G|} \sum_{g \in G} \phi(g) \chi_p^{(G)}(g) \\
&= |N| \left(\phi,\, \chi_p^{(G)}\right)_G .
\end{aligned}
$$

Also ist $\left(\psi^{(G/N)},\, \chi_p^{(G/N)}\right)_{G/N}$ genau dann eine positive ganze Zahl, wenn $|N| \left(\phi,\, \chi_p^{(G)}\right)_G$ eine solche ist. Dies ist offensichtlich äquivalent dazu, dass $\left(\phi,\, \chi_p^{(G)}\right)_G$ eine natürliche Zahl ist. Damit ist gezeigt: Ist $\chi_p^{(G)}$ ein Charakter von $G$, so ist auch $\chi_p^{(G/N)}$ ein Charakter von $G/N$.

Die andere Implikation folgt nun aber aus der Konstanz von $\chi_p^{(G)}$ auf den Nebenklassen von $N$. Denn jeder irreduzible Konstituent von $\chi_p^{(G)}$ ist demnach ebenfalls konstant auf den Nebenklassen von $N$. Somit lässt sich das Skalarprodukt von $\chi_p^{(G)}$ mit einem seiner Konstituenten mit einer analogen Rechnung wie oben berechnen und auf $\chi_p^{(G/N)}$ zurückführen. $\square$

**(2.11) Bemerkung**

Im vorigen Satz kann man auf die Teilerfremdheit der Ordnung des Normalteilers zur Primzahl $p$ nicht verzichten. Als Gegenbeispiel betrachte die Gruppe der invertierbaren $2 \times 2$-Matrizen über dem endlichen Körper mit 3 Elementen

$$
G = GL_2(\mathbb{F}_3) = \left\{ A \in \mathbb{F}_3^{2\times 2} \mid A \text{ invertierbar} \right\}.
$$

Mit GAP lässt sich nachrechnen, dass $\chi_2$ für diese Gruppe ein Charakter ist. Weiter hat $Z(G) = \{a \cdot E_n \mid a \in \mathbb{F}_3 \setminus \{0\}\}$ Ordnung 2 und die zentrale Faktorgruppe ist isomorph zur $S_4$, was unser Minimalgegenbeispiel aus (2.3) ist.

Als Anwendung erhalten wir ein Resultat für dierekte Produkte.

**(2.12) Korollar**

Es seien $A,\, B$ endliche Gruppen mit $p \nmid \operatorname{ggT}(|A|,\, |B|)$ und sei $G = A \times B$.

(a) Es gilt

$$
\chi_p^{(G)}(g) = \chi_p^{(A)}(a) \cdot \chi_p^{(B)}(b)
$$

für alle $g \in G$ mit $g = ab,\ a \in A,\ b \in B$.

(b) $\chi_p^{(G)}$ ist genau dann ein Charakter von $G$, wenn $\chi_p^{(A)}$ und $\chi_p^{(B)}$ Charaktere sind.

**Beweis**

(a) Aufgrund der Voraussetzung nehmen wir ohne Einschränkung an, dass $p \nmid |B|$. Dann ist $B$ ein Normalteiler von $G$, der die Voraussetzung von (2.9) erfüllt. Es gilt also $\chi_p^{(G)}(g) = |B| \cdot \chi_p^{(G/B)}(gB)$. Mit $\chi_p^{(B)} = |B| \cdot \mathbb{1}_B$ und $G/B \cong A$ folgt nun die Behauptung.

(b) Wie bei (a) sei zunächst ohne Beschränkung der Allgemeinheit angenommen, dass $p \nmid |B|$.

„$\Rightarrow$“:
Es gilt $\chi_p^{(B)} = |B| \cdot \mathbb{1}_B$ und $\chi_p^{(G/B)}$ ist nach (2.10) ein Charakter von $G/B$. Mit $G/B \cong A$ folgt die Behauptung.

„$\Leftarrow$“:
Es sei $\psi \in \mathrm{Irr}(G)$ beliebig. Nach (C.5) können wir dann $\psi = \psi^{(A)} \boxtimes \psi^{(B)}$ schreiben für zwei irreduzible Charaktere $\psi^{(A)} \in \mathrm{Irr}(A)$ und $\psi^{(B)} \in \mathrm{Irr}(B)$. Damit gilt:

$$\begin{aligned}
\left(\chi_p^{(G)}, \psi\right)_G &= \frac{1}{|G|} \sum_{x \in G} \chi_p^{(G)}(x)\overline{\psi(x)} \\
&= \frac{1}{|A| \cdot |B|} \sum_{a \in A} \sum_{b \in B} \chi_p^{(G)}(ab)\overline{\psi(ab)} \\
&= \frac{1}{|A| \cdot |B|} \sum_{a \in A} \sum_{b \in B} \chi_p^{(A)}(a)\overline{\psi(ab)} \cdot \chi_p^{(B)}(b) \\
&= \frac{1}{|A| \cdot |B|} \sum_{b \in B} \sum_{a \in A} \chi_p^{(A)}(a)\overline{\psi^{(A)}(a) \cdot \psi^{(B)}(b)} \cdot \chi_p^{(B)}(b) \\
&= \frac{1}{|B|} \sum_{b \in B} \overline{\psi^{(B)}(b)}\chi_p^{(B)}(b) \cdot \frac{1}{|A|} \sum_{a \in A} \chi_p^{(A)}(a)\overline{\psi^{(A)}(a)} \\
&= \left(\chi_p^{(B)}, \psi^{(B)}\right)_B \cdot \left(\chi_p^{(A)}, \psi^{(A)}\right)_A
\end{aligned}$$

Da nach Voraussetzung $\chi_p^{(A)}$ und $\chi_p^{(B)}$ Charaktere ihrer jeweiligen Gruppen sind, sind beide Faktoren natürliche Zahlen und somit auch ihr Produkt. $\square$

Für semi-direkte Produkte kann man eine zu (2.12)(b) ähnliche Aussage nicht erwarten. Alexander Moreto gab in [Mor04] ein Beispiel für eine Gruppe an, für die $\chi_3$ kein Charakter ist. Die angegebene Gruppe ist ein semi-direktes Produkt aus einer 3-Gruppe $U$ und einer zyklischen Gruppe $V$. Gruppen dieser Art haben wir bereits untersucht und daher gilt, dass $\chi_3^{(U)}$ und $\chi_3^{(V)}$ jeweils Charaktere sind. Somit können wir bei semi-direkten nicht wie bei den direkten Produkten von den einzelnen Faktoren auf das Produkt schließen. Im nächsten Abschnitt werden wir das angegebene Beispiel noch genauer untersuchen und zu einer unendlichen Serie von Gruppen mit ähnlichen Eigenschaften verallgemeinern.

**(2.13) Definition**
Eine Gruppe $G$ heißt *p-nilpotent*, falls ein Normalteiler $N \trianglelefteq G$ existiert mit $p \nmid |N|$ und $G/N$ ist $p$-Gruppe.

**(2.14) Satz**
Ist $G$ $p$-nilpotent, so ist $\chi_p^{(G)}$ ein Charakter.

**Beweis**
Es sei $N \trianglelefteq G$ mit $p \nmid |N|$ und $G/N$ ist $p$-Gruppe. Dann gilt nach (2.4)

$$\chi_p^{(G)}(g) = |N| \cdot \chi_p^{(G/N)}(gN) = |N| \cdot |C_{G/N}(gN)|$$

für $g \in G$. Nach (C.4) im Anhang ist die Funktion

$$\phi : G \to \mathbb{C},\ g \mapsto |C_{G/N}(gN)|$$

ein Charakter von $G$. Es sei weiter $\psi \in \mathrm{Irr}(G)$. Es gilt:

$$\begin{aligned}
\left(\chi_p^{(G)}, \psi\right)_G &= \frac{1}{|G|} \sum_{g \in G} |N| \cdot |C_{G/N}(gN)| \cdot \overline{\psi(g)} \\
&= \frac{|N|}{|G|} \sum_{g \in G} |C_{G/N}(gN)| \cdot \overline{\psi(g)} \\
&= \frac{|N|}{|G|} \sum_{g \in G} \phi(g) \cdot \overline{\psi(g)} \\
&= |N| \cdot (\phi, \psi)_G \in \mathbb{N}.
\end{aligned}$$

Damit ist $\chi_p^{(G)}$ ein Charakter. $\square$

Aus der Gruppentheorie ist bekannt, dass eine endliche Gruppe genau dann nilpotent ist, wenn sie $p$-nilpotent ist für alle Primzahlen $p \in \mathbb{P}$. Also folgt die nächste Bemerkung eigentlich bereits aus (2.14). Wir können aber auch ausschließlich auf Ergebnisse dieser Arbeit zurückgreifen:

**(2.15) Bemerkung**
Es sei $g \in G$ und $|G| = p^m \cdot r$ mit $m,\ r \in \mathbb{N},\ p \nmid r$.
Ist $G$ nilpotent, so ist $\chi_p^{(G)}$ ein Charakter von $G$ und es gilt

$$\chi_p^{(G)}(g) = |C_G(g)|_p \cdot r,$$

wobei $|C_G(g)|_p$ den $p$-Anteil von $|C_G(g)|$ bezeichnet.

**Beweis**
Als endliche, nilpotente Gruppe können wir $G$ schreiben als

$$G = P \times R$$

mit einer $p$-Sylow-Gruppe $P$ und einem $R \leq G$ mit $p \nmid |R|$. Dann folgt die Behauptung aus (2.12) zusammen mit (2.4) und der Tatsache, dass $|C_P(g)| = |C_G(g)|_p$ für alle $g \in G$. □

# 2.4 Existenz von Gegenbeispielen

## 2.4.1 Generische Gegenbeispiele

Wir haben bereits gesehen, dass für $p = 2$ das Gegenbeispiel $S_4$ existiert. In diesem Abschnitt werden wir für jede beliebige ungerade Primzahl ein Gegenbeispiel konstruieren.

Im Folgenden sei $p \in \mathbb{P}$ eine beliebige, ungerade Primzahl. Weiter sei $P$ eine extra-spezielle $p$-Gruppe der Ordnung $p^3$ mit Exponent $p$, d.h.

- $P$ besitzt ein zyklisches Zentrum von Ordnung $p$,
- die zentrale Faktorgruppe $P/Z(P)$ ist elementar-abelsch und

- $g^p = 1$ für alle $g \in P$.

Insbesondere fällt die Kommutatoruntergruppe von $P$ mit dem Zentrum zusammen, das heißt

$$P' = Z(P).$$

Diese Tatsache werden wir in diesem Abschnitt oft ausnutzen.

Der *Kommutator* zweier Elemente $x,\ y$ einer beliebigen Gruppe sei definiert als

$$[x,y] := x^{-1}y^{-1}xy.$$

**(2.16) Lemma**
Es seien $x,\ y \in P$.

(a) Die Abbildungen

$$P \to P,\ g \mapsto [x,g],$$

$$P \to P,\ g \mapsto [g,x]$$

sind Gruppenhomomorphismen.

(b) Es gilt $[x,y] = [x^{-1},y^{-1}]$.

**Beweis**
(a) Es seien $g,\ h \in P$. Wir nutzen aus, dass wegen $P' = Z(P)$ jeder Kommutator im Zentrum liegt. Es gilt:

$$\begin{aligned}[x,gh] &= x^{-1}h^{-1}g^{-1}xgh \\ &= x^{-1}h^{-1}(xhh^{-1}x^{-1})g^{-1}xgh \\ &= (x^{-1}h^{-1}xh)h^{-1}(x^{-1}g^{-1}xg)h \\ &= [x,g][x,h].\end{aligned}$$

Bei der zweiten Abbildung rechnet man analog.

(b) Da nach (a) die Abbildung $P \to P,\ g \mapsto [x,g]$ ein Homomorphismus ist, gilt zunächst

$$[x,y] = [x,y^{-1}]^{-1}.$$

Nun ist aber auch $P \to P,\ g \mapsto [g, x]$ ein Homomorphismus, so dass weiter

$$[x, y^{-1}]^{-1} = \left([x^{-1}, y^{-1}]^{-1}\right)^{-1} = [x^{-1}, y^{-1}]$$

gilt. Dies war zu zeigen. □

In (2.6) haben wir gesehen, dass wir alle Elemente von $P$ darstellen können als

$$P = \left\{ a^r b^s z^t \mid 0 \leq r,\ s,\ t \leq p-1 \right\},$$

wobei $Z(P) = \langle z \rangle$ und $a, b \in P$ mit $P/Z(P) = \langle aZ(P), bZ(P) \rangle$ sind. Um spätere Rechnungen zu vereinfachen, wählen wir speziell

$$z := [b, a] \in P' = Z(P).$$

Denn mit dieser Wahl und (2.16) können wir beliebige Vertauschungen von $a$ und $b$ durch Potenzen von $z$ beschreiben, d.h.

$$b^y \cdot a^x = a^x \cdot b^y \cdot [b^y, a^x] = a^x \cdot b^y \cdot [b, a]^{xy} = a^x \cdot b^y \cdot z^{xy}.$$

Weiter gelten für den Rest dieses Abschnitts die Festsetzungen

$$0 \leq r,\ r_1,\ r_2,\ r_3 \leq p-1,$$
$$0 \leq s,\ s_1,\ s_2,\ s_3 \leq p-1,$$
$$0 \leq t,\ t_1,\ t_2,\ t_3\ \leq p-1,$$

falls an konkreter Stelle nicht anders definiert. Mit Hilfe der gerade erhaltenen Darstellung der Gruppenelemente konstruieren wir nun einen Automorphismus auf $P$. Es sei $\alpha:\ P \to P$ definiert durch

$$\alpha(a^r b^s z^t) = a^{-r} b^{-s} z^t.$$

**(2.17) Bemerkung**
Die Abbildung $\alpha$ definiert einen Automorphismus der Ordnung zwei von $P$.

**Beweis**
Es seien $g = a^{r_1} b^{s_1} z^{t_1}$ und $h = a^{r_2} b^{s_2} z^{t_2}$. Dann gilt

$$\begin{aligned} gh = a^{r_1} b^{s_1} z^{t_1} a^{r_2} b^{s_2} z^{t_2} \qquad &= a^{r_1} b^{s_1} a^{r_2} b^{s_2} z^{t_1+t_2} \\ = a^{r_1} a^{r_2} b^{s_1} [b^{s_1}, a^{r_2}] b^{s_2} z^{t_1+t_2} &= a^{r_1+r_2} b^{s_1+s_2} [b^{s_1}, a^{r_2}] z^{t_1+t_2}. \end{aligned}$$

Also gilt

$$\begin{aligned} \alpha(gh) &= a^{-r_1-r_2} b^{-s_1-s_2} [b^{s_1}, a^{r_2}] z^{t_1+t_2} \\ &= a^{-r_1} a^{-r_2} b^{-s_1} [b^{s_1}, a^{r_2}] b^{-s_2} z^{t_1} z^{t_2} \\ &= a^{-r_1} a^{-r_2} b^{-s_1} [b^{-s_1}, a^{-r_2}] b^{-s_2} z^{t_1} z^{t_2} \\ &= a^{-r_1} b^{-s_1} a^{-r_2} b^{-s_2} z^{t_1} z^{t_2} \\ &= a^{-r_1} b^{-s_1} z^{t_1} a^{-r_2} b^{-s_2} z^{t_2} \\ &= \alpha(g)\alpha(h), \end{aligned}$$

wobei bei der dritten Gleichheit Lemma (2.16)(b) benutzt wurde. Damit ist $\alpha$ ein Homomorphismus und offensichtlich selbstinvers. Also ist $\alpha$ sogar ein Automorphismus der Ordnung zwei, wie behauptet. □

**(2.18) Definition**
Im Folgenden sei mit $G$ stets die endliche Gruppe bezeichnet, die vermöge $\alpha$ aus dem semi-direkten Produkt einer zyklischen Gruppe der Ordnung zwei mit $P$ entsteht, d.h.

$$G = \langle c \rangle \ltimes_\alpha P.$$

Wir schreiben die Elemente von $G$ als Tupel $(c^k,\ h),\ k \in \{0,\ 1\},\ h \in P$.

Die Multiplikation in $G$ ist also gegeben durch

$$\begin{aligned} (c,\ a^{r_1} b^{s_1} z^{t_1}) \cdot (c,\ a^{r_2} b^{s_2} z^{t_2}) &= (1,\ a^{-r_1} b^{-s_1} z^{t_1} a^{r_2} b^{s_2} z^{t_2}) \\ &= (1,\ a^{r_2-r_1} b^{s_2-s_1} [b^{-s_1}, a^{r_2}] z^{t_1+t_2}) \\ &= (1,\ a^{r_2-r_1} b^{s_2-s_1} z^{t_1+t_2-r_2 s_1}). \end{aligned}$$

Wir werden die zu $P$ isomorphe Untergruppe von $G$ ebenfalls mit $P$ bezeichnen, wenn aus dem Kontext klar ist, ob $P$ oder ihre Einbettung in $G$ gemeint ist.

Zunächst leiten wir einige Strukturaussagen über die Gruppe $G$ her, um dann die Werte der Klassenfunktion $\chi_p$ ausrechnen zu können.

**(2.19) Lemma**

(a) $G' = P$.

(b) $Z(G) = Z(P)$.

**Beweis**

(a) Wegen $\mathrm{ggT}(2, p) = 1$ können wir $x,\ y \in \mathbb{Z}$ mit $2x + yp = 1$ wählen. Dann gilt:

$$\begin{aligned}[(c,\ 1), (1, a^x)] &= (c,\ 1)(1,\ a^{-x})(c,\ 1)(1,\ a^x) \\ &= (1,\ a^{2x}) = (1,\ a^{2x+yp}) \\ &= (1,\ a) \in G'\end{aligned}$$

Analog rechnet man $(1,\ b) \in G'$ nach. Mit $Z(P) = P' \leq G'$ folgt nun $(1,\ h) \in G'$ für alle $h \in P$, also $P \leq G'$. Andererseits ist $G/P \cong C_2$ abelsch, also $G' \leq P$.

(b) Angenommen, $(c,\ a^r b^s z^t) \in Z(G)$. Dann kommutiert $(c,\ a^r b^s z^t)$ insbesondere mit $(1,\ a)$. Jedoch ist die Aussage

$$(c,\ a^r b^s z^t)(1,\ a) = (1,\ a)(c,\ a^r b^s z^t)$$

äquivalent zu

$$a^2 = [b^s, a]^{-1}.$$

Dies ist ein Widerspruch, denn wegen $a \notin Z(P)$ hat die Restklasse $aZ(P)$ Ordnung $p$. Es kann also nicht $a^2 \in Z(P)$ gelten. Also war die Annahme falsch, und jedes Element des Zentrums liegt bereits in $P$. Damit folgt die Behauptung. $\square$

Das folgende Lemma gibt einen Überblick über die Konjugation in $G$, die im weiteren Verlauf dieses Abschnitts von Bedeutung sein wird.

**(2.20) Lemma**

Für Konjugation in $G$ gilt:

(a) $(1,\ a^{r_1} b^{s_1} z^{t_1})^{(1,\ a^{r_2} b^{s_2} z^{t_2})} = (1,\ a^{r_1} b^{s_1} z^{t_1 + s_1 r_2 - s_2 r_1})$.

(b) $(1,\ a^{r_1}b^{s_1}z^{t_1})^{(c,\, a^{r_2}b^{s_2}z^{t_2})} = (1,\ a^{-r_1}b^{-s_1}z^{t_1-(s_1r_2-s_2r_1)})$.

(c) $(c,\ a^{r_1}b^{s_1}z^{t_1})^{(1,\, a^{r_2}b^{s_2}z^{t_2})} = (c,\ a^{r_1+2r_2}b^{s_1+2s_2}z^{t_1+r_2(s_1+s_2)+s_2(r_1+r_2)})$.

(d) $(c,\ a^{r_1}b^{s_1}z^{t_1})^{(c,\, a^{r_2}b^{s_2}z^{t_2})} = (c,\ a^{-r_1+2r_2}b^{-s_1+2s_2}z^{t_1+r_2(s_2-s_1)+s_2(r_2-r_1)})$.

**Beweis**

(a) Wir rechnen die Behauptungen nach und machen dabei Gebrauch von den Rechenregeln für den Kommutator (2.16) und der speziellen Wahl von $z$.

$$\begin{aligned}
(1,\ a^{r_1}b^{s_1}z^{t_1})^{(1,\, a^{r_2}b^{s_2}z^{t_2})} &= (1,\ b^{-s_2}a^{-r_2}z^{-t_2})(1,\ a^{r_1}b^{s_1}z^{t_1})(1,\ a^{r_2}b^{s_2}z^{t_2})\\
&= (1,\ b^{-s_2}a^{-r_2}z^{-t_2}a^{r_1}b^{s_1}z^{t_1}a^{r_2}b^{s_2}z^{t_2})\\
&= (1,\ a^{r_1-r_2}b^{-s_2}[b^{-s_2}, a^{r_1-r_2}]b^{s_1}a^{r_2}b^{s_2}z^{t_1})\\
&= (1,\ a^{r_1-r_2}b^{s_1-s_2}a^{r_2}b^{s_2}[b^{-s_2}, a^{r_1-r_2}]z^{t_1})\\
&= (1,\ a^{r_1-r_2}a^{r_2}b^{s_1-s_2}[b^{s_1-s_2}, a^{r_2}]b^{s_2}[b^{-s_2}, a^{r_1-r_2}]z^{t_1})\\
&= (1,\ a^{r_1}b^{s_1}[b,a]^{(s_1-s_2)r_2+(r_1-r_2)s_2}z^{t_1})\\
&= (1,\ a^{r_1}b^{s_1}z^{t_1+s_1r_2-s_2r_1}).
\end{aligned}$$

(b) Die Situation hier führen wir auf Teil (a) zurück:

$$\begin{aligned}
(1,\ a^{r_1}b^{s_1}z^{t_1})^{(c,\, a^{r_2}b^{s_2}z^{t_2})} &= (c,\ b^{s_2}a^{r_2}z^{-t_2})(1,\ a^{r_1}b^{s_1}z^{t_1})(c,\ a^{r_2}b^{s_2}z^{t_2})\\
&= (1,\ b^{-s_2}a^{-r_2}z^{-t_2})(1,\ a^{r_1}b^{s_1}z^{t_1})^{(c,\ 1)}(1,\ a^{r_2}b^{s_2}z^{t_2})\\
&= (1,\ b^{-s_2}a^{-r_2}z^{-t_2})(1,\ a^{-r_1}b^{-s_1}z^{t_1})(1,\ a^{r_2}b^{s_2}z^{t_2})\\
&\underset{(a)}{=} (1,\ a^{-r_1}b^{-s_1}z^{t_1-(s_1r_2-s_2r_1)}).
\end{aligned}$$

(c) Analog zu (a) rechnet man

$$\begin{aligned}
(c,\ a^{r_1}b^{s_1}z^{t_1})^{(1,\, a^{r_2}b^{s_2}z^{t_2})} &= (1,\ b^{-s_2}a^{-r_2}z^{-t_2})(c,\ a^{r_1}b^{s_1}z^{t_1})(1,\ a^{r_2}b^{s_2}z^{t_2})\\
&= (c,\ b^{s_2}a^{r_2}z^{-t_2}a^{r_1}b^{s_1}z^{t_1}a^{r_2}b^{s_2}z^{t_2})\\
&= (c,\ b^{s_2}a^{r_1+r_2}b^{s_1}a^{r_2}b^{s_2}z^{t_1})\\
&= (c,\ a^{r_1+r_2}b^{s_2}[b^{s_2}, a^{r_1+r_2}]b^{s_1}a^{r_2}b^{s_2}z^{t_1})\\
&= (c,\ a^{r_1+r_2}a^{r_2}b^{s_2}b^{s_1}[b^{s_1+s_2}, a^{r_2}]b^{s_2}[b^{s_2}, a^{r_1+r_2}]z^{t_1})\\
&= (c,\ a^{r_1+2r_2}b^{s_1+2s_2}z^{t_1+r_2(s_1+s_2)+s_2(r_1+r_2)}).
\end{aligned}$$

(d) Auch hier benutzen wir das bereits gezeigte:

$$\begin{aligned}(c,\ a^{r_1}b^{s_1}z^{t_1})^{(c,\ a^{r_2}b^{s_2}z^{t_2})} &= (1,\ b^{-s_2}a^{-r_2}z^{-t_2})(c,\ a^{r_1}b^{s_1}z^{t_1})^{(}c,\ 1)(1,\ a^{r_2}b^{s_2}z^{t_2})\\ &= (1,\ b^{-s_2}a^{-r_2}z^{-t_2})(c,\ a^{-r_1}b^{-s_1}z^{t_1})(1,\ a^{r_2}b^{s_2}z^{t_2})\\ &\underset{(c)}{=} (c,\ a^{-r_1+2r_2}b^{-s_1+2s_2}z^{t_1+r_2(s_2-s_1)+s_2(r_2-r_1)}).\end{aligned}$$

□

**(2.21) Korollar**
Es seien $g,\ h_1 \in G \setminus P,\ h_2 \in P$.

(a) Der Kommutator $[g, h_1]$ liegt genau dann in $Z(P)$, wenn $g$ und $h_1$ kommutieren.

(b) Der Kommutator $[g, h_2]$ liegt genau dann in $Z(P)$, wenn $h_2$ in $Z(P)$ liegt.

**Beweis**
Bezeichne mit $\bar{\ }\colon G \to G/Z(P)$ den kanonischen Epimorphismus auf $G/Z(P)$.

(a) Schreibe kurz $g = cx,\ h_1 = cy$ mit $x, y \in P$. Falls $g$ und $h$ kommutieren, ist die Behauptung offensichtlich. Es ist also nur die andere Implikation zu zeigen. Darum gelte $[g, h_1] \in Z(P)$. Dann ist

$$\begin{aligned}1 &= \overline{[g, h_1]} = [\overline{g}, \overline{h_1}] = [\overline{cx}, \overline{cy}]\\ &= \overline{x}^{-1}\overline{c}^{-1}\overline{y}^{-1}\overline{c}^{-1}\overline{c}\ \overline{x}\ \overline{c}\ \overline{y} = \overline{x}^{-1}\overline{c}^{-1}\overline{y}^{-1}\overline{x}\ \overline{c}\ \overline{y}\end{aligned}$$

Da $\overline{c}$ die Elemente von $P/Z(P)$ invertiert, lässt sich die obige Gleichungkette fortsetzen durch

$$\overline{x}^{-1}\overline{y}\ \overline{x}^{-1}\overline{c}^{-1}\overline{c}\ \overline{y} = \overline{x}^{-1}\overline{y}\ \overline{x}^{-1}\overline{c}^{-1}\overline{c}\ \overline{y} = \left(\overline{x}^{-1}\overline{y}\right)^2.$$

Es gilt also $1 = \left(\overline{x}^{-1}\overline{y}\right)^2$, woraus $\overline{x} = \overline{y}$ folgt. Das bedeutet, $x$ und $y$ unterscheiden sich nur um einen zentralen Anteil. Es gibt also ein $w \in Z(P)$ mit $x = yw$. Damit ergibt sich nun

$$gh_1 = cxcy = cywcy = cycyw = cycx = h_1 g,$$

also die Behauptung.

(b) Auch hier ist nur eine Richtung zu zeigen, sei also $[g, h_2] \in Z(P)$. Mit den Bezeichnungen $g = cx,\ h_2 = y$ für $x, y \in P$ ergibt sich mit einer analogen Rechnung wie bei (a), dass

$$1 = [\overline{cx}, \overline{y}] = \overline{y}^2$$

gilt. Daraus folgt $\overline{y} = 1$, also $y \in Z(P)$. □

**(2.22) Lemma**
Jeder Normalteiler von $P$ ist bereits Normalteiler von $G$.

**Beweis**
Auf $P/Z(P)$ operiert $c$ durch invertieren. Deshalb wird jede Untergruppe von $P/Z(P)$ von $c$ festgelassen. Klar ist die triviale Untergruppe von $P$ ein Normalteiler in $G$. Jeder andere Normalteiler von $P$ enthält $Z(P)$. Daraus folgt die Behauptung. □

**(2.23) Korollar**
Es sei $g \in P$. Dann ist $C_P(g) \trianglelefteq G$ und es gilt

$$|C_P(g)| = \begin{cases} p^3, & g \in Z(P) \\ p^2, & \text{sonst.} \end{cases}$$

**Beweis**
Die Untergruppe $C_P(g)$ ist gerade der Kern der Abbildung $x \mapsto [x, g]$, die nach (2.16)(a) ein Homomorphismus von $P$ ist. Also ist $C_P(g)$ Normalteiler in $P$, nach (2.22) auch in $G$. Für $g \in Z(P)$ ist $C_P(g) = P$ klar. Anderenfalls liegt sowohl $\langle g \rangle$ als auch $Z(P)$ in $C_P(g)$. Damit folgt $|C_P(g)| = p^2$. □

**(2.24) Satz**
$G$ kann nicht von zwei Elementen erzeugt werden.

**Beweis**
Angenommen, es existieren $g,\ h \in G$ mit $\langle g, h \rangle = G$. Da $P$ eine echte Untergruppe von $G$ ist, liegt mindestens eines der beiden Elemente nicht in $P$. Ohne Einschränkung nehmen wir an, dass $g$ nicht in $P$ liegt. Wir möchten nun

auschließen, dass $[g,h] \in Z(P)$ gilt. Dazu verwenden wir Korollar (2.21) und unterscheiden nach der Untergruppenzugehörigkeit von $h$. Läge $h$ ebenfalls nicht in $P$, so gilt $[g,h] \in Z(P)$ genau dann, wenn $g$ und $h$ vertauschen. Nach Annahme wäre $G$ dann aber abelsch, was nicht zutrifft. Im anderen Fall $h \in P$ tritt $[g,h] \in Z(P)$ genau dann ein, wenn $h \in Z(P)$ ist. Wegen $Z(P) = Z(G)$ nach (2.19) wäre also auch in diesem Fall die Gruppe $G$ abelsch, da sie nach Annahme von den kommutierenden Elementen $g$ und $h$ erzeugt wird. Es gilt also $[g,h] \in P \setminus Z(P)$. Wir setzen $x := [g,h]$. Dann hat nach Korollar (2.23) der Zentralisator $C := C_P(x)$ die Ordnung $p^2$ und $C$ ist außerdem ein Normalteiler von $G$. Nach Konstruktion kommutieren die Restklassen $gC$ und $hC$, also ist $G/C$ abelsch. Aber dann folgt $G' = P \leq C$, was ein Widerspruch ist.
Also können solche Elemente $g,h \in G$ nicht existieren. □

**(2.25) Korollar**
Es gilt

$$\chi_P(g) = \begin{cases} 2p^3, & g \in G \setminus P, \\ p^3 + p^2, & g \in P \setminus Z(P), \\ 2p^3, & g \in Z(P). \end{cases}$$

**Beweis**
**1. Fall:**
Es sei $g \in G \setminus P$. Hier ist die Ordnung von $g$ gerade, da die $p$-Sylow-Gruppe $P$ normal ist. Für jedes $h \in G$ ist nach (2.24) das Erzeugnis $\langle g,h \rangle$ eine echte Untergruppe von $G$, die nicht in $P$ liegt. Also ist die Ordnung von $\langle g,h \rangle$ ein Teiler von $2p^2$ und hat somit stets eine abelsche $p$-Sylow-Gruppe. Das bedeutet $\chi_P(g) = |G| = 2p^3$.

**2. Fall:**
Es sei $g \in P \setminus Z(P)$. Für $h \in G \setminus P$ sind wir in der Situation von Fall 1 mit vertauschten Rollen von $g$ und $h$. Also sind die $p$-Sylow-Gruppen von $\langle g,h \rangle$ abelsch. Für $h \in P \setminus C_P(g)$ ist $\langle g,h \rangle = P$, da $\langle g,h \rangle$ nicht-abelsch ist. Insbesondere sind hier die zu betrachtenden Sylow-Gruppen nicht abelsch. Schließlich hat man für $h \in C_P(g)$, dass $\langle g,h \rangle$ abelsch ist. Insgesamt gilt also

$$\text{die } p\text{-Sylow Gruppen von } \langle g,h \rangle \text{ sind abelsch } \Leftrightarrow \ h \in G \setminus P \text{ oder } h \in C_P(g)$$

und man erhält mit (2.23)

$$\chi_P(g) = (2p^3 - p^3) + p^2 = p^3 + p^2.$$

**3. Fall:**
Für $g \in Z(P) = Z(G)$ gilt offensichtlich $\chi_P(g) = |G| = 2p^3$. $\square$

Im nächsten Schritt geben wir die irreduziblen Charaktere von $G$ an. Zunächst liefert $P$ einige nicht-triviale Charaktere vom Grad zwei.

**(2.26) Satz**
Es seien $\mu,\ \nu \in \mathrm{Irr}(P) \setminus \{\mathbb{1}_P\}$ linear.

(a) $\mu^G \in \mathrm{Irr}(G)$ und $\mu^G(1) = 2$.

(b) Es gilt $\mu^G = \nu^G$ genau dann, wenn $\mu = \nu$ oder $\mu = \overline{\nu}$ ist.

**Beweis**
Es sei $\mu \in \mathrm{Irr}(P) \setminus \{\mathbb{1}_P\}$ mit $\mu(1) = 1$. Nach (2.7) hat $\mu$ die Form

$$\mu = \chi_{u,v} \;\text{ mit }\; 0 \leq u,\ v \leq p-1,\ (u,v) \neq (0,0)$$

und

$$\chi_{u,v}(a^r b^s z^t) = \epsilon^{ru+sv}$$

für eine $p$-te primitive Einheitswurzel $\epsilon$.

(a) Zunächst gilt $\mu^G(1) = [G:P] = 2$. Wir zeigen nun, dass die Trägheitsgruppe von $\chi_{u,v}$ in $G$ gleich $P$ ist. Es sei dazu $h = a^r b^s z^t$. Dann gilt:

$$\chi_{u,v}^{(c,1)}(h) = \chi_{u,v}(ca^r b^s z^t c) = \chi_{u,v}(a^{-r} b^{-s} z^t) = \epsilon^{-ru-sv}$$

Nehmen wir nun an, dass $\chi_{u,v}^{(c,1)} = \chi_{u,v}$, so folgt

$$\epsilon^{ru+sv} = \epsilon^{-ru-sv} \qquad \text{für alle } 0 \leq r,\ s,\ t \leq p-1.$$

Da $p$ eine ungerade Primzahl ist, erhalten wir durch äquivalentes Umformen, dass

$$\epsilon^{ru+sv} = 1 \qquad \text{für alle } 0 \leq r,\ s,\ t \leq p-1$$

ist. Dies bedeutet aber genau $u = v = 0$ im Widerspruch zur Wahl von $\chi_{u,v}$. Es gilt also $\chi_{u,v}^{(c,1)} \neq \chi_{u,v}$ und damit ist $P$ die Trägheitsgruppe von $\chi_{u,v}$ in $G$. Nach Clifford ist damit $\mu^G = \chi_{u,v}^G$ irreduzibel.

(b) Für $g \in G$ gilt

$$\chi_{u,v}^G(g) = \frac{1}{|P|} \sum_{\substack{x \in G \\ x^{-1}gx \in P}} \chi_{u,v}(x^{-1}gx)$$

nach Definition des induzierten Charakters. Ist $g \in G \setminus P$, so folgt $\chi_{u,v}^G(g) = 0$, da $x^{-1}gx \notin P$ für alle $x \in G$.

Es sei nun $g \in P$ und $x \in G \setminus P$. Aus dem Beweis von (2.22) entnimmt man, dass $x^{-1}gx = g^{-1} \cdot w$ ist für ein Element $w \in Z(P)$. Da aber $\chi_{u,v}$ unabhängig vom zentralen Anteil von $g$ ist, folgt nun

$$\chi_{u,v}(x^{-1}gx) = \chi_{u,v}(g^{-1}).$$

Also können wir schreiben:

$$\begin{aligned}
\chi_{u,v}^G(g) &= \frac{1}{|P|} \sum_{\substack{x \in G \\ x^{-1}gx \in P}} \chi_{u,v}(x^{-1}gx) = \frac{1}{|P|} \sum_{x \in P} \chi_{u,v}(x^{-1}gx) + \frac{1}{|P|} \sum_{x \notin P} \chi_{u,v}(x^{-1}gx) \\
&= \chi_{u,v}(g) + \chi_{u,v}(g^{-1}) \qquad = (\chi_{u,v} + \overline{\chi_{u,v}})(g).
\end{aligned}$$

Daraus folgt die Behauptung. $\square$

**(2.27) Bemerkung**

Die durch (2.26) erhaltenen irreduziblen Charaktere von $G$ können wir durch

$$\chi_{u,v}^G \;\text{ mit }\; 0 \leq u,\ v \leq p-1,\ (u,v) \neq (0,0)$$

beschreiben mit

$$\chi_{u,v}^G(g) = \begin{cases} 0, & g \in G \setminus P, \\ \chi_{u,v}(g) + \overline{\chi_{u,v}(g)}, & g \in P. \end{cases}$$

Wegen (b) erhalten wir aber jeden dieser Charaktere zweimal, so dass wir die

Wahlen von $u$ und $v$ noch einschränken können. Es seien

$$0 \leq u_1,\ u_2,\ v_1,\ v_2 \leq p-1 \text{ mit } (u_1,v_1) \neq (u_2,v_2) \text{ und } (u_1,v_1),\ (u_2,v_2) \neq (0,0).$$

Dann folgt mit (2.26)(b), dass $\chi^G_{u_1,v_1}$ und $\chi^G_{u_2,v_2}$ genau dann übereinstimmen, falls $\chi_{u_1,v_1} = \overline{\chi_{u_2,v_2}}$ gilt. Äquivalent dazu ist

$$\epsilon^{r(u_1+u_2)+s(v_1+v_2)} = 1 \text{ für alle } 0 \leq r,s \leq p-1.$$

Da $\epsilon$ eine $p$-te primitive Einheitswurzel ist, lässt sich dies wiederum umformen zu

$$p \mid u_1+u_2,\ v_1+v_2$$

und schließlich weiter zu

$$u_1 = p-u_2,\ v_1 = p-v_2.$$

Daher geben folgende Indizes eine eindeutige und vollständige Charakterisierung der in (2.26) bestimmten Charaktere an:

$$\begin{aligned} & 1 \leq\ v \leq\ \frac{p-1}{2},\ \ u=0 \\ \text{oder} \quad & 1 \leq\ u \leq\ \frac{p-1}{2},\ \ v=0 \\ \text{oder} \quad & 1 \leq\ u \leq\ p-1,\ \ 1 \leq\ v \leq\ \frac{p-1}{2}. \end{aligned}$$

**(2.28) Bemerkung**
Es sei $\hat{\lambda} \in \mathrm{Irr}(G/P)$ der nicht-triviale, irreduzible Charakter von $G/P \cong C_2$. Dann ist

$$\lambda : G \to \mathbb{C},\ g \mapsto \hat{\lambda}(g) = \begin{cases} 1, & g \in P, \\ -1, & \text{sonst}, \end{cases}$$

ein irreduzibler Charakter von $G$.

Wir werden später sehen, dass dieser Charakter mit $\chi_p$ negatives Skalarprodukt hat, was sich allerdings an dieser Stelle schon leicht ausrechnen ließe. Als nächstes benötigen wir eine Beschreibung der Konjugiertenklassen von $G$.

**(2.29) Satz**
(a) Für $g \in P \setminus Z(P)$ ist $g^G = g^P \,\dot{\cup}\, (g^{-1})^P$.

(b) $P$ besitzt genau $p^2 + p - 1$ $P$-Konjugiertenklassen.

(c) $G$ besitzt genau $p$ Konjugiertenklassen, die nicht in $P$ liegen.

(d) Die Elemente

$$\begin{aligned} &(1,\, z^t), \quad 0 \le t \le p-1, \\ &(c,\, z^t), \quad 0 \le t \le p-1, \\ &(1,\, a^r b^s), \end{aligned}$$

mit den Indexbereichen

$$\begin{aligned} &1 \le s \le \frac{p-1}{2}, \ r = 0 \\ \text{oder} \quad &1 \le r \le \frac{p-1}{2}, \ s = 0 \\ \text{oder} \quad &1 \le r \le p-1, \ 1 \le s \le \frac{p-1}{2} \end{aligned}$$

bilden ein Repräsentantensystem der Konjugiertenklassen von $G$. Insbesondere besitzt $G$ genau $\frac{1}{2}(p^2 + 4p - 1)$ Konjugiertenklassen.

**Beweis**

Zunächst sei darauf hingewiesen, dass $P$ als Kommutatoruntergruppe ein Normalteiler von $G$ ist, und dass deshalb jede Konjugiertenklasse von $G$ entweder in $P$ oder in $G \setminus P$ liegt.

(a) Sei $g \in P \setminus Z(P)$. Nach Konstruktion von $G$ gilt

$$(1,\, a^r b^s)^{(c,\,1)} Z(P) = (1,\, a^{-r} b^{-s}) Z(P).$$

Aus (2.23) entnimmt man $\left|g^P\right| = p$. Da wegen $P' = Z(P)$ Konjugaion in $P$ nur den zentralen Anteil von $g$ ändert, existiert ein $h \in P$, so dass

$$g^{(c,\,1)h} = g^{-1}$$

ist. Daher ist $g$ in $G$ zu seinem Inversen konjugiert, aufgrund der ungeraden Ordnung von $P$ jedoch nicht in $P$. Aus (2.23) erhält man somit, dass

$$\left|g^G\right| \ge \left|g^P\right| + \left|(g^{-1})^P\right| = 2p$$

ist. Da aber $C_P(g)$ in $C_G(g)$ enthalten ist, folgt aus Ordnungsgründen bereits

Gleichheit. Es gilt also wie behauptet

$$g^G = g^P \,\dot{\cup}\, (g^{-1})^P.$$

(b) Wie bereits in (a) gesehen, ändert die Konjugation in $P$ nur den zentralen Anteil eines Elementes aus $P \setminus Z(P)$. Wegen (2.23) durchläuft der zentrale Anteil das gesamte Zentrum; die Bahnenlänge ist also für die nicht-zentrale Elemente stets $p$. Zusammengefasst bilden die Mengen

$$\left\{a^r b^s z^t \;\middle|\; 0 \le t \le p-1\right\}, \quad 0 \le r,\ s \le p-1,\ (r,s) \ne (0,0).$$

die nicht-trivialen Konjugiertenklassen von $P$. Zusätzlich bildet jedes Zentrumselement eine $P$-Konjugiertenklasse. Insgesamt gibt es also genau $p^2 + p - 1$ Konjugiertenklassen in $P$.

(c) Wir betrachten $g := (c,\ z^t)$ für ein $0 \le t \le p-1$. Wegen $\langle g \rangle,\ Z(P) \subseteq C_G(g)$ wird $|C_G(g)|$ von $2p$ geteilt. Die Konjugiertenklasse von $g$ enthält also höchstens $p^2$ Elemente.
Es sei $x := (1,\ a^r b^s)$. Dann ist

$$g^x = (c,\ a^{2r} b^{2s} z^{t+2rs}).$$

Wegen $0 \le r,\ s \le p-1$ und $\mathrm{ggT}(2,p) = 1$ hat nach obiger Rechnung die Konjugiertenklasse von $g$ mindestens $p^2$ Elemente. Außerdem ist diese Klasse durch $z^t$ bereits eindeutig bestimmt. Mit der Vorüberlegung zum Zentralisator von $g$ folgt insgesamt, dass $|g^G| = p^2$ ist, und dass die $p$ Elemente

$$(c,\ z^t),\ 0 \le t \le p-1,$$

Verteter von $p$ paarweise verschiedenen Konjugiertenklassen bilden. Diese decken $p \cdot p^2 = p^3$ Elemente von $G \setminus P$ ab. Wegen $|G \setminus P| = p^3$ sind dies bereits alle Konjugiertenklassen von $G$, die nicht in $P$ liegen.

(d) Die Zentrumselemente $(1,\ z^t),\ 0 \le t \le p-1$, bilden einelementige Konjugiertenklassen.
Aus Teil (b) wissen wir, dass die Elemente

$$(1,\ a^r b^s),\ 0 \le r,\ s \le p-1,\ (r,s) \ne (0,0)$$

ein Vertretersystem für die Konjugiertenklassen von $P \setminus Z(P)$ bilden. Nach (a) liegen bei Konjugation in $G$ zueinander inverse Elemente in der gleichen Konjugiertenklasse. Somit suchen wir eine maximale Teilmenge des obigen Systems, das keine paarweise inversen Elemente (bis auf Konjugation) mehr enthält. Dazu schränken wir den Indexbereich wie in der Behauptung ein:

$$\begin{aligned} & 1 \leq\ s \leq\ \frac{p-1}{2},\ \ r = 0 \\ \text{oder}\quad & 1 \leq\ r \leq\ \frac{p-1}{2},\ \ s = 0 \\ \text{oder}\quad & 1 \leq\ r \leq\ p-1,\ \ 1 \leq\ s \leq\ \frac{p-1}{2}. \end{aligned}$$

Die Behauptung ist für die Vertreter der Form $(1,\ z^t)$ klar und für $(c,\ z^t)$ folgt diese aus Teil (c). Betrachten wir jetzt die Elemente ohne $a$- oder $b$-Anteil. Da Konjugation mit $(c,\ 1)$ den $a$- bzw $b$-Anteil lediglich invertiert und Konjugation in $P$ nur den zentralen Anteil verändert, besitzen die Vertreter dieser Form (im eingeschränken Repräsentantensystem) keine Inversen. Für $1 \leq\ r \leq\ p-1,\ \ 1 \leq\ s \leq\ \frac{p-1}{2}$ gilt

$$\frac{p+1}{2} \leq p - s \leq p - 1,$$

und daher ist

$$(1,\ a^r b^s)^{-1} = (1,\ a^{-r} b^{-s} z^x) = (1,\ a^{p-r} b^{p-s} z^x),\ \ x \in \mathbb{Z} \text{ geeignet},$$

in keiner der durch die angegebenen Vertreter repräsentierten Konjugiertenklassen enthalten. Dieses eingeschränkte System erfüllt also unsere gewünschte Eigenschaft. Außerdem werden durch die obigen Parameter genau

$$\frac{p-1}{2} + \frac{p-1}{2} + (p-1)\frac{p-1}{2} = \frac{p^2-1}{2}$$

Konjugiertenklassen beschrieben. Das ist nach (a), (b) und (c) die richtige Anzahl. Schließlich entnimmt man (c), dass die Elemente

$$(c,\ z^t),\ 0 \leq t \leq p-1$$

Vertreter für die Konjugiertenklassen in $G \setminus P$ sind. □

Im nächsten Schritt werden wir irreduzible Charaktere vom Grad $p$ konstruieren. Dazu betrachten wir lineare Charaktere einer geeigneten Untergruppe und induzieren diese hoch zu $G$. Es gilt

$$(c,\ 1)(1,\ a) = (c,\ a) = (1,\ a^{-1})(c,\ 1) = (1,\ a)^{-1}(c,\ 1)$$

und $|(c,\ 1)| = 2,\ |(1,\ a)| = p$. Daraus folgt

$$\langle (c,\ 1), (1,\ a) \rangle \cong D_{2p}$$

und sogar

$$\langle (c,\ 1), (1,\ a), (1,\ z) \rangle \cong D_{2p} \times C_p.$$

Es sei im Folgenden $H := \langle (c,\ 1), (1,\ a), (1,\ z) \rangle$. Die Untergruppe $H$ hat Index $p$ in $G$, das heißt, ein nach $G$ induzierter linearer Charakter von $H$ hat Grad $p$. Wir werden zeigen, dass fast alle dieser induzierten Charaktere dann sogar irreduzibel sind.

Zum Beispiel aus [JL93, 18.3, S. 181ff] entnimmt man, dass

$$(1,\ 1),\ (c,\ a) \text{ und } (1,\ a^r) \text{ für } 1 \leq r \leq \frac{p-1}{2}$$

Repräsentanten für die Konjugiertenklassen von $\langle (c,\ 1), (1,\ a) \rangle \cong D_{2p}$ sind. Weiter ist die Charaktertafel gegeben durch

| | $(1,\ 1)$ | $(1,\ a^r)$ | $(c,\ a)$ |
|---|---|---|---|
| $\mathbb{1}_{D_{2p}}$ | $1$ | $1$ | $1$ |
| $\eta$ | $1$ | $1$ | $-1$ |
| $\psi_j$ | $2$ | $\epsilon^{jr} + \epsilon^{-jr}$ | $0$ |

Dabei gilt $1 \leq r,\ j \leq \frac{p-1}{2}$ und $\epsilon$ ist eine primitive $p$-te Einheitswurzel. Die irreduziblen Charaktere von $\langle z \rangle$ lassen sich leicht angeben:

$$\vartheta_k(z^t) = \epsilon^{kt},\ 0 \leq t \leq p-1,\ 1 \leq k \leq p.$$

Die Charaktertafel von $H$ lässt sich dann darstellen als

| | $(1,\ z^t)$ | $(1,\ a^r z^t)$ | $(c,\ az^t)$ |
|---|---|---|---|
| $\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k$ | $\epsilon^{kt}$ | $\epsilon^{kt}$ | $\epsilon^{kt}$ |
| $\eta \boxtimes \vartheta_k$ | $\epsilon^{kt}$ | $\epsilon^{kt}$ | $-\epsilon^{kt}$ |
| $\psi_j \boxtimes \vartheta_k$ | $2\epsilon^{kt}$ | $\epsilon^{jr}(\epsilon^{jr} + \epsilon^{-jr})$ | $0$ |

mit

$$1 \leq r,\ j \leq \frac{p-1}{2},$$
$$0 \leq t \leq p-1 \text{ und}$$
$$1 \leq k \leq p.$$

**(2.30) Lemma**

Die induzierten Charaktere

$$\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)^G \quad \text{und} \quad (\eta \boxtimes \vartheta_k)^G$$

sind irreduzible Charaktere von $G$ mit Klassenwerten

| | $(1,\ z^t)$ | $(1,\ a^r b^s)$ | $(c,\ z^t)$ |
|---|---|---|---|
| $\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)^G$ | $p\epsilon^{kt}$ | $0$ | $\epsilon^{kt}$ |
| $(\eta \boxtimes \vartheta_k)^G$ | $p\epsilon^{kt}$ | $0$ | $-\epsilon^{kt}$ |

Für die Indizes der Konjugiertenklassenvertreter gilt dabei

$$\begin{aligned} & 1 \leq\ s \leq\ \frac{p-1}{2},\ \ r = 0 \\ \text{oder}\quad & 1 \leq\ r \leq\ \frac{p-1}{2},\ \ s = 0 \\ \text{oder}\quad & 1 \leq\ r \leq\ p-1,\ \ 1 \leq\ s \leq\ \frac{p-1}{2}. \end{aligned}$$

und

$$0 \leq t \leq p-1.$$

**Beweis**
Wir bestimmen zunächst die Klassenwerte. Für die zentralen Elemente $(1,\ z^t)$ ist dies leicht:

$$\begin{aligned}\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)^G ((1,\ z^t)) &= \frac{1}{|H|}\sum_{g\in G}\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)((1,\ z^t)) = \frac{1}{|H|}\sum_{g\in G}\epsilon^{kt} \\ &= \frac{1}{2p^2}\cdot 2p^3 \cdot \epsilon^{kt} \qquad\qquad = p\epsilon^{kt}.\end{aligned}$$

Betrachte nun die Konjugiertenklassen, die durch Elemente der Form $(1,\ a^r b^s)$ beschrieben werden. Für die Bestimmung derer Funktionswerte unter dem induzierten Charakter $\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)^G$ gilt es zu entscheiden, wann Konjugation diese Elemente in $H$ überführt und wann nicht. Aus (2.20)(a)(b) ist schnell ersichtlich, dass Konjugation in $G$ den $b$-Anteil eines Elementes festlässt oder invertiert. Das bedeutet

$$\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)^G ((1,\ a^r b^s)) = 0$$

für $s \neq 0$. Für den Fall $s = 0$ beachten wir $r \neq 0$ und stellen mit (2.20) fest:

$$\begin{aligned}(1,\ a^r)^{(1,\ a^{r_2} b^{s_2} z^{t_2})} &= \left(1,\ a^r z^{-s_2 r}\right) \\ (1,\ a^r)^{(c,\ a^{r_2} b^{s_2} z^{t_2})} &= \left(1,\ a^{-r} z^{s_2 r}\right).\end{aligned}$$

Mit der Charaktertafel von $H$ ergibt sich daraus nun

$$\begin{aligned}\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)^G ((1,\ a^r)) &= \frac{1}{|H|}\sum_{g\in G}\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)((1,\ a^r)^g) \\ &= \frac{1}{|H|}\sum_{r_2=0}^{p-1}\sum_{s_2=0}^{p-1}\sum_{t_2=0}^{p-1}\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)\left((1,\ a^r z^{-s_2 r})\right) \\ &\quad + \frac{1}{|H|}\sum_{r_2=0}^{p-1}\sum_{s_2=0}^{p-1}\sum_{t_2=0}^{p-1}\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)\left((1,\ a^{-r} z^{s_2 r})\right) \\ &= \frac{1}{|H|}p^2\sum_{s_2=0}^{p-1}\epsilon^{-ks_2 r} + \frac{1}{|H|}p^2\sum_{s_2=0}^{p-1}\epsilon^{ks_2 r} \\ &= 0.\end{aligned}$$

Es gilt also stets $\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)^G ((1,\ a^r b^s)) = 0$.

Betrachte schließlich noch die Elemente der Form $(c,\ z^t)$. Mit (2.20) gilt

$$\begin{aligned}
(c,\ z^t)^{(1,\ a^{r_2}b^{s_2}z^{t_2})} &= \left(c,\ a^{2r_2}b^{2s_2}z^{t+2s_2r}\right) \\
(c,\ z^t)^{(c,\ a^{r_2}b^{s_2}z^{t_2})} &= \left(c,\ a^{2r_2}b^{2s_2}z^{t+2s_2r}\right).
\end{aligned}$$

Dem entnehmen wir, dass $(c,\ z^t)^x$ genau dann in $H$ liegt, wenn $x$ keinen $b$-Anteil besitzt. Das bedeutet:

$$\begin{aligned}
\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)^G ((c,\ z^t)) &= \frac{1}{|H|} \cdot 2 \cdot \sum_{r_2=0}^{p-1} \sum_{t_2=0}^{p-1} \left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right) \left((c,\ a^{2r_2}z^t)\right) \\
&= \frac{2p}{2p^2} \sum_{r_2=0}^{p-1} \epsilon^{kt} \\
&= \epsilon^{kt}.
\end{aligned}$$

Die Irreduzibilität nachzuweisen ist nun leicht:

$$\begin{aligned}
&\left(\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)^G,\ \left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)^G\right)_G \\
&= \frac{1}{|G|} \left( \sum_{t=0}^{p-1} \left| \left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)^G ((1,\ z^t)) \right|^2 + 0 + \sum_{t=0}^{p-1} \left| \left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)^G ((1,\ z^t)) \right|^2 \right) \\
&= \frac{1}{2p^3} \left(p \cdot p^2 + p \cdot 2p \cdot 1\right) \\
&= 1.
\end{aligned}$$

Die Rechnungen für $(\eta \boxtimes \vartheta_k)^G$ verlaufen in völliger Analogie (vgl. Charaktertafel von $H$) und werden deshalb an dieser Stelle ausgelassen. □

Damit haben wir nun alle Werkzeuge, um die Charaktertafel von $G$ angeben zu können.

**(2.31) Satz**

Mit den Notationen von oben ist die Charaktertafel von $G$ und die Skalarprodukte von $\chi_p$ mit den irreduziblen Charakteren von $G$ gegeben durch

| | $(1,\ z^t)$ | $(1,\ a^r b^s)$ | $(c,\ z^t)$ | $(\,\cdot\,,\ \chi_p)$ |
|---|---|---|---|---|
| $\mathbb{1}_G$ | $1$ | $1$ | $1$ | $\frac{1}{2}(3p^3+p^2+p-1)$ |
| $\lambda$ | $1$ | $1$ | $-1$ | $-\frac{1}{2}(p-1)^2(p+1)$ |
| $\chi_{u,v}^G$ | $2$ | $\epsilon^{ru+sv}+\epsilon^{-(ru+sv)}$ | $0$ | $p-1$ |
| $\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)^G$ | $p\epsilon^{kt}$ | $0$ | $\epsilon^{kt}$ | $0$ |
| $(\eta \boxtimes \vartheta_k)^G$ | $p\epsilon^{kt}$ | $0$ | $-\epsilon^{kt}$ | $0$ |
| $\chi_p$ | $2p^3$ | $p^3+p^2$ | $2p^3$ | $-$ |

Dabei gilt für die Indizes der Charaktere

$$\begin{aligned} & 1 \leq\ v \leq\ \frac{p-1}{2},\ \ u=0 \\ \text{oder}\quad & 1 \leq\ u \leq\ \frac{p-1}{2},\ \ v=0 \\ \text{oder}\quad & 1 \leq\ u \leq\ p-1,\ \ 1 \leq\ v \leq\ \frac{p-1}{2}, \end{aligned}$$

sowie

$$1 \leq k \leq p-1.$$

Die Konjugiertenklassen werden parametrisiert durch

$$\begin{aligned} & 1 \leq\ s \leq\ \frac{p-1}{2},\ \ r=0 \\ \text{oder}\quad & 1 \leq\ r \leq\ \frac{p-1}{2},\ \ s=0 \\ \text{oder}\quad & 1 \leq\ r \leq\ p-1,\ \ 1 \leq\ s \leq\ \frac{p-1}{2}. \end{aligned}$$

und

$$0 \leq t \leq p-1.$$

Insbesondere ist $\chi_p$ kein Charakter von $G$.

**Beweis**

**1. Schritt:** $\mathbb{1}_G$

Hier rechnet man mit (2.25) leicht nach, dass

$$\left(\mathbb{1}_G,\ \chi_p\right)_G = \frac{1}{2p^3} \sum_{g \in G} \chi_p(g)$$

$$
\begin{aligned}
&= \frac{1}{2p^3}\left(\sum_{g\in G\setminus P}\chi_p(g) + \sum_{g\in P\setminus Z(P)}\chi_p(g) + \sum_{g\in Z(P)}\chi_p(g)\right)\\
&= \frac{1}{2p^3}\left(|G\setminus P|\cdot 2p^3 + |P\setminus Z(P)|\cdot(p^3+p^2) + |Z(P)|\cdot 2p^3\right)\\
&= \frac{1}{2}(3p^3+p^2+p-1)
\end{aligned}
$$

gilt.

**2. Schritt:** $\lambda$

Die Einträge der Zeile in der Charaktertafel ergeben sich aus (2.28) und das Skalarprodukt berechnet man ähnlich zum ersten Schritt:

$$
\begin{aligned}
(\lambda,\, \chi_p)_G &= \frac{1}{2p^3}\sum_{g\in G}\lambda(g)\chi_p(g)\\
&= \frac{1}{2p^3}\left(\sum_{g\in G\setminus P}\lambda(g)\chi_p(g) + \sum_{g\in P\setminus Z(P)}\lambda(g)\chi_p(g) + \sum_{g\in Z(P)}\lambda(g)\chi_p(g)\right)\\
&= \frac{1}{2p^3}\Big(|G\setminus P|\cdot(-1)\cdot 2p^3 + |P\setminus Z(P)|\cdot 1\cdot(p^3+p^2)\\
&\qquad + |Z(P)|\cdot 1\cdot 2p^3\Big)\\
&= \frac{1}{2}(-p^3+p^2+p-1)\\
&= -\frac{1}{2}(p-1)^2(p+1).
\end{aligned}
$$

Wegen $p \geq 3$ ist dieses Skalarprodukt also stets negativ.

**3. Schritt:** $\chi_{u,v}^G$

Irreduzibilität und Zeilen der Charaktertafel erhält man direkt aus (2.27) und der Definition von $\chi_{u,v}$ in (2.7). Mit (2.27) rufen wir uns nochmal die Funktionswerte von $\chi_{u,v}^G$ in Erinnerung

$$
\chi_{u,v}^G(g) = \begin{cases} 0, & g\in G\setminus P,\\ \chi_{u,v}(g)+\overline{\chi_{u,v}(g)}, & g\in P. \end{cases}
$$

Wir rechnen

$$\left(\chi_{u,v}^G,\ \chi_p\right)_G = \frac{1}{2p^3}\left(\sum_{g\in G}\chi_{u,v}^G(g)\chi_p^G(g)\right)$$

aus. Dazu unterscheiden teilen wir den Summationsbereich in die Bereiche $G\setminus P$, $P\setminus Z(P)$ und $Z(P)$ auf. Auf $G\setminus P$ ist $\chi_{u,v}^G$ konstant gleich 0, auf $Z(P)$ nach (2.7) konstant gleich 2. Es gilt also

$$\begin{aligned}\left(\chi_{u,v}^G,\ \chi_p\right)_G &= \frac{1}{2p^3}\left(\sum_{g\in G\setminus P}0\cdot 2p^3 + \sum_{g\in P\setminus Z(P)}\chi_{u,v}^G(g)\left(p^3+p^2\right) + \sum_{g\in Z(P)}2\cdot 2p^3\right)\\ &= \frac{1}{2p^3}\left(\sum_{g\in P\setminus Z(P)}\chi_{u,v}^G(g)\left(p^3+p^2\right)+4p^4\right).\end{aligned}$$

Für die verbleibende Summe verwenden wir zunächst die ersten Orthogonalitätsrelationen für den irreduziblen Charakter $\chi_{u,v}$ von $P$, wobei man $(u,v)\neq(0,0)$ beachte:

$$0=\sum_{x\in P}\chi_{u,v}(x) \quad = \sum_{x\in Z(P)}\chi_{u,v}(x)+\sum_{x\in P\setminus Z(P)}\chi_{u,v}(x) = p+\sum_{x\in P\setminus Z(P)}\chi_{u,v}(x).$$

Umgeformt ergibt sich daraus

$$\sum_{x\in P\setminus Z(P)}\chi_{u,v}(x) = -p.$$

Damit können wir nun

$$\begin{aligned}\sum_{g\in P\setminus Z(P)}\chi_{u,v}^G(g) &= \sum_{g\in P\setminus Z(P)}\chi_{u,v}(g)+\overline{\chi_{u,v}(g)}\\ &= \sum_{g\in P\setminus Z(P)}\chi_{u,v}(g)+\overline{\sum_{g\in P\setminus Z(P)}\chi_{u,v}(g)}\\ &= -2p\end{aligned}$$

ausrechnen und erhalten als Skalarprodukt

$$\left(\chi_{u,v}^G,\ \chi_p\right)_G = \frac{1}{2p^3}\left(\sum_{g\in P\setminus Z(P)}\chi_{u,v}^G(g)\left(p^3+p^2\right)+4p^4\right)$$

$$= \frac{1}{2p^3}\left(-2p\left(p^3+p^2\right)+4p^4\right)$$
$$= p-1.$$

**4. Schritt:** $\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)^G$ und $(\eta \boxtimes \vartheta_k)^G$
Irreduzibilität und Charakterwerte entnimmt man Lemma (2.30). Das Skalarprodukt mit $\chi_p$ ist 0, denn die Konjugiertenklassenvertreter, die zum Träger von $\left(\mathbb{1}_{D_{2p}} \boxtimes \vartheta_k\right)^G$ bzw. $(\eta \boxtimes \vartheta_k)^G$ gehören, liegen im Kern von $\chi_p$. □

Satz (2.31) garantiert also für jede ungerade Primzahl $p$ die Existenz einer Gruppe, für die $\chi_p$ kein Charakter ist. Bemerkenswert ist außerdem, dass die hier behandelte Gruppe $G$ nach (2.2) die kleinstmögliche Ordnung besitzt, die ein Gegenbeispiel besitzen kann, nämlich $2p^3$. Insbesondere ist jede dieser Gruppen auflösbar, das Ergebnis aus (2.15) lässt sich also auch für jede ungerade Primzahl nicht auf auflösbare Gruppen ausweiten, was wir für den Fall $p = 2$ durch das Gegenbeispiel $G = S_4$ ja bereits gesehen haben.

### 2.4.2 Symmetrische Gruppen für $p = 2$ - eine Serie?

In (2.3) haben wir bereits gesehen, dass die symmetrische Gruppe auf vier Punkten $S_4$ ein Gegenbeispiel zu Thompsons Vermutung darstellt, dass $\chi_p$ stets ein Charakter ist. Rechnungen mit GAP zeigten, dass $\chi_2$ für die symmetrischen Gruppen $S_n$,

$$n = 5,\ 6,\ 7,\ 8,\ 9,\ 10,$$

kein Charakter ist. Ebenso stellen $S_9,\ S_{10}$ für $\chi_3$ Gegenbeispiele dar. Mindestens für $p = 2$ deutet sich also in den symmetrischen Gruppen eine Serie von Gegenbeispielen an. Leider erkennt man in den rechnerischen Ergebnissen zu den symmetrischen Gruppen wenig Struktur, so dass wir keinen allgemeinen Beweis dafür angeben können, dass $S_n$ für beliebiges $n \in \mathbb{N}$ ein Gegenbeispiel für $p = 2$ darstellt. Allen voran sind Aussagen über die Klassenwerte von $\chi_p$ bei den symmetrischen Gruppen schwierig. Jedoch ist in einer speziellen Situation der Wert einer Konjugiertenklasse beschreibbar.

**(2.32) Satz**
Es seien $n$ eine 2-Potenz und $x \in S_n$ ein $n$-Zykel. Dann gilt

$$\chi_2(x) = n.$$

**Beweis**
Klar ist, dass für $y \in \langle x \rangle$ die Gruppe $\langle x, y \rangle$ eine abelsche 2-Sylow-Gruppe hat. Es sei also nun $y \in S_n \setminus \langle x \rangle$ und setze $G := \langle x, y \rangle$. Wähle eine 2-Sylow-Gruppe $P$ von $G$ mit $\langle x \rangle \subseteq P$. Wir zeigen zunächst, dass $\langle x \rangle$ echt in $P$ enthalten ist. Es sei das Gegenteil angenommen, also dass $\langle x \rangle$ eine 2-Sylow-Gruppe von $\langle x, y \rangle$ ist. Nach (C.6) existiert ein normales 2-Komplent $N$ zu $\langle x \rangle$, d.h.

$$G = \langle x \rangle N, \quad N \trianglelefteq G, \quad \langle x \rangle \cap N = \{1\}.$$

**1. Fall:** $N \subseteq G_\omega$ für alle $\omega \in \{1, \dots, n\}$.
Dann ist $N = \{1\}$ und insbesondere $y \in \langle x \rangle$ wider der Wahl von $y$.

**2. Fall:** Es existiert ein $\omega \in \{1, \dots, n\}$ mit $N \nsubseteq G_\omega$.
$G$ operiert in natürlicher Weise transitiv auf $\{1, \dots, n\}$, weil $x$ ein transitives Element ist. Bezüglich dieser Operation ist $\omega^N$ ein Block von $G$, da $N$ normal in $G$ ist. Die Blocklänge teilt $|\{1, \dots, n\}| = n = 2^m$, ist also eine 2-Potenz. Da $\omega$ nach Voraussetzung nicht von jedem Element von $N$ fixiert wird, gilt

$$2 \mid \left|\omega^N\right|.$$

Andererseits teilt $\left|\omega^N\right|$ als Bahnlänge die Gruppenordnung von $N$. Insbesondere ist daher $|N|$ gerade. Dies ist ein Widerspruch.

Damit ist gezeigt, dass $\langle x \rangle$ echt in der 2-Sylow-Gruppe $P$ von $\langle x, y \rangle$ enthalten ist. Da $x$ selbstzentralisierend ist, kann $P$ nicht abelsch sein. $\square$

An den Rechenergebnissen in Anhang B liest man ab, dass sich der vorangegangene Satz für den Fall, dass $n$ die Potenz einer ungeraden Primzahl ist, nicht analog verallgemeinern lässt. Eventuell deutet die Verwendung des Satzes (C.6) im obigen Beweis, der in dieser Situation nicht anwendbar ist, einen Grund dafür an.

Eine Strategie um zu beweisen, dass die symmetrischen Gruppen eine Serie von Gegenbeispielen für $\chi_p$ liefern ($n = 1, 2, 3$ ausgenommen), könnte das Einschränken von $\chi_p$ auf (kleine) Untergruppen von $S_n$ sein, für die die Einschränkung dann kein Charakter ist. Tatsächlich kann man für $n = 4$ und $n = 8$ nachrechnen, dass die Einschränkung von $\chi_2$ auf eine 2-Sylow-Gruppe von $S_n$ kein Charakter ist. Hier geht wieder ein, dass $n$ eine 2-Potenz ist, denn für andere $n < 9$ führt die Wahl dieser Untergruppe nicht zum Ziel.

# Kapitel 3

# Die Klassenfunktion $\chi_{\text{solv}}$

Wir wiederholen die Definition aus (1.2). Für eine endliche Gruppe $G$ sei die Funktion $\chi_{\text{solv}}$ definiert durch

$$\chi_{\text{solv}}(g) = |\{h \in G \mid \langle g, h \rangle \text{ ist auflösbar}\}|$$

für $g \in G$. Wie im vorigen Kapitel möchten wir auch für diese Klassenfunktion eingehender untersuchen, wann es sich nicht nur um einen verallgemeinerten Charakter, sondern sogar um einen Charakter von $G$ handelt.

## 3.1 Erste Eigenschaften

Wir geben eine Charakterisierung auflösbarer Gruppen von John Thompson an:

**(3.1) Lemma (vgl. [Tho68, Korollar 2])**
Eine endliche Gruppe $G$ ist genau dann auflösbar, wenn je zwei Elemente von $G$ eine auflösbare Gruppe erzeugen.

Daraus ergibt sich unmittelbar als Konsequenz:

**(3.2) Korollar**
(a) $G$ ist genau dann auflösbar, wenn $\chi_{\text{solv}} = |G| \cdot \mathbb{1}_G$ ist.

(b) Es ist $\text{Kern}(\chi_{\text{solv}})$ stets auflösbar.

**Beweis**
(a) Klar nach Definition von $\chi_{\text{solv}}$ und Lemma (3.1).

(b) Es seien $g, h \in \text{Kern}(\chi_{\text{solv}})$ beliebig. Wegen $\chi_{\text{solv}}(g) = |G|$ ist $\langle g, h \rangle$ auflösbar. Nach (3.1) ist dann $\text{Kern}(\chi_{\text{solv}})$ auflösbar. $\square$

**(3.3) Vermutung**
Rechnungen mit GAP zeigten, dass für Gruppen $G$ mit Ordnung höchstens 2000 die Klassenfunktion $\chi_{\text{solv}}$ genau dann ein Charakter von $G$ ist, falls $G$ auflösbar ist. Man kann also vermuten, dass dies für Gruppen beliebiger Ordnung gilt.

Träfe die Vermutung zu, wäre dies eine sehr einfache Charakterisierung dafür, wann $\chi_{\text{solv}}$ ein Charakter ist.

## 3.2 Faktorgruppen

**(3.4) Lemma**
Es sei $N \trianglelefteq G$ auflösbar. Dann gilt

$$\chi_{\text{solv}}^{(G)}(g) = |N| \cdot \chi_{\text{solv}}^{(G/N)}(gN)$$

für alle $g \in G$. Insbesondere ist $\chi_{\text{solv}}^{(G)}$ konstant auf Nebenklassen von $N$.

**Beweis**
Es seien $g, h \in G$.
Ist $\langle g, h\rangle$ auflösbar, dann auch $\langle gN, hN\rangle$, denn es gilt:

$$\langle gN, hN\rangle = \langle g, h\rangle N/N \cong \langle g, h\rangle / \left(\langle g, h\rangle \cap N\right).$$

Es sei andererseits $\langle gN, hN\rangle$ auflösbar. Dann ist wegen obiger Isomorphiekette auch $\langle g, h\rangle / \left(\langle g, h\rangle \cap N\right)$ eine auflösbare Gruppe. Da aber mit $N$ auch $N \cap \langle g, h\rangle$ auflösbar ist, folgt die Auflösbarkeit von $\langle g, h\rangle$.
Wir haben gezeigt:

$$\langle g, h\rangle \text{ auflösbar } \Leftrightarrow \langle gN, hN\rangle \text{ auflösbar.}$$

Nun ergibt sich

$$\begin{aligned} \chi_{\text{solv}}^{(G/N)}(gN) &= |\{hN \in G/N \mid \langle gN, hN\rangle \text{ ist auflösbar}\}| \\ &= |\{hN \in G/N \mid \langle g, h\rangle \text{ ist auflösbar}\}| \\ &= |\{h \in G \mid \langle g, h\rangle \text{ ist auflösbar}\}| \cdot \frac{1}{|N|} \\ &= \chi_{\text{solv}}^{(G)}(g) \cdot \frac{1}{|N|}, \end{aligned}$$

also
$$|N| \cdot \chi_{\mathrm{solv}}^{(G/N)}(gN) = \chi_{\mathrm{solv}}^{(G)}(g)$$
für alle $g \in G$. $\square$

**(3.5) Satz**
Es sei $N \trianglelefteq G$ auflösbar. Dann gilt:
$\chi_{\mathrm{solv}}^{(G)}$ ist genau dann ein Charakter von $G$, wenn $\chi_{\mathrm{solv}}^{(G/N)}$ ein Charakter von $G/N$ ist.

**Beweis**
Völlig analog zum Beweis von (2.10) bei $\chi_p$ folgt hier die Behauptung aus der Identität (3.4). $\square$

**(3.6) Korollar**
Ein minimales Gegenbeispiel $G$ zu (3.3) besitzt keinen nicht-trivialen, auflösbaren Normalteiler.
Insbesondere gilt $Z(G) = \mathrm{Kern}(\chi_{\mathrm{solv}}) = \{1\}$.

**Beweis**
Es sei $G$ eine nicht-auflösbare Gruppe minimaler Ordnung, so dass $\chi_{\mathrm{solv}}^{(G)}$ ein Charakter von $G$ ist, und $G$ besitze einen nicht-trivialen, auflösbaren Normalteiler $N$. Nach (3.5) ist dann $\chi_{\mathrm{solv}}^{(G/N)}$ ein Charakter von $G/N$. Aus der Minimalität von $G$ und $|G/N| < |G|$ schließen wir die Auflösbarkeit von $G/N$. Mit $G/N$ und $N$ ist dann aber auch $G$ auflösbar, was ein Widerspruch ist.
Dass $\chi_{\mathrm{solv}}^{(G)}$ treu ist, folgt nun aus (3.2). Die Aussage über das Zentrum der Gruppe ist klar. $\square$

## 3.3 $\chi_{\mathrm{solv}}$ und die Gruppen $\mathrm{PSL}(2, p)$

Es sei $p$ eine Primzahl. Es bezeichne $\mathrm{GL}(2, p)$ die *allgemeine lineare Gruppe der Dimension 2 über dem Körper* $\mathbb{F}_p$ mit $p$ Elementen, das heißt $\mathrm{GL}(2, p)$ besteht aus allen invertierbaren $2 \times 2$-Matrizen mit Einträgen aus $\mathbb{F}_p$. Die Untergruppe der invertierbaren $2 \times 2$-Matrizen mit Determinante 1 bezeichnen wir mit $\mathrm{SL}(2, p)$. Dann schreiben wir $\mathrm{PSL}(2, p)$ für die zentrale Faktorgruppe $\mathrm{SL}(2, p)/\mathrm{Z}(\mathrm{SL}(2, p))$, genannt *projektive spezielle lineare Gruppe der Dimension 2 über dem Körper* $\mathbb{F}_p$. Thompson hat in [Tho68] gezeigt, dass für $p > 3$, $p^2 + 1 \equiv$

0 mod 5 die Gruppen $\mathrm{PSL}(2,p)$ *minimal-einfache* Gruppen sind. Das heißt, es handelt sich um endliche, nicht-abelsche, einfache Gruppen, deren sämtliche echte Untergruppen auflösbar sind.

Um die Vermutung (3.3) zu untermauern, wollen wir in diesem Abschnitt zeigen, dass für obige Serie minimal-einfacher, nicht-auflösbarer Gruppen die Klassenfunktion $\chi_{\text{solv}}$ kein Charakter ist. Dabei machen wir uns die spezielle Struktur dieser Gruppen zu Nutze, denn es genügt zur Berechnung der Funktionswerte von $\chi_{\text{solv}}$ zu entscheiden, wann ein Paar von Elementen eine echte Untergruppe erzeugt und wann nicht.

Im Folgenden sei $p > 3$ eine Primzahl mit $p^2 + 1 \equiv 0 \bmod 5$. Da man für die Gruppe $\mathrm{PSL}(2,7)$ mit GAP nachrechnen kann, dass $\chi_{\text{solv}}$ kein Charakter ist, sei in diesem Abschnitt sogar $p \geq 13$ angenommen, da dies manche Aussagen und Rechnungen erleichtert.

### 3.3.1 Allgemeine Eigenschaften von PSL$(2,p)$

Die Gruppen $\mathrm{PSL}(2,p)$ bilden eine der wenigen Klassen von Gruppen, deren Untergruppen man vollständig charakterisieren kann. Der folgende Satz gibt darüber Auskunft. In der angegebenen Quelle ist dieser allgemeiner formuliert. Durch unsere Voraussetzungen an die Primzahl $p$ ergibt sich für uns eine vereinfachte Form. Dabei beachte man insbesondere, dass die Bedingung $p^2 + 1 \equiv 0 \bmod 5$ äquivalent ist zu $p^2 - 1 \not\equiv 0 \mod 5$, da das Quadrat einer Primzahl $p > 5$ nur den Rest 1 oder 4 bei Division mit 5 haben kann.

**(3.7) Satz (vgl. [Hup67, Kap. II, Hauptsatz 8.27])**
Die Gruppe $\mathrm{PSL}(2,p)$ besitzt nur die folgenden Untergruppen:

(1) zyklische Gruppen der Ordnung $p$,

(2) zyklische Gruppen deren Ordnung $z$ ein Teiler von $\frac{p\pm1}{2}$ ist,

(3) Diedergruppen der Ordnung $2z$ mit $z$ wie in (2),

(4) Alternierende Gruppen $A_4$,

(5) Symmetrische Gruppen $S_4$ für $p^2 - 1 \equiv 0 \mod 16$,

(6) Semi-direkte Produkte von zyklischen Gruppen der Ordnung $p$ mit zyklischen Gruppen der Ordnung $t$, wobei $t$ ein Teiler von $\frac{p-1}{2}$ ist,

(7) $\mathrm{PSL}(2, p)$.

Die $p$-Sylow-Gruppen von $\mathrm{PSL}(2, p)$ sind also genau die Untergruppen vom Typ (1). Weiter benötigen wir noch einige Eigenschaften von $\mathrm{PSL}(2, p)$.

**(3.8) Lemma (vgl. [Hup67, Kap. II, Hilfssatz 8.1, Satz 8.2, Satz 8.5])**

(a) $|\mathrm{PSL}(2, p)| = \frac{1}{2}(p+1)p(p-1)$

(b) $\mathrm{PSL}(2, p)$ operiert 2-fach transitiv auf der projektiven Geraden

$$\mathrm{P}(1, p) = \left\{ \langle v \rangle \;\middle|\; v \in \mathbb{F}_p^2,\ v \neq 0 \right\}$$

via

$$(x, \langle v \rangle) \mapsto \langle xv \rangle.$$

(c) Die Elemente einer $p$-Sylow-Gruppe von $\mathrm{PSL}(2, p)$ besitzen einen gemeinsamen Fixpunkt auf $\mathrm{P}(1, p)$ und jedes nicht-triviale Element besitzt nur diesen Fixpunkt. Jeder $p$-Sylow-Gruppe kann auf diese Weise ein Punkt der projektiven Geraden zugeordnet werden und umgekehrt. Somit beträgt die Anzahl der $p$-Sylow-Gruppen genau $p+1$, und darüber hinaus schneiden sich je zwei trivial.

Ist im Folgenden von Fixpunkten die Rede, so sei dabei stets implizit Bezug genommen auf die obige Operation.

**(3.9) Lemma (vgl. [Hup67, Kap. II, Satz 8.3, Satz 8.4, Satz 8.5])**

(1) (a) Die Untergruppe $\mathcal{U}$, die genau zwei fest gewählte Punkte $a, b$ fixiert, ist zyklisch der Ordnung $\frac{p-1}{2}$ und je zwei verschiedene Konjugierte von $\mathcal{U}$ haben trivialen Schnitt.

(b) Für jedes $w \in \mathcal{U} \setminus \{1\}$ ist $N_{\mathrm{PSL}(2,p)}(\langle w \rangle)$ eine Diedergruppe der Ordnung $p-1$.

(2) (a) $\mathrm{PSL}(2, p)$ besitzt eine zyklische Untergruppe $\mathcal{S}$ der Ordnung $\frac{p+1}{2}$. Je zwei verschiedene Konjugierte von $\mathcal{S}$ haben trivialen Schnitt.

(b) Für jedes $z \in \mathcal{S} \setminus \{1\}$ ist $N_{\mathrm{PSL}(2,p)}(\langle z \rangle)$ eine Diedergruppe der Ordnung $p+1$.

(c) Jedes nicht-triviale Element von $\mathcal{S}$ besitzt keine Fixpunkte.

(3) Setze für eine $p$-Sylow-Gruppe $\mathcal{P}$ von $\mathrm{PSL}(2,p)$

$$\mathfrak{P} = \{\mathcal{P}^g, \mathcal{U}^g, \mathcal{S}^g \mid g \in \mathrm{PSL}(2,p)\}.$$

Dann bildet $\mathfrak{P}$ eine Partition von $\mathrm{PSL}(2,p)$, das heißt jedes nicht-triviale Element liegt in genau einer der Gruppen aus $\mathfrak{P}$.

Entscheidend wird im Folgenden die Unterscheidung nach der Kongruenz $p^2-1$ mod 16 sein. Denn von den beiden geraden Zahlen $p-1$ und $p+1$ ist genau eine durch 4 teilbar. Also ist $(p-1)(p+1) = p^2-1$ durch 8 teilbar, aber nicht durch 16, falls $p^2-1$ nicht durch 16 teilbar ist. In diesem Fall besitzt genau eine der obigen zyklischen Gruppen $\mathcal{U}$ oder $\mathcal{S}$ eine gerade Ordnung und 2 ist auch die höchste 2-Potenz, die diese teilt. Da jedes Nicht-$p$-Element in einer dieser Gruppen liegt, bedeutet das, dass es keine Elemente der Ordnung 4 geben kann, falls $p^2-1 \not\equiv 0$ mod 16 ist. Insbesondere kann $S_4$ keine Untergruppe von $\mathrm{PSL}(2,p)$ sein.

Jede echte Untergruppe von $\mathrm{PSL}(2,p)$ liegt in einer maximalen Untergruppe von $\mathrm{PSL}(2,p)$. Deshalb ist es für uns von Interesse, eine vollständige Liste der maximalen Untergruppen zu erhalten. Dabei hilft uns eine Arbeit von Giudici, die - angepasst auf unsere Situation - folgenden Satz liefert:

**(3.10) Satz (vgl. [Giu07, Theorem 2.2])**
Die maximalen Untergruppen von $\mathrm{PSL}(2,p)$ sind vom Typ:

(1) $C_{\frac{p-1}{2}} \ltimes C_p$, der Stabilisator eines Punktes der projektiven Geraden,

(2) Diedergruppen $D_{p-1}$ der Ordnung $p-1$,

(3) Diedergruppen $D_{p+1}$ der Ordnung $p+1$,

(4) Alternierende Gruppen $A_4$ für $p^2-1 \not\equiv 0 \mod 16$,

(5) Symmetrische Gruppen $S_4$ für $p^2 - 1 \equiv 0 \mod 16$.

Man beachte, dass eine ungerade Primzahl nur einen ungeraden Rest bei Division mit 8 haben kann, und dass deswegen die Kongruenzen in [Giu07] den hier angegebenen entsprechen.

**(3.11) Bemerkung**

Die triviale Konjugiertenklasse sei mit $Cl_1 = \{1\}$ bezeichnet. Es existieren genau zwei Konjugiertenklassen von $p$-Elementen, die wir mit $Cl_{p_1}$ und $Cl_{p_2}$ bezeichnen, und es gibt genau eine Konjugiertenklasse von 2-Elementen. Deren Bezeichnung sei $Cl_2$. Alle übrigen Elemente fassen wir in den Klassen $Cl_{\frac{p-1}{2}}(i)$ bzw. $Cl_{\frac{p+1}{2}}(j)$ zusammen, je nachdem, ob sie in einer zyklischen Gruppe der Ordnung $\frac{p-1}{2}$ oder $\frac{p+1}{2}$ liegen. Nach der Partition (3.9) ist diese Aufteilung eindeutig und deckt alle Elemente ab.

Dabei gilt $1 \leq i \leq p-1$ und $1 \leq j \leq p+1$ mit den Ausnahmen

$$i \neq \frac{p-1}{2},\ p-1, \quad j \neq \frac{p+1}{2},\ p+1$$

und zusätzlich

$$\begin{aligned} i &\neq \frac{p-1}{4}, \frac{3(p-1)}{4} \qquad \text{für } \ p \equiv 1 \bmod 4 \\ j &\neq \frac{p+1}{4}, \frac{3(p+1)}{4} \qquad \text{für } \ p \equiv 3 \bmod 4. \end{aligned}$$

Wie wir im Beweis sehen werden, werden die Konjugiertenklassen über die Menge der Eigenwerte der Elemente charakterisiert. Die Indizes $i$ und $j$ beschreiben die verschiedenen Eigenwertmengen.

Durch diese Notation ist jede Konjugiertenklasse genau viermal repräsentiert, d.h. die Anzahl der $i$ bzw. $j$ ist durch 4 zu teilen, um die Gesamtzahl der Konjugiertenklassen jeweils zu bestimmen. Diese Notation geht auf das GAP-Paket CHEVIE zurück, das generische Charaktertafeln bestimmter Gruppen - insbesondere auch von $\mathrm{PSL}(2,p)$ - bereitstellt [GHL$^+$93]. Über die Klassenlängen gibt Tabelle 3.1 Auskunft.

**Beweis**

Die Aussage über $Cl_1$ ist klar.

Nach der Partition (3.9) liegt jedes nicht-triviale Element $x \in \mathrm{PSL}(2,p)$ entweder in einer eindeutig bestimmten zyklischen Gruppe mit Ordnung $\frac{p-1}{2}$ bzw. $\frac{p+1}{2}$

| | $\lvert Cl_1\rvert$ | $\lvert Cl_{p_1}\rvert$ | $\lvert Cl_{p_2}\rvert$ | $\lvert Cl_2\rvert$ | $\lvert Cl_{\frac{p-1}{2}}(i)\rvert$ | $\lvert Cl_{\frac{p+1}{2}}(j)\rvert$ |
|---|---|---|---|---|---|---|
| $p \equiv 1 \bmod 4$ | 1 | $\frac{p^2-1}{2}$ | $\frac{p^2-1}{2}$ | $\frac{p(p+1)}{2}$ | $p(p+1)$ | $p(p-1)$ |
| $p \equiv 3 \bmod 4$ | 1 | $\frac{p^2-1}{2}$ | $\frac{p^2-1}{2}$ | $\frac{(p-1)p}{2}$ | $p(p+1)$ | $p(p-1)$ |

Tabelle 3.1: Konjugiertenklassenlängen der PSL$(2,p)$

oder in einer $p$-Sylow-Gruppe. Die Anzahl der $p$-Sylow-Gruppen beträgt nach (3.8) genau $p+1$. Es sei dagegen $H$ eine zyklische Untergruppe von Ordnung $\frac{p-1}{2}$ oder $\frac{p+1}{2}$. Nach der Partition aus (3.9) ist $H$ zu allen anderen Gruppen des jeweiligen Typs konjugiert. Mit $\left|N_{\mathrm{PSL}(2,p)}(H)\right| = 2 \cdot |H|$ folgt

$$|\{H^g \mid g \in \mathrm{PSL}(2,p)\}| = \frac{|\mathrm{PSL}(2,p)|}{2 \cdot |H|}.$$

**1. Fall:** $|x| = 2$
In diesem Fall gilt $x \in H$ mit $H$ wie oben. Nach (3.9)(1)(2) ist $H$ zyklisch und besitzt deshalb nur $x$ als 2-Element. Da weiter alle Untergruppen vom Typ $H$ konjugiert sind, existiert nur eine Konjugiertenklasse von 2-Elementen in PSL$(2,p)$. Die Klassenlänge ist dann nach obiger Vorüberlegung genau

$$\left|x^{\mathrm{PSL}(2,p)}\right| = \left|H^{\mathrm{PSL}(2,p)}\right| = \begin{cases} \frac{1}{2}p(p+1), & \text{für } p \equiv 1 \bmod 4, \\ \frac{1}{2}(p-1)p, & \text{für } p \equiv 3 \bmod 4. \end{cases}$$

**2. Fall:** $|x| = p$
Hier liegt $x$ also in einer $p$-Sylow-Gruppe, von denen es genau $p+1$ gibt. Da eine $p$-Sylow-Gruppe von PSL$(2,p)$ zyklisch der Ordnung $p$ ist, besitzt jede $p$-Sylow-Gruppe genau $p-1$ Elemente der Ordnung $p$.
Insgesamt beträgt die Anzahl der $p$-Elemente in PSL$(2,p)$ genau

$$(p+1)(p-1) = p^2 - 1.$$

Gäbe es ein Nicht-$p$-Element $y \in \mathrm{PSL}(2,p)$, das mit $x$ vertauscht, läge insbesondere $x$ im Zentralisator von $y$ und damit auch im Normalisator. Nach der Partition aus (3.9)(3) hat der Normalisator von $y$ die Ordnung $p \pm 1$, was nicht durch $p$ teilbar ist. Solch ein $y$ kann also nicht existieren und der Zentralisator von $x$ ist die eindeutig bestimmte, $x$ enthaltende $p$-Sylow-Gruppe von $\mathrm{PSL}(2,p)$. Für die Konjugiertenklasse von $x$ gilt deswegen

$$\left|x^{\mathrm{PSL}(2,p)}\right| = \frac{|\mathrm{PSL}(2,p)|}{p} = \frac{p^2-1}{2},$$

und vergleicht man dies mit der Gesamtanzahl der Elemente mit Ordnung $p$, so zeigt das die Existenz von genau zwei Konjugiertenklassen von $p$-Elementen.

**3. Fall:** $|x|$ teilt $\frac{p-1}{2}$, $|x| > 2$
Hier gilt $x \in H = C_{\mathrm{PSL}(2,p)}(x)$ mit $|H| = \frac{p-1}{2}$. Die Konjugiertenklasse von $x$ hat somit $p(p+1)$ Elemente.

Es sei nun $a \in \mathbb{F}_p$ ein Erzeuger der multiplikativen Gruppe $\mathbb{F}_p^*$. Dann gilt also $|a| = p-1$. Offensichtlich ist

$$\begin{pmatrix} a^i & \\ & a^{-i} \end{pmatrix} \in \mathrm{SL}(2,p)$$

für alle $1 \leq i \leq p-1$. Wann liegt bei Übergang zu $\mathrm{PSL}(2,p)$ die Restklasse einer solchen Matrix nicht in den drei Konjugiertenklassen, die durch die bereits behandelten Fälle abgedeckt wurden? Für $i = p-1$ liegt die Einheitsmatrix vor, diesen Fall können wir also ausschließen. Ebenso führt $i = \frac{p-1}{2}$ zu

$$\begin{pmatrix} a^i & \\ & a^{-i} \end{pmatrix}^2 = \begin{pmatrix} -1 & \\ & -1 \end{pmatrix}$$

und auch diese Matrix fällt in die Restklasse des Einselements in $\mathrm{PSL}(2,p)$. Außerdem ist für $p \equiv 1 \mod 4$ der Fall $i = \frac{p-1}{4}$ oder $i = \frac{3(p-1)}{4}$ möglich. Dann hätte die Matrix modulo $\{\pm 1\}$ Ordnung 2. Auch dies müssen wir ausschließen, da wir die 2-Elemente bereits in einer eigenen Konjugiertenklasse zusammengefasst haben. Alle anderen Wahlen für $i$ erzeugen Matrizen, deren Restklassen die gesuchte Ordnung besitzen. Wegen $-a^i = a^{\frac{p-1}{2}} a^i = a^{i+\frac{p-1}{2}}$ und der in $\mathrm{PSL}(2,p)$

geltenden Identität

$$\begin{pmatrix} -a^i & \\ & -a^{-i} \end{pmatrix} = \begin{pmatrix} a^i & \\ & a^{-i} \end{pmatrix}$$

schließen wir, dass sowohl $i$ als auch $i + \frac{p-1}{2}$ die gleiche Konjugiertenklasse identifizieren. Darüber hinaus treffen auch $i$ und $-i = (p-1) - i$ die gleichen Konjugiertenklassen, da

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \cdot \begin{pmatrix} a^i & \\ & a^{-i} \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a^{-i} & \\ & a^i \end{pmatrix}.$$

Das bedeutet, jede Konjugiertenklasse wird viermal getroffen.

Hat ein Element $x \in \mathrm{PSL}(2, p)$ nur einen Eigenwert, so ist dieser bereits 1, denn das Produkt der Eigenwerte ist gerade die Determinante von $A$. Ist $x$ eine Skalarmatrix, so ist $x$ die Einheitsmatrix und nicht von Interesse. Als andere Möglichkeit bleibt dann nur

$$x = \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix},$$

für ein $s \in \mathbb{F}_p^*$. Mit

$$x^n = \begin{pmatrix} 1 & 0 \\ ns & 1 \end{pmatrix}, \quad n \in \mathbb{N},$$

sieht man leicht, dass $x$ ein $p$-Element ist. Auch solche $x$ wollen wir nicht betrachten, da wir $p$-Elemente bereits behandelt haben. Wir können also annehmen, dass $x$ zwei verschiedene Eigenwerte besitzt. Wegen der Determinante sind diese invers zueinander. Es sei $\lambda \in \mathbb{F}_p$ ein Eigenwert von $x$. Bekanntlich ist die Spur gerade die Summe der Eigenwerte. Daher schließen wir, dass das charakteristische Polynom von $x$ die Gestalt

$$\chi_x(X) = X^2 + \left(\lambda + \frac{1}{\lambda}\right) X + 1 = (X + \lambda)(X + \frac{1}{\lambda})$$

besitzt. Insbesondere ist $x$ diagonalisierbar und somit gilt die Ähnlichkeitsrelation

$$x \sim \begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix}.$$

Die gesuchten Konjugiertenklassen werden also durch die Menge der Eigenwerte charakterisiert. Somit deckt die obige Serie von Diagonalmatrizen der Form

$$\begin{pmatrix} a^i & \\ & a^{-i} \end{pmatrix}$$

alle Klassen ab und jede Klasse wird genau viermal getroffen.

**4. Fall:** $|x|$ teilt $\frac{p+1}{2}$, $|x| > 2$
Es gilt $x \in H = C_{\mathrm{PSL}(2,p)}(x)$ mit $|H| = \frac{p+1}{2}$. Die Konjugiertenklasse von $x$ hat somit $(p-1)p$ Elemente. Die Argumente zu den Indizes $j$ und Konjugiertenklassen verlaufen nun völlig analog zum vorigen Fall. $\square$

Aus diesem Beweis ergibt sich als Konsequenz für 3- und 4-Elemente:

**(3.12) Bemerkung**

(a) Es existiert genau eine Konjugiertenklasse $Cl_3$ von 3-Elementen in $\mathrm{PSL}(2, p)$. Diese wird durch die Indizes

$$\frac{p-1}{3}, \frac{2(p-1)}{3}, \frac{p-1}{6}, \frac{5(p-1)}{6} \quad \text{für} \quad p \equiv 1 \bmod 4$$
$$\frac{p+1}{3}, \frac{2(p+1)}{3}, \frac{p+1}{6}, \frac{5(p+1)}{6} \quad \text{für} \quad p \equiv 3 \bmod 4$$

identifiziert.
Die jeweiligen vier Indizes wollen wir im Folgenden zur Menge $D$ zusammenfassen.

(b) Für den Fall $p^2 - 1 \equiv 0 \bmod 16$ existiert genau eine Konjugiertenklasse $Cl_4$ von 4-Elementen in $\mathrm{PSL}(2, p)$. Diese wird mit

$$\frac{p-1}{8}, \frac{3(p-1)}{8}, \frac{5(p-1)}{8}, \frac{7(p-1)}{8} \quad \text{für} \quad p \equiv 1 \bmod 4$$
$$\frac{p+1}{8}, \frac{3(p+1)}{8}, \frac{5(p+1)}{8}, \frac{7(p+1)}{8} \quad \text{für} \quad p \equiv 3 \bmod 4$$

identifiziert.
Hier wollen wir die jeweiligen vier Indizes zur Menge $V$ zusammenfassen.

**(3.13) Lemma**

Es sei $Cl_2$ die Konjugiertenklasse der 2-Elemente in $\mathrm{PSL}(2,p)$, $Cl_{p_1}$ bzw. $Cl_{p_2}$ die beiden Konjugiertenklassen von $p$-Elementen. Für $i = 1,2$ sei

$$a_{p_i22} = \left|\{(x,y) \mid x \in Cl_{p_i},\ y \in Cl_2,\ xy = g_2\}\right|,$$

wobei $g_2$ ein beliebiges, aber festes 2-Element von $\mathrm{PSL}(2,p)$ sei.
Dann gilt:

$$a_{p_122} = a_{p_222} = \begin{cases} p-1, & \text{für } p \equiv 1 \mod 4, \\ 0, & \text{für } p \equiv 3 \mod 4. \end{cases}$$

**Beweis**

Es seien $x_2 \in Cl_2$ und $x_{p_i} \in Cl_{p_i}$, $i = 1,2$. Dann gilt allgemein

$$\begin{aligned} a_{p_i22} &= \frac{|Cl_{p_i}|\,|Cl_2|}{|\mathrm{PSL}(2,p)|} \cdot \sum_{\chi \in \mathrm{Irr}\mathrm{PSL}(2,p)} \frac{\chi(x_{p_i})\chi(x_2)\chi((x_2)^{-1})}{\chi(1)} \\ &= \frac{|Cl_{p_i}|\,|Cl_2|}{|\mathrm{PSL}(2,p)|} \cdot \sum_{\chi \in \mathrm{Irr}\mathrm{PSL}(2,p)} \frac{\chi(x_{p_i})\,|\chi(x_2)|^2}{\chi(1)}. \end{aligned}$$

Dieser Formel sieht man mit Hilfe der Charaktertafeln aus Anhang A sofort an, dass sowohl $a_{p_122} = a_{p_222}$ gilt, als dass auch die Unterscheidung nach der Kongruenz von $p^2 - 1$ modulo 16 unnötig ist. Es sei also zur leichteren Notation $x_p$ ein beliebiges $p$-Element.

Für $p \equiv 1 \bmod 4$ gilt dann

$$\begin{aligned} a_{p_122} &= \frac{\frac{p^2-1}{2}\frac{p(p+1)}{2}}{|\mathrm{PSL}(2,p)|} \sum_{\chi \in \mathrm{Irr}(\mathrm{PSL}(2,p))} \frac{\chi(x_p)\,|\chi(x_2)|^2}{\chi(1)} \\ &= \frac{p+1}{2}\left(1 + 0 + \frac{1}{\frac{p+1}{2}}\left(\frac{1-\sqrt{p}}{2} + \frac{1+\sqrt{p}}{2}\right)\right. \\ &\qquad\left. + \frac{1}{2}\frac{1}{p+1} \sum_{\substack{k=1 \\ k \neq \frac{p-1}{4}, \frac{p-1}{2}}}^{\frac{p-1}{2}} \left|(-1)^k + (-1)^{-k}\right|^2 + 0\right) \\ &= \frac{p+1}{2}\left(1 + \frac{2}{p+1} + \frac{1}{2}\frac{1}{p+1}\left(\frac{p-1}{2} - 2\right)4\right) \end{aligned}$$

$$\begin{aligned}&= \frac{p+1}{2}\left(\frac{p+3}{p+1}+\frac{p-5}{p+1}\right)\\&= p-1,\end{aligned}$$

und für $p \equiv 3 \bmod 4$ haben wir

$$\begin{aligned}a_{p_1 22} &= \frac{\frac{p^2-1}{2}\frac{p(p-1)}{2}}{|\mathrm{PSL}(2,p)|}\cdot \sum_{\chi\in \mathrm{Irr}(\mathrm{PSL}(2,p))} \frac{\chi(x_p)\,|\chi(x_2)|^2}{\chi(1)}\\
&= \frac{p-1}{2}\left(1+0+\frac{1}{\frac{p-1}{2}}\left(\frac{-1-\sqrt{p}}{2}+\frac{-1+\sqrt{p}}{2}\right)+0\right.\\
&\qquad\left.+\frac{1}{2}\frac{1}{p-1}\sum_{\substack{l=1\\ l\neq \frac{p+1}{4},\frac{p+1}{2}}}^{\frac{p+1}{2}} (-1)\left|-(-1)^l-(-1)^{-l}\right|^2\right)\\
&= \frac{p-1}{2}\left(1-\frac{2}{p-1}-\frac{1}{2}\frac{1}{p-1}\left(\frac{p+1}{2}-2\right)4\right)\\
&= \frac{p-1}{2}\left(\frac{p-3}{p-1}-\frac{p-3}{p-1}\right)\\
&= 0. \qquad \square\end{aligned}$$

Eine zentrale Rolle in diesem Abschnitt werden die Unterguppen vom Typ $A_4$ und $S_4$ spielen. Über deren Anzahl geben die folgenden Lemmata Auskunft:

**(3.14) Lemma (vgl. [Hup67, Kap. II, Hilfssatz 8.16, Hilfssatz 8.17, Satz 8.18])** Es existieren genau $\frac{|\mathrm{PSL}(2,p)|}{12}$ Untergruppen vom Typ $C_2 \times C_2$ in $\mathrm{PSL}(2,p)$. Für eine solche Untergruppe $V$ gilt

$$N_{\mathrm{PSL}(2,p)}(V) \cong A_4 \text{ für } p^2-1 \not\equiv 0 \bmod 16$$

und

$$N_{\mathrm{PSL}(2,p)}(V) \cong S_4 \text{ für } p^2-1 \equiv 0 \bmod 16.$$

Da $V$ von oben in seinem Normalisator $A_4$ charakteristisch ist, und weiter auch $A_4$ in ihrer Automorphismengruppe $S_4$ charakteristisch ist, erhalten wir als Konsequenz:

**(3.15) Korollar**
Es gibt genau $\frac{|\mathrm{PSL}(2,p)|}{12}$ Untergruppen vom Typ $A_4$ in $\mathrm{PSL}(2,p)$. Für $p^2-1 \equiv 0 \bmod 16$ existieren zusätzlich genau $\frac{|\mathrm{PSL}(2,p)|}{12}$ Untergruppen vom Typ $S_4$.

### 3.3.2 Zweierzeuger-Untergruppen

Wie bereits zu Anfang des Kapitels erwähnt, ist es für uns von besonderem Interesse entscheiden zu können, wann ein Paar von Elementen von $\mathrm{PSL}(2,p)$ eine echte Untergruppe erzeugt. Darüberhinaus möchten wir die genaue Anzahl dieser Paare bestimmen, um die Funktionswerte von $\chi_{\mathrm{solv}}$ ausrechnen zu können. Dieses Abzählproblem lösen wir mit einer Technik, die von John Bray vorgeschlagen wurde.

**(3.16) Definition**
Es sei $x \in \mathrm{PSL}(2,p)$ und $G \leq \mathrm{PSL}(2,p)$.

(a) Wir nennen $x$ einen *G-Zweierzeuger*, falls ein $y \in G$ existiert mit $\langle x,y\rangle = G$.

(b) Es sei $x$ ein $G$-Zweierzeuger. Dann definieren wir

$$\begin{aligned} U_{x,G} &:= \{U \leq \mathrm{PSL}(2,p) \mid x \in U,\ U \cong G\} \\ E_{x,G} &:= \{y \in \mathrm{PSL}(2,p) \mid \langle x,y\rangle \cong G\} \end{aligned}$$

(c) Für ein $U \in U_{x,G}$ sei

$$F_{x,U} := \{y \in U \mid \langle x,y\rangle = U\}$$

die Menge der Elemente in $U$, die mit $x$ ein zweielementiges Erzeugendensystem bilden.

Es ist offensichtlich das Ziel, $|E_{x,G}|$ für alle $x \in \mathrm{PSL}(2,p)$ und $G \leq \mathrm{PSL}(2,p)$ zu berechnen. Dies ist relativ leicht möglich, wenn $|U_{x,G}|$ bekannt ist.

**(3.17) Bemerkung**
Es gelte die Notation aus Definition (3.16).

(a) $U_{x,G}$, $E_{x,G}$ sind nicht-leere Mengen.

(b) Es gilt offenbar

$$E_{x,G} = \dot{\bigcup_{U \in U_{x,G}}} F_{x,U}$$

und damit, falls $|F_{x,G}| = |F_{x,U}|$ ist für alle $U \in U_{x,G}$,

$$|E_{x,G}| = |U_{x,G}| \cdot |F_{x,G}|\,.$$

**(3.18) Lemma**
Es sei $x \in \mathrm{PSL}(2,p)$ und $G \leq \mathrm{PSL}(2,p)$, so dass $x$ ein $G$-Zweierzeuger ist. Weiter seien alle $|x|$-Elemente in $\mathrm{PSL}(2,p)$ konjugiert. Dann ist die Kardinalität von $U_{x,G}$ gerade

$$|\{U \leq \mathrm{PSL}(2,p) \mid U \cong G\}| \cdot \frac{|\{y \in G \mid |y| = |x|,\ y \text{ ist } G\text{-Zweierzeuger}\}|}{|Cl(x)|}.$$

**Beweis**
Es seien zunächst $x_1, x_2 \in Cl(x)$, also durch ein $g \in \mathrm{PSL}(2,p)$ konjugiert. Dann sind die Mengen $U_{x_1,G}$ und $U_{x_2,G}$ gleichmächtig, da sie durch Konjugation mit $g$ bzw. $g^{-1}$ ineinander überführt werden. Außerdem gilt offensichtlich

$$|U_{x,G}| = |\{(x,U) \mid U \leq \mathrm{PSL}(2,p),\ U \cong G,\ x \in U\}|\,.$$

Damit erhält man aus

$$\begin{aligned}
|Cl(x)| \cdot |U_{x,G}| &= |Cl(x)| \cdot |\{(x,U) \mid U \leq \mathrm{PSL}(2,p),\ U \cong G,\ x \in U\}| \\
&= \sum_{x_0 \in Cl(x)} |\{(x_0,U) \mid U \leq \mathrm{PSL}(2,p),\ U \cong G,\ x_0 \in U\}| \\
&= |\{(x_0,U) \mid U \leq \mathrm{PSL}(2,p), \\
&\qquad U \cong G,\ x_0 \in U,\ |x_0| = |x|,\ x_0 \text{ ist } G\text{-Zweierzeuger}\}| \\
&= |\{U \leq \mathrm{PSL}(2,p) \mid U \cong G\}| \\
&\qquad \cdot |\{y \in G \mid |y| = |x|,\ y \text{ ist } G\text{-Zweierzeuger}\}|
\end{aligned}$$

die Behauptung. □

### 3.3.3 Elemente der Ordnung 3, 4 oder $p$

Wir werden ab jetzt versuchen, den Wert der Klassenfunktion $\chi_{\text{solv}}$ auf einem Element in Abhängigkeit von der Ordnung des Elementes anzugeben. Für $p$-Elemente ist dies leicht:

**(3.19) Satz**
Es sei $x \in \mathrm{PSL}(2,p)$ von Ordnung $p$. Dann gilt

$$\chi_{\text{solv}}(x) = \frac{1}{2}p(p-1).$$

**Beweis**
Es sei $P := \langle x \rangle$ die von $x$ erzeugte $p$-Sylow-Gruppe von $\mathrm{PSL}(2,p)$. Wir schreiben kurz $N := N_{\mathrm{PSL}(2,p)}(P)$ für den Normalisator von $P$ in $\mathrm{PSL}(2,p)$. Nach den Sylow-Sätzen und (3.8)(c) gilt

$$|N| = \frac{|\mathrm{PSL}(2,p)|}{p+1} = \frac{\frac{1}{2}(p+1)p(p-1)}{p+1} = \frac{1}{2}p(p-1).$$

Weiter ist $N$ eine echte Untergruppe, da $\mathrm{PSL}(2,p)$ einfach ist, aber sonst $P$ ein nicht-trivialer Normalteiler wäre. Nach Thompsons Charakterisierung minimal-einfacher Gruppen ist damit $\langle x,y \rangle$ als echte Untergruppe auflösbar für alle $y \in N$, da $\langle x,y \rangle \subseteq N$. Wir können also abschätzen:

$$\chi_{\text{solv}}(x) \geq |N| = \frac{1}{2}p(p-1).$$

Es sei nun $y \notin N$. Anhand der Liste (3.7) diskutieren wir, welchem Typ von Untergruppe das Gruppenerzeugnis $\langle x,y \rangle$ entspricht.
Da $\langle x,y \rangle$ sicher nicht-abelsch ist, können wir die Typen (1) und (2) ausschließen. Desweiteren enthält $\langle x,y \rangle$ mit $x$ ein Element der Ordnung $p$, womit auch die Typen (3) und (4) ausscheiden, denn es ist $p \geq 13$. Die Anzahl der $p$-Sylow-Gruppen einer Untergruppe vom Typ (5) ist ein Teiler von $t$ und ist gleichzeitig von der Form $1+kp,\ k \in \mathbb{N}$. Da $t$ selbst ein Teiler von $p-1$ ist, kann es nur eine $p$-Sylow-Gruppe in $\langle x,y \rangle$ geben. In unserem Fall wäre diese gerade $P$. Also wäre $P$ normal in $\langle x,y \rangle$ und würde somit insbesondere von $y$ normalisiert werden. Das widerspricht der Wahl von $y$. Als einzig verbleibende Möglichkeit muss also $\langle x,y \rangle = \mathrm{PSL}(2,p)$ sein, also nicht auflösbar.

Wir fassen zusammen:

$$\chi_{\mathrm{solv}}(x) = \frac{1}{2}p(p-1). \qquad \square$$

Als nächsten Schritt betrachten wir 3-Elemente.

**(3.20) Satz**
Es sei $x \in \mathrm{PSL}(2,p)$ von Ordnung 3. Dann gilt

$$\chi_{\mathrm{solv}}(x) = \begin{cases} (p+6)(p-1), & \text{für } p \equiv 1 \mod 3,\ p^2-1 \equiv 0 \mod 16, \\ (p+3)(p-1), & \text{für } p \equiv 1 \mod 3,\ p^2-1 \not\equiv 0 \mod 16, \\ 7(p+1), & \text{für } p \equiv 2 \mod 3,\ p^2-1 \equiv 0 \mod 16, \\ 4(p+1), & \text{für } p \equiv 2 \mod 3,\ p^2-1 \not\equiv 0 \mod 16. \end{cases}$$

**Beweis**
Gesucht ist die Anzahl der $y \in \mathrm{PSL}(2,p)$, so dass $\langle x,y\rangle$ eine echte Untergruppe von $\mathrm{PSL}(2,p)$ ist. Dann liegt diese Untergruppe aber insbesondere in einer maximalen Untergruppe von $\mathrm{PSL}(2,p)$, die wir in (3.10) vollständig bestimmt haben. Nach diesen möglichen maximalen Untergruppen machen wir eine Fallunterscheidung:

**1. Fall:** $D_{p-1}$ oder $D_{p+1}$
Nach der Partition (3.9)(a)(b) liegt $x$ in einer zyklischen Gruppe $H$ von Ordnung $\frac{p\pm1}{2}$. Weiter gilt, dass $N_{\mathrm{PSL}(2,p)}(\langle x\rangle)$ bereits vom Typ $D_{p-1}$ bzw. $D_{p+1}$ ist, je nach Kongruenz von $p$ modulo 3. Kann $x$ in einer anderen maximalen Untergruppe vom gesuchten Typ außer seinem Normalisator liegen? Ist $J = \langle s\rangle \ltimes \langle t\rangle \neq N_{\mathrm{PSL}(2,p)}(\langle x\rangle)$ mit $|s| = 2, |t| = \frac{p\pm1}{2}$ und $t^s = t^{-1}$, so kann $x$ wegen (3.9)(a)(b) nicht in der zyklischen Gruppe $\{1\} \ltimes \langle t\rangle$ liegen. Aber $x$ kann auch kein Element von $J \setminus (\{1\} \ltimes \langle t\rangle)$ sein, da diese Menge nur aus Involutionen besteht. Damit ist gezeigt, dass die einzige Diedergruppe des gesuchten Typs, in der $x$ liegen kann, $N_{\mathrm{PSL}(2,p)}(\langle x\rangle)$ ist. Demnach gibt es genau

$$\left|N_{\mathrm{PSL}(2,p)}(\langle x\rangle)\right| = p \pm 1$$

Elemente $y \in \mathrm{PSL}(2,p)$, so dass $\langle x,y\rangle$ in $D_{p\pm1}$ liegt.

**2. Fall:** $C_{\frac{p-1}{2}} \ltimes C_p$
Dieser Fall kann aus Ordnungsgründen nur für $p \equiv 1 \bmod 3$ eintreten. Es sei $\mathcal{U}$ die zu $x$ gehörige zyklische Untergruppe von Ordnung $\frac{p-1}{2}$. Zunächst beachte man, dass der Spezialfall $\langle x,y\rangle \leq C_{\frac{p-1}{2}} \ltimes \{1\}$ bereits durch den 1. Fall abgedeckt ist, denn $C_{\frac{p-1}{2}} \ltimes \{1\}$ wäre dann genau $\mathcal{U}$. Also suchen wir genau die $y$, so dass $\langle x,y\rangle$ in $C_{\frac{p-1}{2}} \ltimes C_p$, aber $\langle x,y\rangle \not\leq \mathcal{U}$. Wie jedes Element von $\mathcal{U}$ besitzt auch $x$ genau zwei Fixpunkte. Zu jedem dieser Fixpunkte existiert nach (3.8)(c) eine $p$-Sylow-Gruppe von $\mathrm{PSL}(2,p)$, die diesen fest lässt. Also operiert $\mathcal{U}$ auf diesen beiden $p$-Sylow-Gruppen durch Konjugation und sonst auf keiner anderen $p$-Sylow-Gruppe. Das Gruppenerzeugnis von $\mathcal{U}$ mit jeweils einer der beiden $p$-Sylow-Gruppen als semi-direktes Produkt erzeugt jeweils eine maximale Untergruppe vom Typ $C_{\frac{p-1}{2}} \ltimes C_p$, in denen $x$ liegt. Diese maximalen Untergruppen schneiden sich in $\mathcal{U}$, somit ist der Schnitt für die gesuchten $y$ uninteressant und wir können zusammenfassen, dass die Anzahl der $y \in \mathrm{PSL}(2,p)$ mit

$$\langle x,y\rangle \leq C_{\frac{p-1}{2}} \ltimes C_p$$

genau

$$\begin{aligned}
2 \cdot \left|\left(C_{\frac{p-1}{2}} \ltimes C_p\right) \setminus \mathcal{U}\right| &= 2 \cdot \left|\left\{(a,b) \in C_{\frac{p-1}{2}} \ltimes C_p \;\middle|\; b \neq 1\right\}\right| \\
&= 2 \cdot \frac{p-1}{2} \cdot (p-1) = (p-1)^2
\end{aligned}$$

entspricht.

**3. Fall:** $A_4$
Nach (3.15) und (3.18) gilt:

$$\begin{aligned}
\left|U_{x,A_4}\right| = {} & |\{U \leq \mathrm{PSL}(2,p) \mid U \cong A_4\}| \\
& \cdot \frac{|\{y \in A_4 \mid |y| = |x|,\ y \text{ ist } A_4\text{-Zweierzeuger}\}|}{|Cl(x)|} \\
= {} & \frac{|\mathrm{PSL}(2,p)|}{12} \cdot \frac{8}{|Cl(x)|},
\end{aligned}$$

denn jedes 3-Element in einer $A_4$ ist ein $A_4$-Zweierzeuger.

Wegen (3.11) gilt außerdem

$$|Cl(x)| = \frac{2 \cdot |\mathrm{PSL}(2,p)|}{\left|N_{\mathrm{PSL}(2,p)}\left(\langle x \rangle\right)\right|}.$$

Damit folgt

$$\left|U_{x,A_4}\right| = \frac{1}{3}\left|N_{\mathrm{PSL}(2,p)}\left(\langle x \rangle\right)\right|.$$

Es sei nun $U \in U_{x,A_4}$. Jedes $y \in U \setminus \langle x \rangle$ erzeugt mit $x$ zusammen wieder ganz $U$. Also gilt

$$|F_{x,U}| = (12 - 3) = 9$$

für alle $U \in U_{x,A_4}$. Aus (3.17) erhalten wir nun

$$\left|E_{x,A_4}\right| = \left|U_{x,A_4}\right| \cdot (12-3) = 9 \cdot \frac{1}{3}\left|N_{\mathrm{PSL}(2,p)}\left(\langle x \rangle\right)\right| = 3\left|N_{\mathrm{PSL}(2,p)}\left(\langle x \rangle\right)\right|.$$

**4. Fall:** $S_4$
Analog zum vorigen Fall ist

$$\left|U_{x,S_4}\right| = \frac{1}{3}\left|N_{\mathrm{PSL}(2,p)}\left(\langle x \rangle\right)\right|.$$

Es sei $y \in E_{x,S_4}$, d.h. $\langle x,y \rangle \cong S_4$. Wir zählen nun die Elemente aus $\langle x,y \rangle$, die zusammen mit $x$ wieder eine $S_4$ erzeugen. Als 3-Element hat $x$ positives Signum, also liegt jedes Gruppenerzeugnis mit einem weiteren Element positiven Signums in einer $A_4$. Es sei deshalb $z \in \langle x,y \rangle$ mit $\mathrm{sgn}(z) = -1$. Es existiert genau ein $a \in \{1,2,3,4\}$ mit $a^x = a$. Lässt nun auch $z$ diesen Punkt $a$ fest, so gilt bereits $\langle x,z \rangle \cong S_3$. Im anderen Fall ist $\langle x,z \rangle$ eine Gruppe der Ordnung größer oder gleich 6, jedoch weder zu $A_4$ noch zu $S_3$ isomorph. Damit gilt bereits $\langle x,z \rangle \cong S_4$. Es gilt also für $z \in \langle x,y \rangle$:

$$\langle x,z \rangle \cong S_4 \;\Leftrightarrow\; \mathrm{sgn}(z) = -1,\; \langle x,z \rangle \ncong S_3.$$

Da eine Untergruppe von $\langle x,z \rangle \cong S_4$ vom Typ $S_3$ genau drei Elemente negativen Signums enthält und $|S_4 \setminus A_4| = 12$ ist, gilt

$$\left|F_{x,\langle x,y \rangle}\right| = |S_4 \setminus (A_4 \cup S_3)| = 24 - (12+3) = 9,$$

und somit auch $|F_{x,U}| = 9$ für alle $U \in \mathcal{U}_{x,S_4}$. Damit ist nach (3.17)(b)

$$\left|E_{x,S_4}\right| = \left|\mathcal{U}_{x,S_4}\right| \cdot 9 = 3 \left|N_{\text{PSL}(2,p)}\left(\langle x\rangle\right)\right|.$$

**Zusammenfassung:**
Gilt $p \equiv 1 \bmod 3$, so ist $p-1$ durch 3 teilbar und $x$ liegt nach der Partition (3.9) in einer zyklischen Untergruppe von Ordnung $\frac{p-1}{2}$. Dann gilt $|N_{\text{PSL}}\left(\langle x\rangle\right)| = p-1$. Summiert man über die obigen Fälle erhält man

$$\chi_{\text{solv}}(x) = (p-1) + (p-1)^2 + 3(p-1) = (p+3)(p-1)$$

bzw.

$$\chi_{\text{solv}}(x) = (p-1) + (p-1)^2 + 3(p-1) + 3(p-1) = (p+6)(p-1)$$

je nach Kongruenz von $p^2 - 1 \bmod 16$.
Bei $p \equiv 2 \bmod 3$ hat man dagegen $\left|N_{\text{PSL}(2,p)}\left(\langle x\rangle\right)\right| = p+1$ und der zweite Fall kann nicht eintreten. Deswegen folgt hier

$$\chi_{\text{solv}}(x) = (p+1) + 3(p+1) = 4(p+1)$$

bzw.

$$\chi_{\text{solv}}(x) = (p+1) + 3(p+1) + 3(p+1) = 7(p+1). \qquad \square$$

**(3.21) Satz**
Es sei $x \in \text{PSL}(2, p)$ von Ordnung 4. Insbesondere ist also $p^2 - 1 \equiv 0 \mod 16$. Dann gilt

$$\chi_{\text{solv}}(x) = \begin{cases} (p+4)(p-1), & \text{für } p \equiv 1 \mod 4, \\ 5(p+1), & \text{für } p \equiv 3 \mod 4. \end{cases}$$

**Beweis**
Wie bei den 3-Elementen machen wir eine Fallunterscheidung nach den maximalen Untergruppen. Dabei lassen sich jedoch die Fälle "$D_{p\pm1}$" und "$C_{\frac{p-1}{2}} \ltimes C_p$" mit wortgleicher Argumentation wie im dortigen Beweis abhandeln:

**1. Fall:** $D_{p-1}$ oder $D_{p+1}$
Es gibt genau

$$\left|N_{\mathrm{PSL}(2,p)}\left(\langle x\rangle\right)\right| = p \pm 1$$

Elemente $y \in \mathrm{PSL}(2,p)$, so dass $\langle x,y\rangle$ in $D_{p\pm 1}$ liegt.

**2. Fall:** $C_{\frac{p-1}{2}} \ltimes C_p$
Dieser Fall tritt nur bei $p \equiv 1 \bmod 4$ auf, dann gibt es hier genau $(p-1)^2$ Elemente $y \in \mathrm{PSL}(2,p)$, so dass $\langle x,y\rangle$ in $D_{p\pm 1}$ liegt.

**3. Fall:** $A_4$
Eine Gruppe vom Typ $A_4$ enthält keine Elemente der Ordnung 4, somit kann dieser Fall nie eintreten.

**4. Fall:** $S_4$
Man rechnet leicht nach, dass jedes der sechs 4-Elemente in $S_4$ ein $S_4$-Zweierzeuger ist. Wegen (3.11) gilt außerdem

$$|Cl(x)| = \frac{2 \cdot |\mathrm{PSL}(2,p)|}{\left|N_{\mathrm{PSL}(2,p)}\left(\langle x\rangle\right)\right|}.$$

Dann ergibt sich zunächst mit (3.15) und (3.18):

$$\left|U_{x,S_4}\right| = \frac{1}{4}\left|N_{\mathrm{PSL}(2,p)}\left(\langle x\rangle\right)\right|.$$

Weiter verifiziert man z.B. mit GAP, dass es zu jedem 4-Element in einer $S_4$ genau 16 Elemente gibt, die jeweils wieder die ganze Gruppe erzeugen, d.h. $|F_{x,U}| = 16$ für alle $U \in U_{x,S_4}$. Aus (3.17) folgt dann

$$\left|E_{x,S_4}\right| = 4\left|N_{\mathrm{PSL}(2,p)}\left(\langle x\rangle\right)\right|.$$

**Zusammenfassung:**
Gilt $p \equiv 1 \bmod 4$, so ist $p-1$ durch 4 teilbar und $x$ liegt nach der Partition (3.9) in einer zyklischen Untergruppe von Ordnung $\frac{p-1}{2}$. Dann gilt $|N_{\mathrm{PSL}}\left(\langle x\rangle\right)| = p-1$.

Summiert man über die obigen Fälle, erhält man

$$\chi_{\text{solv}}(x) = (p-1) + (p-1)^2 + 4(p-1) = (p+4)(p-1).$$

Bei $p \equiv 3 \bmod 4$ hat man dagegen $\left|N_{\mathrm{PSL}(2,p)}\left(\langle x\rangle\right)\right| = p+1$ und der zweite Fall kann nicht eintreten. Deswegen folgt hier

$$\chi_{\text{solv}}(x) = (p+1) + 4(p+1) = 5(p+1). \qquad \square$$

### 3.3.4 Elemente der Ordnung 2

Als nächstes wollen wir 2-Elemente untersuchen. Auch wird wieder die Erzeugung einer $A_4$ oder einer $S_4$ zentraler Gegenstand unserer Untersuchungen sein. Wir beginnen jedoch zunächst mit einer Untergruppe von $A_4$.

**(3.22) Lemma**
Es sei $x \in \mathrm{PSL}(2,p)$ von Ordnung 2. Setze $N := N_{\mathrm{PSL}(2,p)}\left(\langle x\rangle\right)$. Nach der Partition (3.9)(3) existiert eine eindeutig bestimmte zyklische Gruppe $H$ der Ordnung $\frac{1}{2}|N|$ mit $x \in H$. Dann gilt für ein $y \in \mathrm{PSL}(2,p)$:

$$\langle x, y\rangle \cong C_2 \times C_2 \;\Leftrightarrow\; y \in N \setminus H.$$

**Beweis**
Wegen $x^{-1} = x$ ist $N = C_{\mathrm{PSL}(2,p)}\left(x\right)$. Außerdem folgern wir

$$\begin{aligned}\langle x, y\rangle \cong C_2 \times C_2 &\Leftrightarrow\; |y| = 2 \text{ und } xy = yx \Leftrightarrow\; |y| = 2 \text{ und } y \in C_{\mathrm{PSL}(2,p)}\left(x\right)\\ &\Leftrightarrow\; |y| = 2 \text{ und } y \in N.\end{aligned}$$

Als zyklische Gruppe besitzt $H$ genau ein Element der Ordnung 2, dieses ist nach Voraussetzung gerade x. Nach (3.9) gilt $H \leq N$. Deswegen können wir die Äquivalenz präzisieren auf

$$\langle x, y\rangle \cong C_2 \times C_2 \;\Leftrightarrow\; |y| = 2 \text{ und } y \in N \setminus H.$$

Durch (3.9) wissen wir außerdem, dass $N$ eine Diedergruppe von Ordnung $p \pm 1$

ist. Also können wir $N$ schreiben als

$$N = \langle s \rangle \ltimes \langle t \rangle$$

mit $|s| = 2, |t| = \frac{p \pm 1}{2}$ und $t^s = t^{-1}$. Ein $y \in N \setminus H$ hat dann die Form $y = (s,\ t^n)$ mit $n \in \mathbb{Z}$. Damit gilt:

$$\begin{aligned} y^2 &= (s,\ t^n) \cdot (s,\ t^n) = \left(s \cdot s,\ (t^n)^s \cdot t^n\right) = \left(1,\ (t^n)^{-1} \cdot t^n\right) \\ &= (1,\ 1) \qquad\qquad = 1. \end{aligned}$$

Also ist bereits jedes Element aus $N \setminus H$ eine Involution. Damit ergibt sich die Behauptung. □

**(3.23) Satz**

Es sei $x \in \mathrm{PSL}(2, p)$ von Ordnung 2. Dann existieren genau

$$(p-3) \cdot \left| N_{\mathrm{PSL}(2,p)} \left( \langle x \rangle \right) \right|$$

Elemente $y \in \mathrm{PSL}(2, p)$, so dass $\langle x, y \rangle$ eine nicht-abelsche Untergruppe einer Diedergruppe vom Typ $D_{p-1}$ oder $D_{p+1}$ ist.

**Beweis**

Wir setzen $N := N_{\mathrm{PSL}(2,p)} \left( \langle x \rangle \right)$ und unterscheiden zwei Fälle:

**1. Fall:** $|y| = 2$

Gilt $|y| = 2$, so ist $\langle x, y \rangle$ nach Definition eine Diedergruppe. Deshalb ist

$$y \notin C_{\mathrm{PSL}(2,p)} \left( x \right) = N.$$

Setzen wir weiter $d := xy$, so gilt

$$d^x = yx = y^{-1}x^{-1} = (xy)^{-1} = d^{-1}$$

und deswegen ist $\langle d \rangle$ normal in $\langle x, y \rangle$. Nun kann $x$ kein Element von $\langle d \rangle$ sein, sonst wäre $\langle x, y \rangle = \langle d \rangle$ zyklisch. Also gilt

$$\langle x, y \rangle \cong \langle x \rangle \ltimes \langle d \rangle \,,$$

woraus

$$|\langle x,y\rangle| = |x|\cdot|d| = 2\cdot|xy|$$

folgt. Da also $\langle x,y\rangle$ eine Untergruppe einer Diedergruppe vom Typ $D_{p-1}$ oder $D_{p+1}$ ist, ist die Ordnung von $xy$ ein Teiler von $\frac{p-1}{2}$ oder $\frac{p+1}{2}$. Nach der Partition (3.9)(3) bedeutet das gerade, dass $|xy| \neq p$ ist. Es gilt:

$$\begin{aligned}|\{(y,z) \mid |y|=2,\ |z|=p,\ xy=z\}| &= |\{(y,z) \mid |y|=2,\ |z|=p,\ zy=x\}| \\ &= |\{(z,y)) \mid |y|=2,\ |z|=p,\ zy=x\}| \\ &= 2\cdot a_{p22},\end{aligned}$$

wobei $a_{p22}$ die Strukturkonstante von PSL$(2,p)$ bzgl. der zu $x$ und $p$-Elementen gehörigen Konjugiertenklassen bezeichnet. Der Faktor 2 ergibt sich daraus, dass zwei Konjugiertenklassen von $p$-Elementen existieren.

Wieviele 2-Elemente besitzt $N$?
Nach der Partition (3.9)(3) existiert eine eindeutige zyklische Gruppe

$$H = \langle h\rangle,\ |H| = \frac{1}{2}\cdot|N|$$

und $x \in H$. Damit gilt

$$N \cong \langle s\rangle \ltimes \langle h\rangle.$$

Nach [Con07, Example 2.3] existieren genau $|H|$ Elemente der Ordnung 2, die keine Potenz von $h$ sind. Da $|H|$ gerade Ordnung besitzt und zyklisch ist, existiert genau ein Element in $H$, das eine Involution ist. Insgesamt besitzt $N$ also $|H|+1 = \frac{|N|+2}{2}$ Elemente der Ordnung 2. Multipliziert man ein beliebiges dieser Elemente mit $x$, so besitzt das entstehende Produkt nicht die Ordnung $p$, denn die Ordnung von $N$ ist nicht durch $p$ teilbar. Daher wurden die $\frac{|N|+2}{2}$ Involutionen von $N$ nicht durch die Strukturkonstanten weiter oben abgedeckt.

Zusammengefasst ergibt sich mit (3.13) also für die gesuchte Anzahl der $y \in$ PSL$(2,p)$ der Ordnung 2:

$$\left|x^{\mathrm{PSL}(2,p)}\right| - \frac{|N|+2}{2} - 2\cdot a_{p22} = \begin{cases} \frac{p^2-4p+3}{2}, & \text{für } p \equiv 1 \bmod 4 \\ \frac{p^2-2p-3}{2}, & \text{für } p \equiv 3 \bmod 4 \end{cases}$$

**2. Fall:** $|y| > 2$
Ist $\langle x, y\rangle$ eine Diedergruppe, so schreiben wir zunächst

$$\langle x,y\rangle = \langle x\rangle \ltimes \langle z\rangle$$

für ein $z \in \langle x, y\rangle$. Nach [Con07, Theorem 2.4] hat $y$ eine Darstellung

$$y = x^n z^m, \quad n \in \{0,1\}, \; m \in \mathbb{Z}, \; y \neq x.$$

Wir nehmen an, dass $n = 1$ ist. Dann gilt mit [Con07, Theorem 2.2]

$$y^2 = xz^m xz^m = (z^m)^{-1} z^m = 1$$

im Widerspruch zu Vorraussetzung. Also können wir $n = 0$ annehmen. Somit gilt $y^x = y^{-1}$, also $|xy| = 2$. Wir fassen alle im 1. Fall gefundenen Elemente $y$ von Ordnung 2, die mit $x$ eine nicht-abelsche Untergruppe einer Diedergruppe vom Typ $D_{p-1}$ oder $D_{p+1}$ erzeugen, zu einer Menge $B$ zusammen. Weiter bezeichnet $A$ die Menge der $y$, die wir in diesem Fall suchen. Wir geben nun eine Bijektion zwischen $A$ und $B$ an, um zu zeigen, dass beide Mengen gleichmächtig sind:
Definiere

$$f: \; A \to B, \; y \mapsto xy$$

Da gerade gezeigt wurde, dass $|xy| = 2$ für alle $y \in B$ und da $\langle x, y\rangle = \langle x, xy\rangle$ ist, ist $f$ eine wohldefinierte Abbildung. Weiter ist

$$g: \; B \to A, \; z \mapsto xz$$

ebenfalls wohldefiniert. Denn nimmt man an, dass $|xz| = 2$ gilt, so ist dies äquivalent zu $xz = zx$, da $x$ und $z$ Involutionen sind. Infolgedessen ist $\langle x, z\rangle$ abelsch und dies liefert den Widerspruch $z \notin B$. Außerdem gilt wieder $\langle x, z\rangle = \langle x, xz\rangle$, was die Wohldefiniertheit zeigt. Offensichtlich gilt $g = f^{-1}$ und somit ist $|A| = |B|$. Nun ergibt sich die Gesamtanzahl der gesuchten Elemente $y$ durch

$$\begin{aligned} 2 \cdot \frac{p^2 - 4p + 3}{2} &= p^2 - 4p + 3 \qquad &= (p-3)(p-1), \text{ für } p \equiv 1 \bmod 4 \\ 2 \cdot \frac{p^2 - 2p - 3}{2} &= p^2 - 2p - 3 \qquad &= (p-3)(p+1), \text{ für } p \equiv 3 \bmod 4 \end{aligned}$$

oder kurz $(p-3) \cdot |N|$. $\square$

**(3.24) Satz**
Es sei $x \in \mathrm{PSL}(2,p)$ von Ordnung 2. Dann gilt

$$\chi_{\mathrm{solv}}(x) = \begin{cases} (2p+3)(p-1), & \text{für } p \equiv 1 \mod 4,\ p^2-1 \equiv 0 \mod 16, \\ (2p-1)(p-1), & \text{für } p \equiv 1 \mod 4,\ p^2-1 \not\equiv 0 \mod 16, \\ (p+4)(p+1), & \text{für } p \equiv 3 \mod 4,\ p^2-1 \equiv 0 \mod 16, \\ p(p+1), & \text{für } p \equiv 3 \mod 4,\ p^2-1 \not\equiv 0 \mod 16. \end{cases}$$

**Beweis**
Wir setzen $N := N_{\mathrm{PSL}(2,p)}(\langle x \rangle)$. Es sei $H$ die eindeutig bestimmte zyklische Gruppe von Ordnung $\frac{1}{2} \cdot |N|$, die $x$ enthält. Wie in (3.20) ist die Anzahl der $y \in \mathrm{PSL}(2,p)$ gesucht, für die $\langle x,y \rangle$ eine echte Untergruppe von $\mathrm{PSL}(2,p)$ erzeugen. Dann liegt diese Untergruppe in einer maximalen Untergruppe von $\mathrm{PSL}(2,p)$. Nach den möglichen maximalen Untergruppen machen wir eine Fallunterscheidung:

**1. Fall:** $D_{p-1}$ bzw. $D_{p+1}$
Nach [Con08, Theorem 4.1] ist jede Untergruppe einer Diedergruppe entweder zyklisch oder wieder eine Diedergruppe. Nach diesen Möglichkeiten unterscheiden wir:

(a) **Zyklische Untergruppen**
Ist $\langle x,y \rangle$ zyklisch, dann kommutieren insbesondere $x$ und $y$. Also gilt $y \in C_{\mathrm{PSL}(2,p)}(x) = N$. Jede zyklische Untergruppe von $N$ liegt aber bereits in $H$. Also haben wir

$$\langle x,y \rangle \text{ zyklisch} \quad \Leftrightarrow \quad y \in H.$$

Dies ergibt $\frac{1}{2} \cdot |N|$ Möglichkeiten für $y$.

(b) **Diedergruppen**
Da $|x| = 2$ und $y \neq 1, x$ ist, hat $\langle x,y \rangle$ mindestens Ordnung 4. Nach [Con08, Theorem 1.2] ist eine Diedergruppe der Ordnung 4 abelsch, jede größere Diedergruppe ist nicht abelsch. Eine Diedergruppe von Ordnung 4 ist isomorph zu $C_2 \times C_2$. Die Anzahl der $y \in \mathrm{PSL}(2,p)$ mit $\langle x,y \rangle \cong C_2 \times C_2$ beträgt nach (3.22) genau $|N \setminus H| = \frac{1}{2} \cdot |N|$. Also müssen wir nur noch die $y$ finden, für die $\langle x,y \rangle$ eine nicht-abelsche Diedergruppe ist. Diese Anzahl wurde in (3.23) bestimmt und beträgt $(p-3) \cdot |N|$.

**2. Fall:** $C_{\frac{p-1}{2}} \ltimes C_p$
In Analogie zum entsprechenden Fall in (3.20) ist diese maximale Untergruppe nur für $p \equiv 1 \bmod 4$ möglich, und dann beträgt die Anzahl genau $(p-1)^2$.

**3. Fall:** $A_4$
Nach (3.15) und (3.18) gilt:

$$\begin{aligned}\left|U_{x,A_4}\right| &= |\{U \leq \mathrm{PSL}(2,p) \mid U \cong A_4\}| \\ &\quad \cdot \frac{|\{y \in A_4 \mid |y| = 2,\ y \text{ ist ein } A_4\text{-Zweierzeuger}\}|}{|Cl(x)|} \\ &= \frac{|\mathrm{PSL}(2,p)|}{12} \cdot \frac{3}{|Cl(x)|},\end{aligned}$$

denn jedes 2-Element in einer $A_4$ ist ein $A_4$-Zweierzeuger.
Wegen (3.11) gilt außerdem $|Cl(x)| = \frac{|\mathrm{PSL}(2,p)|}{\left|N_{\mathrm{PSL}(2,p)}(\langle x \rangle)\right|}$. Damit folgt

$$\left|U_{x,A_4}\right| = \frac{1}{4}\left|N_{\mathrm{PSL}(2,p)}\left(\langle x \rangle\right)\right|.$$

Es sei nun $U \in U_{x,A_4}$. Jedes $y \in U \setminus \langle x \rangle$ der Ordnung größer als 2 erzeugt mit $x$ zusammen wieder ganz $U$. Also gilt

$$|F_{x,U}| = (12-4) = 8$$

für alle $U \in U_{x,A_4}$. Aus (3.17)(b) erhalten wir nun

$$\left|E_{x,A_4}\right| = \left|U_{x,A_4}\right| \cdot 8 = 2\left|N_{\mathrm{PSL}(2,p)}\left(\langle x \rangle\right)\right|.$$

**4. Fall:** $S_4$
Wieder nutzen wir (3.15) und (3.18):

$$\begin{aligned}\left|U_{x,S_4}\right| &= |\{U \leq \mathrm{PSL}(2,p) \mid U \cong S_4\}| \cdot \frac{|\{y \in S_4 \mid |y| = 2,\ y \text{ ist ein } S_4\text{-Zweierzeuger}\}|}{|Cl(x)|} \\ &= \frac{|\mathrm{PSL}(2,p)|}{12} \cdot \frac{6}{|Cl(x)|},\end{aligned}$$

denn nur die sechs Zweizykel in einer $S_4$ sind $S_4$-Zweierzeuger der Ordnung 2, die Doppeltranspositionen sind es nicht. Aus (3.11) entnehmen wir $|Cl(x)| = \frac{|\mathrm{PSL}(2,p)|}{\left|N_{\mathrm{PSL}(2,p)}(\langle x\rangle)\right|}$. Damit folgt

$$\left|U_{x,A_4}\right| = \frac{1}{2}\left|N_{\mathrm{PSL}(2,p)}\left(\langle x\rangle\right)\right|.$$

Es sei nun $U \in U_{x,S_4}$. Man rechne z.B. mit GAP nach, dass jeder Zweizykel mit genau 8 weiteren Elementen in einer $S_4$ jeweils wieder eine $S_4$ erzeugt. Also gilt $|F_{x,U}| = 8$ für alle $U \in U_{x,S_4}$ und aus (3.17) erhalten wir nun

$$\left|E_{x,S_4}\right| = \left|U_{x,S_4}\right| \cdot 8 = 4\left|N_{\mathrm{PSL}(2,p)}\left(\langle x\rangle\right)\right|.$$

**Zusammenfassung:**
Wir addieren die Anzahlen der einzelnen Fälle auf. Gilt $p \equiv 1 \bmod 4,\ p^2 - 1 \not\equiv 0 \bmod 16$, so ist $|N| = p - 1$. Daher folgt

$$\begin{aligned}
\chi_{\text{solv}}(x) &= \frac{1}{2} \cdot |N| + \frac{1}{2} \cdot |N| + (p-3) \cdot |N| + (p-1)^2 + 2 \cdot |N| \\
&= (2p-1)\,|N| \\
&= (2p-1)(p-1).
\end{aligned}$$

Falls $p^2 - 1 \equiv 0 \bmod 16$ ist, kommt zusätzlich aus dem vierten Fall der Summand $4 \cdot |N|$ hinzu, was insgesamt

$$\chi_{\text{solv}}(x) = (2p+3)(p-1)$$

bedeutet. Im anderen Fall $p \equiv 3 \bmod 4$ ergibt sich analog

$$\begin{aligned}
\chi_{\text{solv}}(x) &= \frac{1}{2} \cdot |N| + \frac{1}{2} \cdot |N| + (p-3) \cdot |N| + 2 \cdot |N| \\
&= p\,|N| \\
&= p(p+1)
\end{aligned}$$

bzw.

$$\chi_{\text{solv}}(x) = (p+4)(p+1).$$

Das war zu zeigen. □

### 3.3.5 Elemente übriger Ordnung

Dass $\chi_{\text{solv}}(1) = |\text{PSL}(2, p)|$ gilt, ist offensichtlich. Es verbleiben noch die Elemente, deren Ordnung größer als 4 ist. Der folgende Satz deckt diese ab:

**(3.25) Satz**

Es sei $x \in \text{PSL}(2, p)$ mit $|x| > 4$.

(a) Ist die Ordnung von $x$ ein Teiler von $\frac{p+1}{2}$, so gilt $\chi_{\text{solv}}(x) = p + 1$.

(b) Ist die Ordnung von $x$ ein Teiler von $\frac{p-1}{2}$, so gilt $\chi_{\text{solv}}(x) = p(p-1)$.

**Beweis**

(a) Wegen der Ordnung von $x$, Satz (3.10) und der Partition (3.9)(3) liegt eine von $\text{PSL}(2, p)$ verschiedene Gruppe $\langle x, y\rangle$ in genau einer maximalen Untergruppe vom Typ $D_{p+1}$. Also ist $\langle x, y\rangle \neq \text{PSL}(2, p)$ genau für $y \in D_{p+1}$. Aus $|D_{p+1}| = p + 1$ folgt nun die Behauptung.

(b) Aus der Partition (3.9)(3) und der Ordnung von $x$ schließen wir, dass $x$ in einer zyklischen Untergruppe $\mathcal{U}$ von Ordnung $\frac{p-1}{2}$ liegt. Nach (3.9)(1) ist der Normalisator von $\mathcal{U}$ eine Diedergruppe der Ordnung $p - 1$, also eine maximale Untergruppe. Ebendort wird gezeigt, dass alle nicht-trivialen Elemente von $\mathcal{U}$ die gleichen zwei Fixpunkte haben. Zu jedem dieser beiden Fixpunkte existiert nach (3.8)(3) eine $p$-Sylow-Gruppe von $\text{PSL}(2, p)$, die diesen fest lässt. Der Normalisator der jeweiligen Sylow-Gruppe ist eine maximale Untergruppe vom Typ $C_{\frac{p-1}{2}} \ltimes C_p$. Ist also $\langle x, y\rangle$ eine echte Untergruppe, so liegt diese in einer der beiden gerade genannten maximalen Untergruppen. Nach diesen beiden Fällen unterscheiden wir nun: Offensichtlich ist $\langle x, y\rangle \leq D_{p-1}$ genau dann, wenn $y$ im Normalisator von $\mathcal{U}$, also in $D_{p-1}$ liegt. Das ergibt $p - 1$ Möglichkeiten für $y$. Wann liegt $\langle x, y\rangle$ in einer maximalen Untergruppe vom Typ $C_{\frac{p-1}{2}} \ltimes C_p$? Es gibt genau zwei maximale Untergruppen von solchem Typ, in denen $\langle x, y\rangle$ liegen kann. Diese werden durch die Fixpunkte von $x$ bestimmt. Gilt $y \in \mathcal{U}$, so ist zwar $\langle x, y\rangle \leq C_{\frac{p-1}{2}} \ltimes C_p$, jedoch gilt dann sogar $\langle x, y\rangle \leq \mathcal{U}$. Diese Elemente haben wir bereits gezählt. Also verbleiben noch die $y$, für die $\langle x, y\rangle$ eine Untergruppe von $C_{\frac{p-1}{2}} \ltimes C_p$ ist, aber keine Untergruppe von $\mathcal{U}$. Dies wird genau von den $(a, b) \in C_{\frac{p-1}{2}} \ltimes C_p$ geleistet, für die $b \neq 1$ ist. Für deren Anzahl ergibt sich:

$$|C_{\frac{p-1}{2}} \ltimes C_p| - |\{(a, 1) \mid a \in C_{\frac{p-1}{2}}\}| = p \cdot \frac{p-1}{2} - \frac{p-1}{2} = \frac{1}{2}(p-1)^2.$$

Da es zwei solcher maximalen Untergruppen gibt, erhält man noch genau ein weiteres Mal diese Anzahl. Aufsummiert sind dies $(p-1)^2$ Möglichkeiten. Insgesamt ist also $\langle x, y \rangle$ auflösbar für genau

$$(p-1) + (p-1)^2 = p(p-1)$$

Elemente $y \in \mathrm{PSL}(2,p)$. □

### 3.3.6 $\chi_{\mathrm{solv}}$ ist kein Charakter von PSL$(2,p)$

Wir kommen nun zum finalen Resultat dieses Abschnitts.

**(3.26) Satz**
Es sei $p \in \mathbb{P}$ mit $p^2 + 1 \equiv 0 \bmod 5$.
Dann ist $\chi_{\mathrm{solv}}$ kein Charakter von $\mathrm{PSL}(2,p)$.

**Beweis**
Mit (3.11), (3.19), (3.20), (3.24) und (3.25) sowie der Notation und den Charaktertafeln aus Anhang A rechnen wir das Skalarprodukt mit geeigneten irreduziblen Charakteren von $\mathrm{PSL}(2,p)$ aus. Seien dazu

$$x_2 \in Cl_2,\ x_3 \in Cl_3,\ x_4 \in Cl_4,\ x_{p_1} \in Cl_{p_1},\ x_{p_2} \in Cl_{p_2}$$

und

$$x_i \in Cl_{\frac{p-1}{2}}(i),\ x_j \in Cl_{\frac{p+1}{2}}(j).$$

Wir unterscheiden insgesamt acht Fälle, die sich wiederum jeweils nach den möglichen Kongruenzen von $p$ modulo 3 und 4 bzw. von $p^2-1$ modulo 16 aufspalten. Dabei fassen wir nach (3.11) die Ausnahmen für die Indizes $i$ bzw. $j$ der Konjugiertenklassen $Cl_{\frac{p-1}{2}}(i)$ bzw $Cl_{\frac{p+1}{2}}(j)$ in den Mengen $A_i$ bzw. $A_j$ zusammen. Außerdem betrachten wir die Indexmengen $D$ und $V$ aus (3.12), die die Konjugiertenklasse der 3- und 4-Elemente beschreiben.

**1. Fall:** $p \equiv 1 \bmod 4,\ p \equiv 1 \bmod 3,\ p^2 - 1 \not\equiv 0 \bmod 16$

Es gilt

$$\begin{aligned} A_i &= \left\{ \frac{p-1}{4}, \frac{p-1}{2}, \frac{3(p-1)}{4}, p-1 \right\}, \\ D\ &= \left\{ \frac{p-1}{3}, \frac{2(p-1)}{3}, \frac{p-1}{6}, \frac{5(p-1)}{6} \right\}. \end{aligned}$$

Es sei $\psi \in \operatorname{Irr}(\mathrm{PSL}(2,p))$ mit $\psi(1) = \frac{p+1}{2}$ beliebig. Damit gilt

$$\begin{aligned} (\chi_{\text{solv}}, \psi) = \frac{1}{|\mathrm{PSL}(2,p)|} \cdot \Bigg( & \chi_{\text{solv}}(1)\psi(1) + \left|Cl_{p_1}\right| \chi_{\text{solv}}(x_{p_1})\psi(x_{p_1}) \\ & + \left|Cl_{p_2}\right| \chi_{\text{solv}}(x_{p_2})\psi(x_{p_2}) \\ & + |Cl_2|\, \chi_{\text{solv}}(x_2)\psi(x_2) + |Cl_3|\, \chi_{\text{solv}}(x_3)\psi(x_3) \\ & + \sum_{\substack{i=1 \\ i \notin A_i}}^{p-1} \left| Cl_{\frac{p-1}{2}}(i) \right| \chi_{\text{solv}}(x_i)\psi(x_i) \\ & + \sum_{\substack{j=1 \\ j \notin A_j}}^{p+1} \left| Cl_{\frac{p+1}{2}}(j) \right| \chi_{\text{solv}}(x_j)\psi(x_j) \Bigg) \\ = \frac{1}{|\mathrm{PSL}(2,p)|} \cdot \Bigg( & |\mathrm{PSL}(2,p)|\, \frac{p+1}{2} + \frac{p^2-1}{2}\frac{p(p-1)}{2}\frac{1-\sqrt{p}}{2} \\ & + \frac{p^2-1}{2}\frac{p(p-1)}{2}\frac{1+\sqrt{p}}{2} \\ & + \frac{p(p+1)}{2}(2p-1)(p-1)(-1) \\ & + \frac{1}{4}\sum_{i \in D} p(p+1)(p+3)(p-1)(-1)^i \\ & + \frac{1}{4}\sum_{\substack{i=1 \\ i \notin A_i \cup D}}^{p-1} p(p+1)p(p-1)(-1)^i \Bigg) \end{aligned}$$

Jedes $i \in D$ ist gerade und deshalb haben wir $(-1)^i = 1$. Da $p$ eine ungerade Primzahl ist, ist $p-1$ gerade. Die Menge $\{1, \ldots, p-1\}$ enthält also gleichviele gerade wie ungerade Elemente. Die Ausnahmenmenge $A_i$ besteht aus genau zwei geraden und zwei ungeraden Elementen.
Zusammenfassend beinhaltet $\{1, \ldots, p-1\} \setminus (A_i \cup D)$ also vier ungerade Ele-

mente mehr als gerade Elemente. Es folgt:

$$\begin{aligned}(\chi_{\text{solv}}, \psi) &= \frac{p+1}{2} + \frac{p-1}{2} - (2p-1) + \frac{1}{4}2(p+3)4 + \frac{1}{4}(4 \cdot 2p(-1)) \\ &= -p+7\end{aligned}$$

**2. Fall:** $p \equiv 1 \bmod 4,\ p \equiv 2 \bmod 3,\ p^2 - 1 \not\equiv 0 \bmod 16$

Dieser Fall verläuft sehr ähnlich zum vorherigen. Es sei wieder $\psi \in \operatorname{Irr}(\mathrm{PSL}(2,p))$ mit $\psi(1) = \frac{p+1}{2}$ beliebig. Weiter ist hier

$$\begin{aligned}A_i &= \left\{\frac{p-1}{4}, \frac{p-1}{2}, \frac{3(p-1)}{4}, p-1\right\} \\ D &= \left\{\frac{p+1}{3}, \frac{2(p+1)}{3}, \frac{p+1}{6}, \frac{5(p+1)}{6}\right\}.\end{aligned}$$

und $A_i \cap D = \emptyset$ Dann gilt

$$\begin{aligned}(\chi_{\text{solv}}, \psi) = \frac{1}{|\mathrm{PSL}(2,p)|} \cdot \Bigg( &|\mathrm{PSL}(2,p)| \frac{p+1}{2} + \frac{p^2-1}{2}\frac{p(p-1)}{2}\frac{1-\sqrt{p}}{2} \\ &+ \frac{p^2-1}{2}\frac{p(p-1)}{2}\frac{1+\sqrt{p}}{2} \\ &+ \frac{p(p+1)}{2}(2p-1)(p-1)(-1) \\ &+ \frac{1}{4}\sum_{\substack{i=1\\ i\notin A_i}}^{p-1} p(p+1)p(p-1)(-1)^i + 0\Bigg).\end{aligned}$$

Im Gegensatz zum ersten Fall summiert man in der Summe über gleich viele gerade wie ungerade Indizes, wodurch sie wegfällt. Es verbleibt:

$$\begin{aligned}(\chi_{\text{solv}}, \psi) &= \frac{p+1}{2} + \frac{p-1}{2} - (2p-1) \\ &= -p+1.\end{aligned}$$

**3. Fall:** $p \equiv 3 \bmod 4,\ p \equiv 1 \bmod 3,\ p^2 - 1 \not\equiv 0 \bmod 16$

Hier gilt

$$A_i = \left\{ \frac{p-1}{2}, p-1 \right\} \quad \text{und} \quad D = \left\{ \frac{p-1}{3}, \frac{2(p-1)}{3}, \frac{p-1}{6}, \frac{5(p-1)}{6} \right\}.$$

Wir wählen ein $\psi_5(k) \in \operatorname{Irr}(\mathrm{PSL}(2,p))$ mit $\psi_5(k)(1) = p+1$. Im Verlauf dieses Falles werden wir die Wahl von $k$ noch konkretisieren. Zunächst rechnen wir allgemein

$$\begin{aligned}
(\chi_{\text{solv}}, \psi_5(k)) = \frac{1}{|\mathrm{PSL}(2,p)|} \cdot \Bigg( & |\mathrm{PSL}(2,p)|\,(p+1) + \frac{p^2-1}{2}\frac{p(p-1)}{2} \\
& + \frac{p^2-1}{2}\frac{p(p-1)}{2} + 0 \\
& + \frac{1}{4}\sum_{i \in D} p(p+1)(p+3)(p-1)\left(\zeta^{2ik} + \zeta^{-2ik}\right) \\
& + \frac{1}{4}\sum_{\substack{i=1 \\ i \notin A_i \cup D}}^{p-1} p(p+1)p(p-1)\left(\zeta^{2ik} + \zeta^{-2ik}\right) + 0 \Bigg) \\
= (p+1) + (p-1) + \frac{p+3}{2} & \sum_{i \in D} \zeta^{2ik} + \zeta^{-2ik} + \frac{p}{2} \sum_{\substack{i=1 \\ i \notin A_i \cup D}}^{p-1} \zeta^{2ik} + \zeta^{-2ik}.
\end{aligned}$$

Nun wähle $z \in \mathbb{N}$ mit $3^z \mid p-1,\ 3^{z+1} \nmid p-1$. Wir setzen $k := \frac{p-1}{3^z}$.
Damit gilt $\zeta^{2ik} = \epsilon_{3^z}^{-i}$. Da $i \in d$ durch $3^{z-1}$ teilbar ist, gilt $\zeta^{2ik} \in \left\{\epsilon_3, \epsilon_3^{-1}\right\}$ für alle $i \in D$. Das bedeutet

$$\sum_{i \in D} \zeta^{2ik} + \zeta^{-2ik} = 4(-1) = -4.$$

Desweiteren gilt $3^z \mid i$ für alle $i \in A_i$. Damit können wir die letzte Summe ausrechnen:

$$\begin{aligned}
\sum_{\substack{i=1 \\ i \notin A_i \cup D}}^{p-1} \zeta^{2ik} + \zeta^{-2ik} &= \sum_{\substack{i=1 \\ i \notin A_i \cup D}}^{p-1} \epsilon_{3^z}^{i} + \epsilon_{3^z}^{-i} \\
&= \sum_{i=1}^{p-1} \epsilon_{3^z}^{i} + \epsilon_{3^z}^{-i} - \sum_{i \in D} \epsilon_{3^z}^{i} + \epsilon_{3^z}^{-i} - \sum_{i \in A_i} \epsilon_{3^z}^{i} + \epsilon_{3^z}^{-i}
\end{aligned}$$

$$\begin{aligned} &= 0 - (-4) - |A_i| \cdot 2 \\ &= 0. \end{aligned}$$

Somit vereinfacht sich die Gesamtrechnung zu:

$$\begin{aligned} (\chi_{\mathrm{solv}}, \psi_5(k)) &= (p+1) + (p-1) + \frac{p+3}{2}(-4) + 0 \\ &= -6. \end{aligned}$$

**4. Fall:** $p \equiv 3 \bmod 4,\ p \equiv 2 \bmod 3,\ p^2 - 1 \not\equiv 0 \bmod 16$

Dieser Fall verläuft sehr ähnlich zum dritten Fall. Zunächst wählen wir einen irreduziblen Charakter $\psi_6(l) \in \mathrm{Irr}\,(\mathrm{PSL}(2,p))$ mit $\psi_6(l)(1) = p-1$. Es gilt

$$\begin{aligned} A_j &= \left\{ \frac{p+1}{4}, \frac{p+1}{2}, \frac{3(p+1)}{4}, p+1 \right\} \\ D &= \left\{ \frac{p+1}{3}, \frac{2(p+1)}{3}, \frac{p+1}{6}, \frac{5(p+1)}{6} \right\} \end{aligned}$$

und wir rechnen

$$\begin{aligned} (\chi_{\mathrm{solv}}, \psi_6(l)) = \frac{1}{|\mathrm{PSL}(2,p)|} \cdot \Bigg( &|\mathrm{PSL}(2,p)|\,(p-1) + \frac{p^2-1}{2}\frac{p(p-1)}{2}(-1) \\ &+ \frac{p^2-1}{2}\frac{p(p-1)}{2}(-1) \\ &+ \frac{(p-1)p}{2} p(p+1) \left( -(-1)^l - (-1)^{-l} \right) + 0 \\ &+ \frac{1}{4} \sum_{j \in D} p(p-1) \left( -\xi^{2jl} - \xi^{-2jl} \right) 4(p+1) \\ &+ \frac{1}{4} \sum_{\substack{j=1 \\ j \notin A_j \cup D}}^{p+1} p(p-1) \left( -\xi^{2jl} - \xi^{-2jl} \right)(p+1) \Bigg) \\ = (p-1) - (p-1) + (-p) &\left( (-1)^l + (-1)^{-l} \right) \\ &- 2 \sum_{j \in D} \left( \xi^{2jl} + \xi^{-2jl} \right) - \frac{1}{2} \sum_{\substack{j=1 \\ i \notin A_j \cup D}}^{p+1} \left( \xi^{2jl} + \xi^{-2jl} \right) \end{aligned}$$

Nun sei wieder $z \in \mathbb{N}$ mit $3^z \mid p+1$ und $3^{z+1} \nmid p+1$. Wir setzen $l := \frac{p+1}{3^z}$ und folgern $\zeta^{2jl} = \epsilon_{3^z}^{-j}$. Wegen $3^{z-1} \mid j$ für alle $j \in D$ schließen wir, dass $\zeta^{2jl} \in \left\{\epsilon_3, \epsilon_3^{-1}\right\}$ für $j \in D$ ist. Wir haben damit

$$\sum_{j \in D} \left(\zeta^{2jl} + \zeta^{-2jl}\right) = \sum_{j \in D} -1 = -4$$

und wegen $3^z \mid j$ für jedes $j \in A_j$ außerdem

$$\begin{aligned}
\sum_{\substack{j=1 \\ j \notin A_j \cup D}}^{p+1} \zeta^{2jl} + \zeta^{-2jl} &= \sum_{\substack{j=1 \\ j \notin A_j \cup D}}^{p+1} \epsilon_{3^z}^{j} + \epsilon_{3^z}^{-j} \\
&= \sum_{j=1}^{p+1} \epsilon_{3^z}^{j} + \epsilon_{3^z}^{-j} - \sum_{j \in D} \epsilon_{3^z}^{j} + \epsilon_{3^z}^{-j} - \sum_{j \in A_j} \epsilon_{3^z}^{j} + \epsilon_{3^z}^{-j} \\
&= 0 - (-4) - \left|A_j\right| \cdot 2 \\
&= -4.
\end{aligned}$$

Mit $2 \mid l$ folgt schließlich

$$\begin{aligned}
(\chi_{\text{solv}}, \psi_6(l)) &= (p-1) - (p-1) + (-p)\,(1+1) - 2(-4) - \frac{1}{2}(-4) \\
&= -2p + 10
\end{aligned}$$

**5. Fall:** $p \equiv 1 \bmod 4,\ p \equiv 1 \bmod 3,\ p^2 - 1 \equiv 0 \bmod 16$

Zunächst gilt

$$\begin{aligned}
A_i &= \left\{\frac{p-1}{4}, \frac{p-1}{2}, \frac{3(p-1)}{4}, p-1\right\}, \\
V\ &= \left\{\frac{p-1}{8}, \frac{3(p-1)}{8}, \frac{5(p-1)}{8}, \frac{7(p-1)}{8}\right\}, \\
D\ &= \left\{\frac{p-1}{3}, \frac{2(p-1)}{3}, \frac{p-1}{6}, \frac{5(p-1)}{6}\right\}.
\end{aligned}$$

Es sei $\psi_5(k) \in \operatorname{Irr}(\mathrm{PSL}(2,p))$ mit $\psi_5(k)(1) = p+1$. Dann gilt:

$$\begin{aligned}
(\chi_{\text{solv}}, \psi_5(k)) = \frac{1}{|\mathrm{PSL}(2,p)|} \cdot \Bigg( & |\mathrm{PSL}(2,p)|\,(p+1) + \frac{p^2-1}{2}\frac{p(p-1)}{2} \\
& + \frac{p^2-1}{2}\frac{p(p-1)}{2} \\
& + \frac{p(p+1)}{2} p(2p+3)(p-1)\left((-1)^k + (-1)^{-k}\right) \\
& + p(p+1)(p+6)(p-1)\left(\omega^k + \omega^{-k}\right) \\
& + p(p+1)(p+4)(p-1)\left(\tau^k + \tau^{-k}\right) \\
& + \frac{1}{4} \sum_{\substack{i=1 \\ i \notin A_i \cup D \cup V}}^{p-1} p(p+1)p(p-1)\left(\zeta^{2ik} - \zeta^{-2ik}\right)\Bigg) \\
= (p+1) - (p-1) + (2p+3) & \left((-1)^k + (-1)^{-k}\right) \\
& + 2(p+6)\left(\omega^k + \omega^{-k}\right) + 2(p+4)\left(\tau^k + \tau^{-k}\right) \\
& + \frac{p}{2} \sum_{\substack{i=1 \\ i \notin A_i \cup D \cup V}}^{p-1} \zeta^{2ik} - \zeta^{-2ik}
\end{aligned}$$

Es seien $n, m \in \mathbb{N}$ mit $2^n, 3^m \mid p-1$, aber $2^{n+1}, 3^{m+1} \nmid p-1$. Wir setzen nun $k := \frac{p-1}{2^n 3^m}$. Unmittelbar folgt:

$$(-1)^k + (-1)^{-k} = -2, \quad \omega^k + \omega^{-k} = -1, \quad \tau^k + \tau^{-k} = 0$$

und $\zeta^{2ik} = (\epsilon_{2^n 3^m})^{2i}$. Für $i \in A_i, V, D$ rechnen wir diese Einheitswurzel nun aus:

$$\begin{aligned}
\zeta^{2ik} &= (\epsilon_{2^n 3^m})^{2i} = 1 \ \text{ für } \quad i = \frac{p-1}{2}, p-1 \\
\zeta^{2ik} &= -1 \qquad\qquad\quad \text{ für } \quad i = \frac{p-1}{4}, \frac{3(p-1)}{4}
\end{aligned}$$

Dies bedeutet $\sum_{i \in A_i} \zeta^{2ik} + \zeta^{-2ik} = 0$.

$$\begin{aligned}
\zeta^{2ik} &= \tau \quad\ \ \text{für} \quad i = \frac{p-1}{8}, \frac{5(p-1)}{8} \\
\zeta^{2ik} &= \tau^{-1} \ \text{für} \quad i = \frac{3(p-1)}{8}, \frac{7(p-1)}{8}
\end{aligned}$$

Somit hat man $\sum_{i\in V} \zeta^{2ik} + \zeta^{-2ik} = 0$.

$$\begin{aligned}
\zeta^{2ik} &= \omega^{-k} \quad \text{für} \quad i = \frac{p-1}{3}, \frac{5(p-1)}{6} \\
\zeta^{2ik} &= \omega^{k} \quad\ \ \text{für} \quad i = \frac{2(p-1)}{3}, \frac{p-1}{6}
\end{aligned}$$

Da $3 \nmid k$ bedeutet dies $\sum_{i\in D} \zeta^{2ik} + \zeta^{-2ik} = |D| \cdot (-1) = -4$.
Nun lässt sich für das Skalarprodukt der letzte Summand bestimmen:

$$\begin{aligned}
\sum_{\substack{i=1 \\ i\notin A_i\cup D\cup V}}^{p-1} \zeta^{2ik} - \zeta^{-2ik} &= \sum_{i=1}^{p-1} \zeta^{2ik} - \zeta^{-2ik} - \sum_{i\in A_i} \zeta^{2ik} - \zeta^{-2ik} \\
&\quad - \sum_{i\in D} \zeta^{2ik} - \zeta^{-2ik} - \sum_{i\in V} \zeta^{2ik} - \zeta^{-2ik} \\
&= 0 - 0 - (-4) - 0 \\
&= 4
\end{aligned}$$

Somit gilt schließlich:

$$\begin{aligned}
(\chi_{\text{solv}}, \psi_5(k)) &= 2p - 2(2p+3) - 2(p+6) + 0 + \frac{p}{2} \cdot 4 \\
&= -2p - 18
\end{aligned}$$

**6. Fall:** $p \equiv 1 \bmod 4,\ p \equiv 2 \bmod 3,\ p^2 - 1 \equiv 0 \bmod 16$

Zunächst gilt

$$A_j = \left\{ \frac{p+1}{2}, p+1 \right\} \quad \text{und} \quad D = \left\{ \frac{p+1}{3}, \frac{2(p+1)}{3}, \frac{p+1}{6}, \frac{5(p+1)}{6} \right\}.$$

Es sei $\psi_6(l) \in \operatorname{Irr}(\mathrm{PSL}(2,p))$ mit $\psi_6(l)(1) = p - 1$. Dann gilt:

$$\begin{aligned}
(\chi_{\text{solv}}, \psi_6(l)) = \frac{1}{|\mathrm{PSL}(2,p)|} \cdot \Bigg( &|\mathrm{PSL}(2,p)|\,(p-1) + \frac{p^2-1}{2}\frac{p(p-1)}{2}(-1) \\
&+ \frac{p^2-1}{2}\frac{p(p-1)}{2}(-1) + 0 \\
&+ p(p-1)7(p+1)\left(-\omega^k - \omega^{-k}\right) + 0 + 0
\end{aligned}$$

$$+\frac{1}{4}\sum_{\substack{j=1\\ j\notin A_j\cup D}}^{p+1} p(p-1)(p+1)\left(-\zeta^{2jl}-\zeta^{-2jl}\right)\Bigg)$$

$$=-14\left(\omega^k+\omega^{-k}\right)-\frac{1}{2}\sum_{\substack{j=1\\ j\notin A_j\cup D}}^{p+1}\zeta^{2jl}+\zeta^{-2jl}$$

Es sei $l=3$. Nach Anhang A ist $l\neq\frac{p+1}{2}$. Damit gilt $\omega^l+\omega^{-l}=1+1=2$ und für jedes $j\in A_j\cup D$ ist $\xi^{2jl}=1$. Es ergibt sich

$$\begin{aligned}\sum_{\substack{j=1\\ j\notin A_j\cup D}}^{p+1}\xi^{2jl}-\xi^{-2jl} &= \sum_{j=1}^{p+1}\xi^{2jl}-\xi^{-2jl}-\sum_{j\in A_j}\xi^{2jl}-\xi^{-2jl}-\sum_{j\in D}\xi^{2jl}-\xi^{-2jl}\\ &= 0-(1+1)\cdot|A_j|-(1+1)\cdot|D|\\ &= -12\end{aligned}$$

und schließlich

$$(\chi_{\text{solv}},\,\psi_6(l))=-14\cdot 2-\frac{1}{2}\cdot(-12)=-22$$

**7. Fall:** $p\equiv 3 \bmod 4,\ p\equiv 1 \bmod 3,\ p^2-1\equiv 0 \bmod 16$

Es gilt

$$A_j=\left\{\frac{p+1}{4},\frac{p+1}{2},\frac{3(p+1)}{4},p+1\right\}$$

und

$$V=\left\{\frac{p+1}{8},\frac{3(p+1)}{8},\frac{5(p+1)}{8},\frac{7(p+1)}{8}\right\},$$

weiter wählen wir $\psi\in\operatorname{Irr}(\mathrm{PSL}(2,p))$ mit $\psi(1)=\frac{p-1}{2}$. Zunächst folgt:

$$\begin{aligned}(\chi_{\text{solv}},\,\psi)=\frac{1}{|\mathrm{PSL}(2,p)|}\cdot\Bigg(&|\mathrm{PSL}(2,p)|\,\frac{p-1}{2}+\frac{p^2-1}{2}\frac{p(p-1)}{2}\frac{-1+\sqrt{-p}}{2}\\ &+\frac{p^2-1}{2}\frac{p(p-1)}{2}\frac{-1-\sqrt{-p}}{2}\\ &+\frac{(p-1)p}{2}(-1)(p+4)(p+1)+0\end{aligned}$$

$$
\begin{aligned}
&\quad + \left(-(-1)^{\frac{p+1}{8}}\right) + 0 \\
&\quad + \frac{1}{4} \sum_{\substack{j=1 \\ j \notin A_j \cup V}}^{p+1} (p+1)p(p-1)\left(-(-1)^{\frac{p+1}{8}}\right)\Bigg) \\
&= \frac{p-1}{2} - \frac{p-1}{2} - (p+4) - 10(-1)^{\frac{p+1}{8}} - \frac{1}{2} \sum_{\substack{j=1 \\ j \notin A_j \cup V}}^{p+1} (-1)^{\frac{p+1}{8}} \\
&= -p - 4 - 10(-1)^{\frac{p+1}{8}} - \frac{1}{2} \sum_{\substack{j=1 \\ j \notin A_j \cup V}}^{p+1} (-1)^{\frac{p+1}{8}}
\end{aligned}
$$

Nun ist eine Fallunterscheidung nötig, da $\frac{p+1}{8}$ entweder gerade oder ungerade ist.

1. $16 \mid p+1$
   Zunächst folgt hier, dass $(-1)^{\frac{p+1}{8}} = 1$ ist und dass $V$ ausschließlich gerade ganze Zahlen enthält. Außerdem sind die Elemente in $A_j$ allesamt gerade. Das bedeutet, dass die Menge $\{1, \dots, p\} \setminus \left(A_j \cup V\right)$ genau 8 ungerade Zahlen mehr enthält als gerade. Für die obige Summe bedeutet das:

   $$\frac{1}{2} \sum_{\substack{j=1 \\ j \notin A_j \cup V}}^{p+1} (-1)^{\frac{p+1}{8}} = \frac{1}{2} \cdot 8 \cdot (-1) = -4$$

   Insgesamt vereinfacht sich das Skalarprodukt zu

   $$(\chi_{\text{solv}}, \psi) = -p - 4 - 10 + 4 = -p - 10.$$

2. $16 \nmid p+1$
   Hier gilt $(-1)^{\frac{p+1}{8}} = -1$, und $V$ enthält ausschließlich ungerade Zahlen. Die Menge $A_j$ besteht weiterhin aus geraden Elementen. Da $V$ und $A_j$ gleichmächtig sind, besitzt in diesem Fall $\{1, \dots, p\} \setminus \left(A_j \cup V\right)$ gleich viele gerade wie ungerade Elemente. Somit gilt

   $$\frac{1}{2} \sum_{\substack{j=1 \\ j \notin A_j \cup V}}^{p+1} (-1)^{\frac{p+1}{8}} = 0,$$

es folgt daher

$$(\chi_{\text{solv}}, \psi) = -p - 4 + 10 + 0 = -p - 6.$$

**8. Fall:** $p \equiv 3 \bmod 4,\ p \equiv 2 \bmod 3,\ p^2 - 1 \equiv 0 \bmod 16$

Dieser Fall verhält sich ähnlich wie der vorige Fall. Zunächst haben wir

$$\begin{aligned} A_j &= \left\{ \frac{p+1}{4}, \frac{p+1}{2}, \frac{3(p+1)}{4}, p+1 \right\}, \\ V\ &= \left\{ \frac{p+1}{8}, \frac{3(p+1)}{8}, \frac{5(p+1)}{8}, \frac{7(p+1)}{8} \right\} \end{aligned}$$

und

$$D = \left\{ \frac{p+1}{3}, \frac{2(p+1)}{3}, \frac{p+1}{6}, \frac{5(p+1)}{6} \right\}.$$

Wir wählen $\psi \in \operatorname{Irr}(\mathrm{PSL}(2,p))$ mit $\psi(1) = \frac{p-1}{2}$. Es gilt:

$$\begin{aligned} (\chi_{\text{solv}}, \psi) = \frac{1}{|\mathrm{PSL}(2,p)|} \cdot \Bigg( & |\mathrm{PSL}(2,p)| \frac{p-1}{2} + \frac{p^2-1}{2} \frac{p(p-1)}{2} \frac{-1+\sqrt{-p}}{2} \\ & + \frac{p^2-1}{2} \frac{p(p-1)}{2} \frac{-1-\sqrt{-p}}{2} \\ & + \frac{(p-1)p}{2} (-1)(p+4)(p+1) \\ & + (-1) \cdot 7(p+1)p(p-1) \\ & + 5(p+1)p(p-1) \left( -(-1)^{\frac{p+1}{8}} \right) + 0 \\ & + \frac{1}{4} \sum_{\substack{j=1 \\ j \notin A_j \cup V \cup D}}^{p+1} (p+1)p(p-1) \left( -(-1)^{\frac{p+1}{8}} \right) \Bigg) \\ = \frac{p-1}{2} - \frac{p-1}{2} - (p+4) - 14 - 10(-1)^{\frac{p+1}{8}} - \frac{1}{2} \sum_{\substack{j=1 \\ j \notin A_j \cup V \cup D}}^{p+1} (-1)^{\frac{p+1}{8}} \\ = -p - 4 - 14 - 10(-1)^{\frac{p+1}{8}} - \frac{1}{2} \sum_{\substack{j=1 \\ j \notin A_j \cup V \cup D}}^{p+1} (-1)^{\frac{p+1}{8}} \end{aligned}$$

Wie im letzten Fall machen wir eine Fallunterscheidung:

(1) $16 \mid p+1$
Es gilt $(-1)^{\frac{p+1}{8}} = 1$, und $V$ enthält wieder ausschließlich gerade Zahlen. Außerdem sind die Elemente in $A_j$ und $D$ allesamt gerade. Das bedeutet nun, dass die Menge $\{1, \ldots, p\} \setminus \left(A_j \cup V \cup D\right)$ genau 12 ungerade Zahlen mehr als gerade enthält. Für die obige Summe bedeutet das:

$$\frac{1}{2} \sum_{\substack{j=1 \\ j \notin A_j \cup V}}^{p+1} (-1)^{\frac{p+1}{8}} = \frac{1}{2} \cdot 12 \cdot (-1) = -6,$$

woraus nun

$$(\chi_{\text{solv}}, \psi) = -p - 4 - 14 - 10 + 6 = -p - 22$$

folgt.

(2) $16 \nmid p+1$
Hier gilt $(-1)^{\frac{p+1}{8}} = -1$, und $V$ enthält ausschließlich ungerade Zahlen. Die Mengen $A_j$ und $D$ bestehen aus geraden Elementen. Hier besitzt also $\{1, \ldots, p\} \setminus \left(A_j \cup V \cup D\right)$ genau vier ungerade Elemente mehr als gerade. Somit gilt

$$\frac{1}{2} \sum_{\substack{j=1 \\ j \notin A_j \cup V}}^{p+1} (-1)^{\frac{p+1}{8}} = -4,$$

und daher

$$(\chi_{\text{solv}}, \psi) = -p - 4 - 14 + 10 + 2 = -p - 6.$$

Wegen $p \geq 13$ ist in allen Fällen das angegebene Skalarprodukt negativ und somit $\chi_{\text{solv}}$ kein Charakter. $\square$

# Anhang A

# Charaktertafeln der Gruppen PSL$(2,p)$

Die Bezeichnungen der Konjugiertenklassen seien wie in den Bemerkungen (3.11) und (3.12) definiert. Da $\chi_{\text{solv}}$ auf 3- bzw. 4-Elementen spezielle Werte annimmt, sind in den folgenden Charaktertafeln diese Konjugiertenklassen zusätzlich aufgeführt, obwohl sie (je nach Fall) zu $Cl_{\frac{p-1}{2}}(j)$ bzw. $Cl_{\frac{p+1}{2}}(j)$ gezählt werden müssten. Weiter seien

$$\begin{aligned}
\zeta &:= \exp\left(\frac{2\pi\sqrt{-1}}{p-1}\right) \text{ eine primitive } (p-1)\text{-te,}\\
\xi &:= \exp\left(\frac{2\pi\sqrt{-1}}{p+1}\right) \text{ eine primitive } (p+1)\text{-te,}\\
\omega &:= \exp\left(\frac{2\pi\sqrt{-1}}{3}\right) \text{ eine primitive dritte und}\\
\tau &:= \exp\left(\frac{2\pi\sqrt{-1}}{4}\right) \text{ eine primitive vierte}
\end{aligned}$$

Einheitswurzel.

In den folgenden Tafeln kommen Serien von irreduziblen Charakteren vor, die durch Parameter $k$ und $l$ beschrieben werden. Diese Notation geht - wie auch die Charaktertafeln an sich - auf das GAP-Paket Chevie [GHL$^+$93] zurück und sei hier nur sehr kurz erläutert.
Wir unterscheiden zwei Fälle mit jeweils vier Unterfällen:

## A.1 $p \equiv 1 \bmod 4$

Im Folgenden gilt $1 \leq k \leq \frac{p-1}{2}$, $k \neq \frac{p-1}{4}, \frac{p-1}{2}$. Die beiden Ausnahmen entstehen dadurch, dass für diese $k$ der Charakter $\chi_5(k)$ nicht mehr irreduzibel ist. Genauer gilt

$$\chi_5\left(\frac{p-1}{4}\right) = \chi_3 + \chi_4 \quad \text{und} \quad \chi_5\left(\frac{p-1}{2}\right) = \chi_1 + \chi_2.$$

Für die Serie $\chi_6(l)$ ist $1 \leq l \leq \frac{p+1}{2}$, $l \neq \frac{p+1}{2}$, da sonst $\chi_6\left(\frac{p+1}{2}\right) = \chi_1 - \chi_2$ gilt.
Weiter sieht man leicht, dass für $1 \leq k < \frac{q-1}{4}$ stets $\chi_5(k) = \chi_5\left(k + \frac{p-1}{4}\right)$ gilt. Also kommt jeder irreduzible Charakter in der Serie $\chi_5(k)$ doppelt vor. Analoges gilt für die Anzahl der $\chi_6(l)$.

**Charaktertafel im Fall** $p \equiv 1 \bmod 4$, $p \equiv 1 \bmod 3$, $p^2 - 1 \not\equiv 0 \bmod 16$:

| | $Cl_1$ | $Cl_{p_1}$ | $Cl_{p_2}$ | $Cl_2$ | $Cl_3$ |
|---|---|---|---|---|---|
| $\chi_1$ | $1$ | $1$ | $1$ | $1$ | $1$ |
| $\chi_2$ | $p$ | $0$ | $0$ | $1$ | $1$ |
| $\chi_3$ | $\frac{p+1}{2}$ | $\frac{1-\sqrt{p}}{2}$ | $\frac{1+\sqrt{p}}{2}$ | $-1$ | $1$ |
| $\chi_4$ | $\frac{p+1}{2}$ | $\frac{1+\sqrt{p}}{2}$ | $\frac{1-\sqrt{p}}{2}$ | $-1$ | $1$ |
| $\chi_5(k)$ | $p+1$ | $1$ | $1$ | $(-1)^k + (-1)^{-k}$ | $\omega^k + \omega^{-k}$ |
| $\chi_6(l)$ | $p-1$ | $-1$ | $-1$ | $0$ | $0$ |
| $\chi_{\text{solv}}$ | $\frac{1}{2}p(p^2-1)$ | $\frac{1}{2}p(p-1)$ | $\frac{1}{2}p(p-1)$ | $(2p-1)(p-1)$ | $(p+3)(p-1)$ |

| | $Cl_{\frac{p-1}{2}}(i)$ | $Cl_{\frac{p+1}{2}}(j)$ |
|---|---|---|
| $\chi_1$ | $1$ | $1$ |
| $\chi_2$ | $1$ | $-1$ |
| $\chi_3$ | $(-1)^i$ | $0$ |
| $\chi_4$ | $(-1)^i$ | $0$ |
| $\chi_5(k)$ | $\zeta^{2ik} + \zeta^{-2ik}$ | $0$ |
| $\chi_6(l)$ | $0$ | $-\xi^{2jk} - \xi^{-2jk}$ |
| $\chi_{\text{solv}}$ | $p(p-1)$ | $p+1$ |

**Charaktertafel im Fall** $p \equiv 1 \bmod 4,\ p \equiv 2 \bmod 3,\ p^2 - 1 \not\equiv 0 \bmod 16$:

| | $Cl_1$ | $Cl_{p_1}$ | $Cl_{p_2}$ | $Cl_2$ | $Cl_3$ |
|---|---|---|---|---|---|
| $\chi_1$ | $1$ | $1$ | $1$ | $1$ | $1$ |
| $\chi_2$ | $p$ | $0$ | $0$ | $1$ | $-1$ |
| $\chi_3$ | $\frac{p+1}{2}$ | $\frac{1-\sqrt{p}}{2}$ | $\frac{1+\sqrt{p}}{2}$ | $-1$ | $0$ |
| $\chi_4$ | $\frac{p+1}{2}$ | $\frac{1+\sqrt{p}}{2}$ | $\frac{1-\sqrt{p}}{2}$ | $-1$ | $0$ |
| $\chi_5(k)$ | $p+1$ | $1$ | $1$ | $(-1)^k + (-1)^{-k}$ | $0$ |
| $\chi_6(l)$ | $p-1$ | $-1$ | $-1$ | $0$ | $-\omega^l - \omega^{-l}$ |
| $\chi_{\text{solv}}$ | $\frac{1}{2}p(p^2-1)$ | $\frac{1}{2}p(p-1)$ | $\frac{1}{2}p(p-1)$ | $(2p-1)(p-1)$ | $4(p+1)$ |

| | $Cl_{\frac{p-1}{2}}(i)$ | $Cl_{\frac{p+1}{2}}(j)$ |
|---|---|---|
| $\chi_1$ | $1$ | $1$ |
| $\chi_2$ | $1$ | $-1$ |
| $\chi_3$ | $(-1)^i$ | $0$ |
| $\chi_4$ | $(-1)^i$ | $0$ |
| $\chi_5(k)$ | $\zeta^{2ik} + \zeta^{-2ik}$ | $0$ |
| $\chi_6(l)$ | $0$ | $-\xi^{2jl} - \xi^{-2jl}$ |
| $\chi_{\text{solv}}$ | $p(p-1)$ | $p+1$ |

**Charaktertafel im Fall** $p \equiv 1 \bmod 4,\ p \equiv 1 \bmod 3,\ p^2 - 1 \equiv 0 \bmod 16$:

| | $Cl_1$ | $Cl_{p_1}$ | $Cl_{p_2}$ | $Cl_2$ | $Cl_3$ | $Cl_4$ |
|---|---|---|---|---|---|---|
| $\chi_1$ | $1$ | $1$ | $1$ | $1$ | $1$ | $1$ |
| $\chi_2$ | $p$ | $0$ | $0$ | $1$ | $1$ | $1$ |
| $\chi_3$ | $\frac{p+1}{2}$ | $\frac{1-\sqrt{p}}{2}$ | $\frac{1+\sqrt{p}}{2}$ | $1$ | $1$ | $(-1)^{\frac{p-1}{8}}$ |
| $\chi_4$ | $\frac{p+1}{2}$ | $\frac{1+\sqrt{p}}{2}$ | $\frac{1-\sqrt{p}}{2}$ | $1$ | $1$ | $(-1)^{\frac{p-1}{8}}$ |
| $\chi_5(k)$ | $p+1$ | $1$ | $1$ | $(-1)^k + (-1)^{-k}$ | $\omega^k + \omega^{-k}$ | $\tau^k + \tau^{-k}$ |
| $\chi_6(l)$ | $p-1$ | $-1$ | $-1$ | $0$ | $0$ | $0$ |
| $\chi_{\text{solv}}$ | $\frac{1}{2}p(p^2-1)$ | $\frac{1}{2}p(p-1)$ | $\frac{1}{2}p(p-1)$ | $(2p+3)(p-1)$ | $(p+6)(p-1)$ | $(p+4)(p-1)$ |

| | $Cl_{\frac{p-1}{2}}(i)$ | $Cl_{\frac{p+1}{2}}(j)$ |
|---|---|---|
| $\chi_1$ | $1$ | $1$ |
| $\chi_2$ | $1$ | $-1$ |
| $\chi_3$ | $(-1)^i$ | $0$ |
| $\chi_4$ | $(-1)^i$ | $0$ |
| $\chi_5(k)$ | $\zeta^{2ik} + \zeta^{-2ik}$ | $0$ |
| $\chi_6(l)$ | $0$ | $-\xi^{2jk} - \xi^{-2jk}$ |
| $\chi_{\text{solv}}$ | $p(p-1)$ | $p+1$ |

**Charaktertafel im Fall** $p \equiv 1 \bmod 4,\ p \equiv 2 \bmod 3,\ p^2 - 1 \equiv 0 \bmod 16$:

| | $Cl_1$ | $Cl_{p_1}$ | $Cl_{p_2}$ | $Cl_2$ | $Cl_3$ | $Cl_4$ |
|---|---|---|---|---|---|---|
| $\chi_1$ | $1$ | $1$ | $1$ | $1$ | $1$ | $1$ |
| $\chi_2$ | $p$ | $0$ | $0$ | $1$ | $-1$ | $1$ |
| $\chi_3$ | $\frac{p+1}{2}$ | $\frac{1-\sqrt{p}}{2}$ | $\frac{1+\sqrt{p}}{2}$ | $1$ | $0$ | $(-1)^{\frac{p-1}{8}}$ |
| $\chi_4$ | $\frac{p+1}{2}$ | $\frac{1+\sqrt{p}}{2}$ | $\frac{1-\sqrt{p}}{2}$ | $1$ | $0$ | $(-1)^{\frac{p-1}{8}}$ |
| $\chi_5(k)$ | $p+1$ | $1$ | $1$ | $(-1)^k + (-1)^{-k}$ | $0$ | $\tau^k + \tau^{-k}$ |
| $\chi_6(l)$ | $p-1$ | $-1$ | $-1$ | $0$ | $-\omega^l - \omega^{-l}$ | $0$ |
| $\chi_{\text{solv}}$ | $\frac{1}{2}p(p^2-1)$ | $\frac{1}{2}p(p-1)$ | $\frac{1}{2}p(p-1)$ | $(2p+3)(p-1)$ | $7(p+1)$ | $(p+4)(p-1)$ |

| | $Cl_{\frac{p-1}{2}}(i)$ | $Cl_{\frac{p+1}{2}}(j)$ |
|---|---|---|
| $\chi_1$ | $1$ | $1$ |
| $\chi_2$ | $1$ | $-1$ |
| $\chi_3$ | $(-1)^i$ | $0$ |
| $\chi_4$ | $(-1)^i$ | $0$ |
| $\chi_5(k)$ | $\zeta^{2ik} + \zeta^{-2ik}$ | $0$ |
| $\chi_6(l)$ | $0$ | $-\xi^{2jl} - \xi^{-2jl}$ |
| $\chi_{\text{solv}}$ | $p(p-1)$ | $p+1$ |

## A.2 $p \equiv 3 \bmod 4$

Wie oben gibt es auch hier wieder zwei parametrisierte Serien irreduzibler Charaktere. Die Parametrisierung ändert sich nur geringfügig. Es gilt zum einen $1 \leq k \leq \frac{p-1}{2}$, $k \neq \frac{p-1}{2}$. Ähnlich wie zuvor entsteht die Ausnahme durch $\chi_5\left(\frac{p-1}{2}\right) = \chi_1 + \chi_2$.
Zum anderen ist $1 \leq l \leq \frac{p+1}{2}$, $k \neq \frac{p+1}{4}, \frac{p+1}{2}$, da hier

$$\chi_5\left(\frac{p+1}{4}\right) = \chi_3 + \chi_4 \quad \text{und} \quad \chi_5\left(\frac{p+1}{2}\right) = \chi_1 - \chi_2.$$

Analog zum vorigen Fall sind die Anzahlen wieder zu halbieren.

**Charaktertafel im Fall** $p \equiv 3 \bmod 4,\ p \equiv 1 \bmod 3,\ p^2 - 1 \not\equiv 0 \bmod 16$:

| | $Cl_1$ | $Cl_{p_1}$ | $Cl_{p_2}$ | $Cl_2$ | $Cl_3$ |
|---|---|---|---|---|---|
| $\chi_1$ | $1$ | $1$ | $1$ | $1$ | $1$ |
| $\chi_2$ | $p$ | $0$ | $0$ | $-1$ | $1$ |
| $\chi_3$ | $\frac{p-1}{2}$ | $\frac{-1+\sqrt{-p}}{2}$ | $\frac{-1-\sqrt{-p}}{2}$ | $1$ | $0$ |
| $\chi_4$ | $\frac{p-1}{2}$ | $\frac{-1-\sqrt{-p}}{2}$ | $\frac{-1+\sqrt{-p}}{2}$ | $1$ | $0$ |
| $\chi_5(k)$ | $p+1$ | $1$ | $1$ | $0$ | $\omega^k + \omega^{-k}$ |
| $\chi_6(l)$ | $p-1$ | $-1$ | $-1$ | $-(-1)^l - (-1)^{-l}$ | $0$ |
| $\chi_{\text{solv}}$ | $\frac{1}{2}p(p^2-1)$ | $\frac{1}{2}p(p-1)$ | $\frac{1}{2}p(p-1)$ | $p(p+1)$ | $(p+3)(p-1)$ |

| | $Cl_{\frac{p-1}{2}}(i)$ | $Cl_{\frac{p+1}{2}}(j)$ |
|---|---|---|
| $\chi_1$ | $1$ | $1$ |
| $\chi_2$ | $1$ | $-1$ |
| $\chi_3$ | $0$ | $-(-1)^j$ |
| $\chi_4$ | $0$ | $-(-1)^j$ |
| $\chi_5(k)$ | $\zeta^{2ik} + \zeta^{-2ik}$ | $0$ |
| $\chi_6(l)$ | $0$ | $-\xi^{2jl} - \xi^{-2jl}$ |
| $\chi_{\text{solv}}$ | $p(p-1)$ | $p+1$ |

**Charaktertafel im Fall** $p \equiv 3 \bmod 4,\ p \equiv 2 \bmod 3,\ p^2 - 1 \not\equiv 0 \bmod 16$:

| | $Cl_1$ | $Cl_{p_1}$ | $Cl_{p_2}$ | $Cl_2$ | $Cl_3$ |
|---|---|---|---|---|---|
| $\chi_1$ | $1$ | $1$ | $1$ | $1$ | $1$ |
| $\chi_2$ | $p$ | $0$ | $0$ | $-1$ | $-1$ |
| $\chi_3$ | $\frac{p-1}{2}$ | $\frac{-1+\sqrt{-p}}{2}$ | $\frac{-1-\sqrt{-p}}{2}$ | $1$ | $-1$ |
| $\chi_4$ | $\frac{p-1}{2}$ | $\frac{-1-\sqrt{-p}}{2}$ | $\frac{-1+\sqrt{-p}}{2}$ | $1$ | $-1$ |
| $\chi_5(k)$ | $p+1$ | $1$ | $1$ | $0$ | $0$ |
| $\chi_6(l)$ | $p-1$ | $-1$ | $-1$ | $-(-1)^l - (-1)^{-l}$ | $-\omega^k - \omega^{-k}$ |
| $\chi_{\text{solv}}$ | $\frac{1}{2}p(p^2-1)$ | $\frac{1}{2}p(p-1)$ | $\frac{1}{2}p(p-1)$ | $p(p+1)$ | $4(p+1)$ |

| | $Cl_{\frac{p-1}{2}}(i)$ | $Cl_{\frac{p+1}{2}}(j)$ |
|---|---|---|
| $\chi_1$ | $1$ | $1$ |
| $\chi_2$ | $1$ | $-1$ |
| $\chi_3$ | $0$ | $-(-1)^j$ |
| $\chi_4$ | $0$ | $-(-1)^j$ |
| $\chi_5(k)$ | $\zeta^{2ik} + \zeta^{-2ik}$ | $0$ |
| $\chi_6(l)$ | $0$ | $-\xi^{2jl} - \xi^{-2jl}$ |
| $\chi_{\text{solv}}$ | $p(p-1)$ | $p+1$ |

**Charaktertafel im Fall** $p \equiv 3 \bmod 4,\ p \equiv 1 \bmod 3,\ p^2 - 1 \equiv 0 \bmod 16$:

| | $Cl_1$ | $Cl_{p_1}$ | $Cl_{p_2}$ | $Cl_2$ | $Cl_3$ | $Cl_4$ |
|---|---|---|---|---|---|---|
| $\chi_1$ | $1$ | $1$ | $1$ | $1$ | $1$ | $1$ |
| $\chi_2$ | $p$ | $0$ | $0$ | $-1$ | $1$ | $-1$ |
| $\chi_3$ | $\frac{p-1}{2}$ | $\frac{-1+\sqrt{-p}}{2}$ | $\frac{-1-\sqrt{-p}}{2}$ | $-1$ | $0$ | $-(-1)^{\frac{p+1}{8}}$ |
| $\chi_4$ | $\frac{p-1}{2}$ | $\frac{-1-\sqrt{-p}}{2}$ | $\frac{-1+\sqrt{-p}}{2}$ | $-1$ | $0$ | $-(-1)^{\frac{p+1}{8}}$ |
| $\chi_5(k)$ | $p+1$ | $1$ | $1$ | $0$ | $\omega^k + \omega^{-k}$ | $0$ |
| $\chi_6(l)$ | $p-1$ | $-1$ | $-1$ | $-(-1)^l - (-1)^{-l}$ | $0$ | $-\tau^k - \tau^{-k}$ |
| $\chi_{\text{solv}}$ | $\frac{1}{2}p(p^2-1)$ | $\frac{1}{2}p(p-1)$ | $\frac{1}{2}p(p-1)$ | $(p+4)(p+1)$ | $(p+6)(p-1)$ | $5(p+1)$ |

| | $Cl_{\frac{p-1}{2}}(i)$ | $Cl_{\frac{p+1}{2}}(j)$ |
|---|---|---|
| $\chi_1$ | $1$ | $1$ |
| $\chi_2$ | $1$ | $-1$ |
| $\chi_3$ | $0$ | $-(-1)^j$ |
| $\chi_4$ | $0$ | $-(-1)^j$ |
| $\chi_5(k)$ | $\zeta^{2ik}+\zeta^{-2ik}$ | $0$ |
| $\chi_6(l)$ | $0$ | $-\xi^{2jl}-\xi^{-2jl}$ |
| $\chi_{\text{solv}}$ | $p(p-1)$ | $p+1$ |

**Charaktertafel im Fall** $p \equiv 3 \bmod 4,\ p \equiv 2 \bmod 3,\ p^2-1 \equiv 0 \bmod 16$:

| | $Cl_1$ | $Cl_{p_1}$ | $Cl_{p_2}$ | $Cl_2$ | $Cl_3$ | $Cl_4$ |
|---|---|---|---|---|---|---|
| $\chi_1$ | $1$ | $1$ | $1$ | $1$ | $1$ | $1$ |
| $\chi_2$ | $p$ | $0$ | $0$ | $-1$ | $-1$ | $-1$ |
| $\chi_3$ | $\frac{p-1}{2}$ | $\frac{-1+\sqrt{-p}}{2}$ | $\frac{-1-\sqrt{-p}}{2}$ | $-1$ | $-1$ | $-(-1)^{\frac{p+1}{8}}$ |
| $\chi_4$ | $\frac{p-1}{2}$ | $\frac{-1-\sqrt{-p}}{2}$ | $\frac{-1+\sqrt{-p}}{2}$ | $-1$ | $-1$ | $-(-1)^{\frac{p+1}{8}}$ |
| $\chi_5(k)$ | $p+1$ | $1$ | $1$ | $0$ | $0$ | $0$ |
| $\chi_6(l)$ | $p-1$ | $-1$ | $-1$ | $-(-1)^l-(-1)^{-l}$ | $-\omega^k-\omega^{-k}$ | $-\tau^k-\tau^{-k}$ |
| $\chi_{\text{solv}}$ | $\frac{1}{2}p(p^2-1)$ | $\frac{1}{2}p(p-1)$ | $\frac{1}{2}p(p-1)$ | $(p+4)(p+1)$ | $7(p+1)$ | $5(p+1)$ |

| | $Cl_{\frac{p-1}{2}}(i)$ | $Cl_{\frac{p+1}{2}}(j)$ |
|---|---|---|
| $\chi_1$ | $1$ | $1$ |
| $\chi_2$ | $1$ | $-1$ |
| $\chi_3$ | $0$ | $-(-1)^j$ |
| $\chi_4$ | $0$ | $-(-1)^j$ |
| $\chi_5(k)$ | $\zeta^{2ik}+\zeta^{-2ik}$ | $0$ |
| $\chi_6(l)$ | $0$ | $-\xi^{2jl}-\xi^{-2jl}$ |
| $\chi_{\text{solv}}$ | $p(p-1)$ | $p+1$ |

# Anhang B

# Klassenwerte und Konstituenten von $\chi_p$ für symmetrische Gruppen

| $S_4$ | $[1^4]$ | $[2,1^2]$ | $[2^2]$ | $[3,1]$ | $[4]$ |
|---|---|---|---|---|---|
| $\chi_2$ | 24 | 12 | 16 | 15 | 4 |
| $(\,\cdot\,,\,\chi_2)$ | 4 | $-1$ | 1 | 3 | 12 |

| $S_5$ | $[1^5]$ | $[2,1^3]$ | $[2^2,1]$ | $[3,1^2]$ | $[3,2]$ | $[4,1]$ | $[5]$ |
|---|---|---|---|---|---|---|---|
| $\chi_2$ | 120 | 36 | 88 | 66 | 12 | 36 | 70 |
| $(\,\cdot\,,\,\chi_2)$ | 23 | $-3$ | 9 | $-2$ | 1 | 5 | 51 |

| $S_6$ | $[1^6]$ | $[2,1^4]$ | $[2^2,1^2]$ | $[2^3]$ | $[3,1^3]$ | $[3,2,1]$ | $[3^2]$ | $[4,1^2]$ |
|---|---|---|---|---|---|---|---|---|
| $\chi_2$ | 720 | 192 | 336 | 192 | 234 | 54 | 234 | 72 |
| $(\,\cdot\,,\,\chi_2)$ | 46 | 22 | 0 | 38 | $-6$ | $-12$ | 22 | $-6$ |

| $S_6$ | $[4,2]$ | $[5,1]$ | $[6]$ |
|---|---|---|---|
| $\chi_2$ | 72 | 120 | 54 |
| $(\,\cdot\,,\,\chi_2)$ | 30 | 38 | 116 |

| $S_7$ | $[1^7]$ | $[2,1^5]$ | $[2^2,1^3]$ | $[2^3,1]$ | $[3,1^4]$ | $[3,2,1^2]$ | $[3,2^2]$ | $[3^2,1]$ |
|---|---|---|---|---|---|---|---|---|
| $\chi_2$ | 5040 | 960 | 1008 | 1008 | 936 | 252 | 96 | 558 |
| $(\,\cdot\,,\,\chi_2)$ | 27 | 62 | $-24$ | 70 | 69 | $-45$ | 47 | $-23$ |

| $S_7$ | $[4,1^3]$ | $[4,2,1]$ | $[4,3]$ | $[5,1^2]$ | $[5,2]$ | $[6,1]$ | $[7]$ |
|---|---|---|---|---|---|---|---|
| $\chi_2$ | 216 | 152 | 24 | 240 | 140 | 126 | 42 |
| $(\,\cdot\,,\,\chi_2)$ | 26 | 15 | 84 | −37 | 94 | 140 | 211 |

| $S_8$ | $[1^8]$ | $[2,1^6]$ | $[2^2,1^4]$ | $[2^3,1^2]$ | $[2^4]$ | $[3,1^5]$ | $[3,2,1^3]$ | $[3,2^2,1]$ |
|---|---|---|---|---|---|---|---|---|
| $\chi_2$ | 40320 | 5760 | 4224 | 4320 | 3072 | 4680 | 1260 | 672 |
| $(\,\cdot\,,\,\chi_2)$ | 142 | 37 | −14 | −10 | 189 | 192 | −78 | 186 |

| $S_8$ | $[3^2,1^2]$ | $[3^2,2]$ | $[4,1^4]$ | $[4,2,1^2]$ | $[4,2^2]$ | $[4,3,1]$ | $[4^2]$ | $[5,1^3]$ |
|---|---|---|---|---|---|---|---|---|
| $\chi_2$ | 3060 | 468 | 864 | 560 | 320 | 252 | 32 | 720 |
| $(\,\cdot\,,\,\chi_2)$ | −133 | −32 | 261 | −66 | 83 | 110 | 181 | 91 |

| $S_8$ | $[5,2,1]$ | $[5,3]$ | $[6,1^2]$ | $[6,2]$ | $[7,1]$ | $[8]$ |
|---|---|---|---|---|---|---|
| $\chi_2$ | 520 | 420 | 252 | 720 | 336 | 8 |
| $(\,\cdot\,,\,\chi_2)$ | −38 | 270 | −74 | 334 | 355 | 564 |

| $S_9$ | $[1^9]$ | $[2,1^7]$ | $[2^2,1^5]$ | $[2^3,1^3]$ | $[2^4,1]$ | $[3,1^6]$ | $[3,2,1^4]$ |
|---|---|---|---|---|---|---|---|
| $\chi_2$ | 362880 | 60480 | 30720 | 21600 | 36864 | 32400 | 7632 |
| $(\,\cdot\,,\,\chi_2)$ | 1496 | 6 | 45 | 20 | 43 | 101 | 114 |
| $\chi_3$ | 362880 | 282240 | 228480 | 165888 | 99456 | 241920 | 181440 |
| $(\,\cdot\,,\,\chi_3)$ | 126 | −12 | −16 | −30 | 50 | −14 | −14 |

| $S_9$ | $[3,2^2,1^2]$ | $[3,2^3]$ | $[3^2,1^3]$ | $[3^2,2,1]$ | $[3^3]$ | $[4,1^5]$ | $[4,2,1^3]$ |
|---|---|---|---|---|---|---|---|
| $\chi_2$ | 5040 | 2880 | 23652 | 2484 | 19764 | 4320 | 1680 |
| $(\,\cdot\,,\,\chi_2)$ | −208 | 1629 | −147 | −250 | 324 | 404 | −145 |
| $\chi_3$ | 112896 | 38880 | 133056 | 62208 | 16200 | 201600 | 137088 |
| $(\,\cdot\,,\,\chi_3)$ | −116 | 146 | 214 | −36 | 84 | 74 | −64 |

| $S_9$ | $[4,2^2,1]$ | $[4,3,1^2]$ | $[4,3,2]$ | $[4^2,1]$ | $[5,1^4]$ | $[5,2,1^2]$ | $[5,2^2]$ |
|---|---|---|---|---|---|---|---|
| $\chi_2$ | 1632 | 1224 | 432 | 544 | 2880 | 1440 | 1120 |
| $(\,\cdot\,,\,\chi_2)$ | 28 | $-376$ | $-146$ | 1817 | 1754 | $-421$ | 681 |
| $\chi_3$ | 66432 | 88702 | 16704 | 45952 | 161280 | 94080 | 22080 |
| $(\,\cdot\,,\,\chi_3)$ | 18 | 126 | $-52$ | $-58$ | $-124$ | 412 | 370 |

| $S_9$ | $[5,3,1]$ | $[5,4]$ | $[6,1^3]$ | $[6,2,1]$ | $[6,3]$ | $[7,1^2]$ | $[7,2]$ |
|---|---|---|---|---|---|---|---|
| $\chi_2$ | 1350 | 280 | 1188 | 6552 | 3024 | 3024 | 84 |
| $(\,\cdot\,,\,\chi_2)$ | 40 | 279 | $-36$ | $-178$ | 1460 | 153 | 1181 |
| $\chi_3$ | 46080 | 2880 | 120960 | 51840 | 4716 | 81424 | 10080 |
| $(\,\cdot\,,\,\chi_3)$ | $-884$ | 862 | 1014 | $-1834$ | 2214 | $-6170$ | 5716 |

| $S_9$ | $[8,1]$ | $[9]$ |
|---|---|---|
| $\chi_2$ | 136 | 5184 |
| $(\,\cdot\,,\,\chi_2)$ | 730 | 2784 |
| $\chi_3$ | 40576 | 504 |
| $(\,\cdot\,,\,\chi_3)$ | 40996 | 48758 |

| $S_{10}$ | $[1^{10}]$ | $[2,1^8]$ | $[2^2,1^6]$ | $[2^3,1^4]$ | $[2^4,1^2]$ | $[2^5]$ | $[3,1^7]$ |
|---|---|---|---|---|---|---|---|
| $\chi_2$ | 3628800 | 564480 | 195840 | 91008 | 141312 | 65280 | 226800 |
| $(\,\cdot\,,\,\chi_2)$ | 1700 | 1726 | 302 | 580 | 13 | 655 | $-36$ |
| $\chi_3$ | 3628800 | 2661120 | 1877760 | 1237248 | 804096 | 1086720 | 1874880 |
| $(\,\cdot\,,\,\chi_3)$ | 126 | $-56$ | 70 | $-342$ | 16 | 3706 | $-116$ |

| $S_{10}$ | $[3,2,1^5]$ | $[3,2^2,1^3]$ | $[3,2^3,1]$ | $[3^2,1^4]$ | $[3^2,2,1]$ | $[3^2,2^2]$ | $[3^3,1]$ |
|---|---|---|---|---|---|---|---|
| $\chi_2$ | 40320 | 27792 | 9504 | 106272 | 11448 | 3744 | 30942 |
| $(\,\cdot\,,\,\chi_2)$ | $-6$ | $-331$ | 1248 | 366 | $-411$ | 1311 | 56 |
| $\chi_3$ | 1209600 | 695520 | 431136 | 729216 | 356832 | 303264 | 139644 |
| $(\,\cdot\,,\,\chi_3)$ | $-220$ | $-368$ | $-976$ | 8 | $-496$ | 180 | 886 |

| $S_{10}$ | $[4,1^6]$ | $[4,2,1^4]$ | $[4,2^2,1^2]$ | $[4,2^3]$ | $[4,3,1^3]$ | $[4,3,2,1]$ | $[4,3^2]$ |
|---|---|---|---|---|---|---|---|
| $\chi_2$ | 25920 | 6912 | 8512 | 3840 | 7272 | 1560 | 936 |
| $(\cdot,\chi_2)$ | 90 | 61 | −1060 | 2255 | −183 | −1158 | 332 |
| $\chi_3$ | 1301760 | 748800 | 402176 | 503040 | 378432 | 181440 | 86400 |
| $(\cdot,\chi_3)$ | −82 | 810 | −288 | 2590 | 754 | −1196 | 98 |

| $S_{10}$ | $[4^2,1^2]$ | $[4^2,2]$ | $[5,1^5]$ | $[5,2,1^3]$ | $[5,2^2,1]$ | $[5,3,1^2]$ | $[5,3,2]$ |
|---|---|---|---|---|---|---|---|
| $\chi_2$ | 4672 | 2112 | 168000 | 4320 | 6960 | 6120 | 840 |
| $(\cdot,\chi_2)$ | 1623 | 2357 | 2833 | 750 | 829 | −914 | 571 |
| $\chi_3$ | 187392 | 239616 | 820800 | 417600 | 235200 | 158400 | 136800 |
| $(\cdot,\chi_3)$ | 1062 | 1652 | −24 | −892 | 1186 | 100 | −1152 |

| $S_{10}$ | $[5,4,1]$ | $[5,5]$ | $[6,1^4]$ | $[6,2,1^2]$ | $[6,2^2]$ | $[6,3,1]$ | $[6,4]$ |
|---|---|---|---|---|---|---|---|
| $\chi_2$ | 2720 | 6800 | 4752 | 13680 | 3600 | 3942 | 216 |
| $(\cdot,\chi_2)$ | 1772 | 757 | 2913 | −835 | 1374 | 617 | 2885 |
| $\chi_3$ | 43200 | 53800 | 490752 | 209664 | 285984 | 47376 | 77760 |
| $(\cdot,\chi_3)$ | −4736 | −3274 | −412 | 3482 | 216 | −8308 | 32492 |

| $S_{10}$ | $[7,1^3]$ | $[7,2,1]$ | $[7,3]$ | $[8,1^2]$ | $[8,2]$ | $[9,1]$ | $[10]$ |
|---|---|---|---|---|---|---|---|
| $\chi_2$ | 9072 | 840 | 252 | 272 | 784 | 5184 | 450 |
| $(\cdot,\chi_2)$ | 124 | 726 | 3446 | −152 | 2874 | 3922 | 4416 |
| $\chi_3$ | 244272 | 100800 | 30240 | 86528 | 141824 | 504 | 33800 |
| $(\cdot,\chi_3)$ | 1438 | −18060 | 17658 | −14428 | 115458 | 89168 | 139370 |

# Anhang C

# Ausgewählte Sätze der Gruppen- und Darstellungstheorie

**(C.1) Lemma (vgl. [Isa06], Chapter 2, Lemma 2.15)**
Sei $\mathfrak{X}$ eine Darstellung der endlichen Gruppe $G$ und sei $g \in G$ von Ordnung $n$. Dann ist $\mathfrak{X}(g)$ ähnlich zu einer Diagonalmatrix aus $n$-ten Einheitswurzeln.

**(C.2) Satz (vgl. [Hup67], Kapitel V, Satz 11.7)**
Die Gruppe $G$ besitzt einen Zerfällungskörper, der über $\mathbb{Q}$ endlich-algebraisch und galoissch ist.

**(C.3) Lemma**
Sei $G$ eine endliche Gruppe und $g \in G$ und $p \in \mathbb{P}$. Dann existieren eindeutig bestimmte Elemente $g_p,\ g_{p'} \in G$ mit den Eigenschaften

(a) $|g_p|$ ist $p$-Potenz und $p \nmid |g_{p'}|$,

(b) $g_p g_{p'} = g = g_{p'} g_p$.

**Beweis**
Sei $|g| = p^r \cdot l$ mit $\mathrm{ggT}(p,\ l) = 1$. Schreibe $1 = ap^r + bl$ für geeignete $a, b \in \mathbb{Z}$. Dann erfüllen

$$g_p := g^{bl},$$
$$g_{p'} := g^{p^r l}$$

die gewünschten Eigenschaften. $\square$

**(C.4) Lemma (vgl. [Isa06], Chapter 2, Lemma 2.22)**
Sei $G$ eine endliche Gruppe und $N \trianglelefteq G$.

(a) Ist $\chi$ ein Charakter von $G$ und $N \subseteq \mathrm{Kern}(\chi)$, so ist $\chi$ konstant auf den Nebenklassen von $N$ in $G$ und die Funktion $\hat{\chi}$ auf $G/N$, definiert durch

$$\hat{\chi}(gN) = \chi(g),$$

ist ein Charakter von $G/N$.

(b) Ist $\hat{\chi}$ ein Charakter von $G/N$, so ist die Funktion $\chi$ auf $G$, definiert durch

$$\chi(g) = \hat{\chi}(gN),$$

ein Charakter von $G$.

(c) In (a) und (b) gilt:

$$\chi \in \mathrm{Irr}(G) \;\Leftrightarrow\; \hat{\chi} \in \mathrm{Irr}(G/N).$$

**(C.5) Satz (vgl. [JL93], Chapter 19, Theorem 19.18)**
Seien $G$ und $H$ endliche Gruppen. Seien

$$\begin{aligned} &\chi_1, \ldots, \chi_a \ \text{ die irreduziblen Charaktere von } G,\\ &\psi_1, \ldots, \psi_b \ \text{ die irreduziblen Charaktere von } H. \end{aligned}$$

Dann besitzt $G \times H$ genau $a \cdot b$ irreduzible Charaktere und diese sind die Abbildungen

$$\chi_i \boxtimes \psi_j : \ G \times H \to \mathbb{C}, \ (g, h) \mapsto \chi_i(g)\psi_j(h)$$

für $1 \leq i \leq a$ und $1 \leq j \leq b$.

**(C.6) Satz (vgl. [Hup67], Kapitel IV, Satz 2.8)**
Sei $G$ eine endliche Gruppe und $p$ der kleinste Primteiler der Ordnung von $G$. Es habe $G$ eine zyklische $p$-Sylow-Gruppe $P$. Dann gibt es einen Normalteiler $N$ von $G$ mit

$$G/N \cong P.$$

# Literaturverzeichnis


[Con07] CONRAD, Keith: *Dihedral groups I*. University of Connecticut, 2007. – http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/dihedral.pdf

[Con08] CONRAD, Keith: *Dihedral groups II*. University of Connecticut, 2008. – http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/dihedral2.pdf

[GHL+93] GECK, M. ; HISS, G. ; LÜBECK, F. ; MALLE, G. ; PFEIFFER, G.: *CHEVIE - Generic Character Tables of Finite Groups of Lie Type, Hecke Algebras and Weyl Groups*. Heidelberg : IWR-Preprint, 1993

[Giu07] GIUDICI, Michael: Maximal subgroups of almost simple groups with socle PSL(2, $q$). (2007)

[Hup67] HUPPERT, Bertram: *Endliche Gruppen I*. Springer-Verlag, 1967

[Isa06] ISAACS, I. M.: *Character Theory of Finite Groups*. AMS Chelsea Publishing, 2006

[JL93] JAMES, Gordon ; LIEBECK, Martin: *Representations and Characters of Groups*. Cambridge University Press, 1993

[Mor04] MORETÓ, Alexander: An answer to a question of J.G. Thompson on some generalized characters. In: *Journal of Algebra* 275 (2004), S. 75–76

[Tho68] THOMPSON, John G.: Nonsolvable finite groups all of whose local subgroups are solvable. In: *Bull. Amer. Math. Soc* 74 (1968), S. 383–437

[Tho96] THOMPSON, John G.: Some generalized characters. In: *Journal of Algebra* 179 (1996), S. 889–893

# Erklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, dass alle Stellen der Arbeit, die wörtlich oder sinngemäß aus anderen Quellen übernommen wurden, als solche kenntlich gemacht und dass die Arbeit in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegt wurde.

Ort, Datum Unterschrift